Beveiliging en Service Level Agreements

Beveiliging en Service Level Agreements

Bedreigingen en normen in een klant-leverancierrelatie

I.J.M. van Gogh
W.H.M. Hafkamp
P.M. Hoogendoorn
F.G.P. van den Hoven
W.R. Nanninga
E.J. Sol

PRAKTIJKREEKS
INFORMATIEBEVEILIGING

tenHagenStam
UITGEVERS

Reeds verschenen in de praktijkreeks informatiebeveiliging:

1 Internet, intranet en beveiliging: het technische kader
2 Wegwijzer voor IT-uitbestedingscontracten
3 Internet, intranet en beveiliging: het organisatorische kader
4 Elektronische werkplekbeveiliging
5 Vier jaar VIR, vloek of zegen?
6 Cryptografie in de praktijk
7 Checklist informatiebeveiliging
8 Technische beveiligingsstandaard Windows NT
9 Outsourcing (***deze al opnemen?***)

PRAKTIJKREEKS INFORMATIEBEVEILIGING

Eindredactie: Christian Jongeneel

Ontwerp omslag en binnenwerk: Bottenheft

ISBN 90----------

Inhoudsopgave

Voorwoord 9

1 Inleiding 11

2 Grondslagen van uitbesteding 21

2.1 ICT-dienstverlening, termen en begrippen 22
2.2 Beveiligingsaspecten 24
2.3 Aanpak van het uitbestedingsproces 25
2.4 Rapportage en controle 29

3 Uitbesteding van rekencentrumprocessen 31

3.1 Inbraak 32
3.1.1 Normen en maatregelen 32
3.2 Disfunctioneren van systemen en operationele processen 33
3.2.1 Normen en maatregelen 33
3.3 Uitval van infrastructurele voorzieningen 34
3.3.1 Normen en maatregelen 35
3.4 Onvoldoende opslagbeheer en afscherming van (output)gegevens 35
3.4.1 Normen en maatregelen 36
3.5 Onvoldoende borging van de beheersprocessen 37
3.5.1 Normen en maatregelen 38
3.6 Onvoldoende autorisatiebeheer 38
3.6.1 Normen en maatregelen 41
3.7 Onvoldoende scheiding tussen ontwikkel-, acceptatie- en productieomgeving 42
3.7.1 Normen en maatregelen 42
3.8 Aandachtspunten in de SLA 43

4 Uitbesteding van netwerkprocessen 49

4.1 Overzicht van netwerkdiensten 49
4.2 Inbraak 54

4.2.1 Normen en maatregelen 55
4.3 Verlies van gegevens 56
4.3.1 Normen en maatregelen 56
4.4 Teruglopen van de transportsnelheid 56
4.4.1 Normen en maatregelen 57
4.5 Onvoldoende configuratiebeheer en kabelbeheer 58
4.5.1 Normen en maatregelen 58
4.6 Onvoldoende capaciteitsbeheer 59
4.6.1 Normen en maatregelen 59
4.7 Onvoldoende wijzigingsbeheer 60
4.7.1 Normen en maatregelen 60
4.8 Aandachtspunten in de SLA 61

5 Uitbesteding van werkplekprocessen 67

5.1 Diefstal 69
5.1.1 Normen en maatregelen 70
5.2 Verlies van gegevens 70
5.2.1 Normen en maatregelen 71
5.3 Ongeoorloofd gebruik van programmatuur en gegevens/output 71
5.3.1 Normen en maatregelen 72
5.4 Niet kunnen werken 72
5.4.1 Normen en maatregelen 73
5.5 Onvoldoende werkplekbeheer 73
5.5.1 Normen en maatregelen 73
5.6 Inadequate helpdesk 74
5.6.1 Normen en maatregelen 74
5.7 Onvoldoende autorisatiebeheer 75
5.7.1 Normen en maatregelen 75
5.8 Onvoldoende configuratiebeheer 76
5.8.1 Normen en maatregelen 76
5.9 Softwarecontrole en -distributie 77
5.9.1 Normen en maatregelen 78
5.10 Aandachtspunten in de SLA 78

6 Uitbesteding van systeemontwikkelingsprocessen 87

6.1 Algemene risico's 89
6.2 Onvoldoende deskundigheid 91
6.2.1 Normen en maatregelen 91
6.3 Ongeschikte methode 92
6.3.1 Normen en maatregelen 93

6.4 Organisatorische ongeschiktheid 93
6.4.1 Normen en maatregelen 94
6.5 Onvoldoende autorisatiemogelijkheden 94
6.5.1. Normen en maatregelen 95
6.6 Onvoldoende softwarebeheer en -distributie 95
6.6.1 Normen en maatregelen 96
6.7 Onvoldoende sturing door de opdrachtgever 96
6.7.1 Normen en maatregelen 97
6.8 Onvoldoende duidelijke specificaties 97
6.8.1 Normen en maatregelen 98
6.9 Aandachtspunten in de SLA 98

7 Conclusies 105

Over Platform Informatiebeveiliging ?

Literatuurlijst 115

Voorwoord

Het Platform Informatiebeveiliging (PI) heeft als doel 'het bevorderen van de beveiliging van alle belangen betreffende gegevensverwerking, -opslag en -transport, alles in de ruimste zin van het woord'. Binnen deze doelstelling wordt het ontwikkelen van aanvaardbare richtlijnen voor de praktische inrichting van informatiebeveiliging als essentieel onderwerp gezien. Door het gezamenlijk opstellen van dergelijke richtlijnen kan worden gebruikgemaakt van praktijkervaringen, zodat een doeltreffende richtlijn ontstaat die ook uitvoerbaar is.

De PI-richtlijnen worden in werkgroepverband ontwikkeld onder auspiciën van een bestuurslid in de rol van projectleider. Deze ziet er onder meer op toe dat de PI-kwaliteitsrichtlijnen door de werkgroep worden gehandhaafd. De deelnemers van de werkgroepen zijn beveiligingsfunctionarissen en IT-auditors van uiteenlopende bedrijven en instellingen. Zij kenmerken zich door de hoge eisen die zij in hun advies- en controlewerkzaamheden aan organisaties moeten stellen in verband met de sterke automatiseringsgraad en de belangen die met de geautomatiseerde informatievoorziening zijn gemoeid. Door deze achtergrond vormen de deelnemers een representatieve afspiegeling van de aanwezige IT-beveiligingsexpertise in Nederland en bieden zij een draagvlak om gezag te verlenen aan de ontwikkelde richtlijnen, hetgeen bevorderlijk is voor de acceptatie door het algemene management en het IT-management.

Meestal zijn de PI-beveiligingsrichtlijnen primair bedoeld voor functionarissen die zijn belast met het implementeren van IT-systemen, zoals systeembeheerders en systeemprogrammeurs. Deze studie is echter vooral bedoeld voor management en medewerkers van projectorganisaties die belast zijn met het realiseren van de uitbesteding van ICT-processen aan een daartoe gespecialiseerde leverancier. Daarnaast zijn de richtlijnen van betekenis voor de volgende doelgroepen:

– IT-beveiligingsfunctionarissen (security officers en administrators). De IT-beveiligingsfunctie binnen een organisatie is verant-

woordelijk voor het (doen) treffen van beveiligingsmaatregelen. De richtlijnen bieden hierbij ondersteuning.
- IT-management en algemeen management. Het management is (eind)verantwoordelijk voor de informatiebeveiliging en geeft hieraan invulling door het (doen) analyseren van risico's en het bepalen van (globale) beveiligingsdoelstellingen.
- IT-auditors. De richtlijnen geven – gemotiveerd – de vereiste beveiligingsmaatregelen aan en de risico''s indien niet aan de vereisten is voldaan. Hierdoor kunnen de richtlijnen ook worden gehanteerd als toetsingsnorm bij IT-audits.

Aldus bieden de richtlijnen enerzijds een handreiking aan beveiligingsfunctionarissen en het algemene management en IT-management om een toereikende en evenwichtige beveiliging van de informatievoorziening te implementeren en bieden zij anderzijds een basis aan IT-auditors voor de normstelling bij de beoordeling van de beveiliging van een IT-systeem.

Deze studie is de vrucht van de samenwerking van verschillende deskundigen op het gebied van de informatiebeveiliging. Mede door de complexiteit van het onderwerp en de daarmee samenhangende duur van de totstandkoming, is er binnen de werkgroep die verantwoordelijk was voor de totstandkoming van dit rapport, enig verloop geweest.
Bij de totstandkoming van deze uitgave zijn in ieder geval de onderstaande organisaties nauw betrokken geweest: KPMG – Information Risk Management, Ministerie van Defensie – Defensie Accountantsdienst, Cap Gemini – Information Systems Management, KPN Telecom – Data Center, AKZO Nobel – Information Services, Rabobank Nederland, Origin en de Belastingdienst. Aan de totstandkoming van deze studie hebben tevens hun medewerking verleend: de heer H. de Zwart (EDP Auditpool), mevrouw A. Vos-Klaver (GAK), de heer J. Bronkhorst (Hewlett-Packard), de heren B. Oldenburg en B. Krijnen (Nederlandse Spoorwegen).

De auteurs:

I.J.M. VAN GOGH, KPMG Information Risk Management
W.H.M. HAFKAMP, Rabobank Nederland
P.M. HOOGENDOORN, KPMG Information Risk Management
F.G.P. VAN DEN HOVEN, Origin Nederland
W.R. NANNINGA, Cap Gemini, Information Systems Management
E.J. SOL, KPN Telecom

1 Inleiding

De toenemende integratie van automatisering met de bedrijfsprocessen en de eveneens toenemende complexiteit van automatiseringsoplossingen noodzaken tot voortdurende aandacht voor zowel het vereiste niveau van informatiebeveiliging als de technische realisering hiervan. Ook gezien de ontwikkelingen op het gebied van wet- en regelgeving met betrekking tot informatiebeveiliging is deze aandacht noodzakelijk.
Objectivering van het vereiste niveau van informatiebeveiliging en van de effectiviteit van gekozen technische oplossingen is voor veel organisaties een probleem, doordat slechts in beperkte mate standaarden voorhanden zijn. Beschikbare standaarden kennen ofwel een te beperkt werkingsgebied, of richten zich te veel op de organisatorische kant van de informatiebeveiliging. Door het gebrek aan deugdelijke standaarden zijn organisaties gedwongen zelf oplossingen te ontwikkelen en hieraan veel energie te besteden. De gevolgen zijn suboptimale oplossingen, verspilling doordat vele malen opnieuw het wiel moet worden uitgevonden en moeizame acceptatie door de afwezigheid van geobjectiveerde criteria.
Tegen deze achtergrond is het initiatief ontstaan om in werkgroepverband concrete, geobjectiveerde richtlijnen te ontwikkelen voor de inrichting respectievelijk de beoordeling van technische beveiligingsmaatregelen. Deze aanpak heeft de volgende voordelen:

- door uitwisseling van kennis, ervaring en inzicht ontstaat een belangrijk synergie-effect tussen de deelnemers; de deelnemers kunnen elkaar ondersteunen bij de keuze en implementatie van beveiligingsmaatregelen;
- met behulp van de ingebrachte kennis en inzichten kan worden gekomen tot de vaststelling van technische beveiligingsrichtlijnen die op een breed draagvlak kunnen rekenen;
- toepassing van de opgestelde beveiligingsrichtlijnen leidt bij de betrokken deelnemers tot een verhoging van de effectiviteit van de beveiliging.

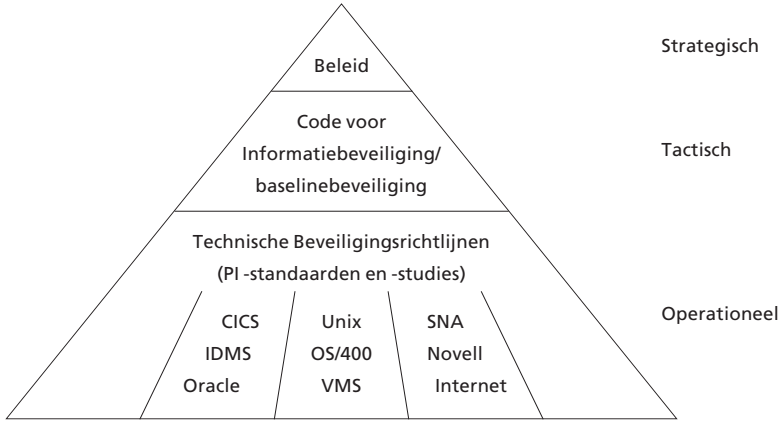
Het uitbesteden van ICT-activiteiten, ook wel outsourcing genoemd, is inmiddels overal geaccepteerd als een effectief instrument voor ICT-beheer. Bij de meeste ICT-inrichtings- of verbeterings-

trajecten speelt de vraag of (en zo ja, in welke mate) er dient te worden uitbesteed. Dit is tegenwoordig een vast onderdeel geworden waarop de ICT-beheersorganisatie en het management een antwoord dienen te geven. Een degelijk antwoord is om verschillende redenen echter niet altijd eenvoudig te geven. Een aantal problemen springt bij het uitbestedingsproces vaak naar voren:

- Het proces van outsourcing vraagt duidelijke afbakening van het uit te besteden ICT-object en de bijbehorende beheersorganisatie. In feite is dit de vraag 'wat besteden we precies uit'. Binnen de complexiteit van de taken en verantwoordelijkheden van de beheerorganisatie zal een afgrenzing gemaakt moeten worden die ook voor de toekomst werkbaar is.
- Als het object van uitbesteding eenmaal duidelijk is vastgelegd, en daarmee tevens de diensten die door de leverancier zullen worden geleverd, zal vastgesteld moeten worden aan welke kwaliteitseisen deze moeten voldoen. Deze normen worden uiteindelijk vastgelegd in het uitbestedingscontract, het Service Level Agreement (SLA) en de andere afspraken tussen de partijen.
- Het uitbestedingsproces is vaak een ingrijpend veranderingsproces met alle gevolgen van dien. Met name de veranderingen in de personele sfeer en daarmee samenhangende cultuurverschillen kunnen vaak tot grote onrust leiden. Deze onzekerheid zal zo goed mogelijk gekanaliseerd moeten worden en vooral niet te lang mogen voortduren. Overigens blijkt dat in het overgrote deel van de gevallen het initiële verzet van personeelsleden tegen de uitbesteding na verloop van tijd in positieve zin omslaat.
- In toenemende mate vormt de ICT een kernonderdeel van het bedrijfsproces. Het uitbesteden van de ICT kan dan ook een risico voor de bedrijfsvoering met zich meebrengen. Niet alleen zal er een zorgvuldige keuze gemaakt moeten worden bij de selectie van de leverancier, maar bovendien zal ervoor gezorgd moeten worden dat de communicatie met de leverancier – ook in de toekomst – optimaal blijft verlopen. Dit kan gewaarborgd worden door de inrichting van een service management organisatie die als intermediair tussen klant en leverancier fungeert.
- Het aangaan van een uitbestedingsrelatie is alleen lonend wanneer dit voor een langere periode gebeurt. Als er eenmaal afspraken gemaakt zijn en het veranderingsproces zich in beweging heeft gezet, dan is het gezien de impact en complexiteit vaak moeilijk om hierin nog al te grote wijzigingen aan te brengen. Eenmaal genomen beslissingen zijn dan ook vaak onherroepelijk.

Context De beveiligingsmaatregelen die in de richtlijnen worden beschreven vormen een onderdeel van de bredere context van het gehele samenstel van beveiligingsmaatregelen om de kwaliteit van de geautomatiseerde informatievoorziening te waarborgen. Beveiligingsmaatregelen binnen deze bredere context zijn bijvoorbeeld beschreven in de publicatie 'Code voor Informatiebeveiliging. Een leidraad voor Beleid en Implementatie' [Code]. Deze Code, die vooral in het bedrijfsleven wordt gebruikt, richt zich in het bijzonder op het tactische niveau binnen organisaties en bestrijkt het gehele terrein van informatiebeveiliging. Door het abstractieniveau geeft de Code echter weinig concrete handvatten voor het implementeren van beveiligingsmaatregelen bij IT-systemen. Hetzelfde geldt voor het besluit Voorschrift Informatiebeveiliging Rijksdienst, dat voor de rijksoverheid van toepassing is [VIR].
De PI-richtlijnen kunnen dan ook worden beschouwd als een verdere uitwerking van de Code en de baselinebeveiliging van het besluit VIR en zijn vooral gericht op het operationele niveau binnen organisaties. Daarnaast kan nog een strategisch niveau worden onderkend, dat betrekking heeft op de eindverantwoordelijkheid voor informatiebeveiliging van het topmanagement. De samenhang tussen deze drie niveaus is schematisch weergegeven in figuur 1.

FIGUUR 1



De informatiebeveiligingspiramide.

Aangezien voor het tactische niveau van informatiebeveiliging en voor de beleidsmatige en organisatorische maatregelen die op het strategische en tactische niveau moeten worden getroffen, al veel literatuur voorhanden is, wordt hierop in de PI-richtlijnen niet nader ingegaan. Het uitgangspunt van de PI-richtlijnen is dat op dit gebied voldaan is aan de Code voor Informatiebeveiliging en vergelijkbare standaarden, hetgeen inhoudt dat er een beveiligingsbeleid is, dat er functiescheiding is tussen ontwikkeling en productie, enzovoort.

Bij de implementatie van een product of architectuur (en in dit geval bij het uitbesteden van ICT-activiteiten) moet een evenwicht worden gevonden tussen risico's en het daarmee samenhangend beveiligingsniveau, invoerings- en beheerkosten en gevolgen voor de prestaties van het geheel van de geautomatiseerde verwerking. De richtlijnen bieden hierbij een praktische leidraad, hetgeen niet wegneemt dat organisaties altijd een vertaalslag moeten maken naar hun eigen specifieke omstandigheden.

Bij het opstellen van deze studie voor het positioneren van beveiligingsaspecten in Service Level Agreements is een achttal uitgangspunten leidend geweest:

Uitgangspunt 1: ICT-objecten Binnen het geheel van uit te besteden ICT-processen is een verdeling te maken in vier zogenaamde ICT-objecten, te weten: Rekencentrumdiensten, Netwerkdiensten, Werkplekautomatisering en Systeemontwikkeling.
Het uitbesteden van ICT-processen aan een daartoe gespecialiseerde leverancier is zo oud als de automatisering zelf. In de loop der jaren heeft de uitbesteding zich voortdurend aangepast aan de behoeften die voortkwamen uit de markt en de mogelijkheden die voortvloeiden uit de nieuwste technische evoluties. Dit heeft er toe geleid dat er inmiddels vele en soms ook zeer complexe vormen van uitbesteding bestaan.
Omdat het in het bestek van dit boek niet mogelijk is om alle vormen van uitbesteding te behandelen, is een selectie gemaakt van de belangrijkste en meest voorkomende vormen van uitbesteding. Uitgaande van het volledige ICT-proces is een opdeling gemaakt in de processen die zich afspelen rond het centrale verwerkingsplatform, de processen die gekoppeld zijn aan de verlening van netwerkdiensten en de processen die zich afspelen rond de werkplek van de gebruiker. Elke van deze drie (bundelingen van) ICT-processen wordt beschouwd als een specifiek 'object' dat kan worden uitbesteed.
Naast het ICT-proces zelf kunnen nog een aantal meer specialistische

ICT-objecten onderscheiden worden zoals bijvoorbeeld: systeemontwikkeling, detachering, opleidingen, (technisch) applicatiebeheer en uitwijk. Omdat alleen het object systeemontwikkeling dermate belangrijk en complex is, ook voor het ICT-proces zelf, zal dit additioneel als vierde uitbestedingsobject worden behandeld.

Deze vier ICT-objecten vormen vooralsnog de belangrijkste onderdelen binnen het volledige ICT-proces. Uitgaande van de dynamiek van de ontwikkelingen in de ICT is niet gezegd dat dit ook zo zal blijven. De gekozen modulaire opzet van deze studie maakt het mogelijk om in de toekomst de bestaande reeks van ICT-objecten verder uit te breiden. Een mogelijke kanshebber in dit verband zou kunnen zijn de uitbesteding van de activiteiten in relatie tot e-business.

Uitgangspunt 2: verantwoordelijkheid Uitbesteden van ICT-processen leidt slechts tot een overdracht van taken en verantwoordelijkheden. De eindverantwoordelijkheid voor de ICT-processen, inclusief de beveiligingsaspecten, kan niet worden overgedragen. Ook de ICT-processen die zijn uitbesteed, blijven verbonden met het bedrijf. De kwaliteit van het uitbestede ICT-proces en de producten die daaruit voortvloeien, behouden een directe invloed op het functioneren van de bedrijfsprocessen. Met name de functionele kant van de ICT is dermate vervlochten met de bedrijfsprocessen dat deze nimmer kan worden uitbesteed. Dit geldt evenzeer voor de instrumentele aspecten van de ICT, waarbij de effectiviteit en efficiency van de gebruikte ICT-middelen van belang zijn.
De uitbesteding heeft tevens tot gevolg dat er een hechte klant-leverancierrelatie ontstaat, waarbij afspraken worden gemaakt over de inhoud en de omvang van de te verrichten werkzaamheden. Niet alleen de leverancier, maar ook de klant zal er op moeten toezien dat deze afspraken ook daadwerkelijk worden nageleefd. Voor wat betreft de beveiligingsaspecten van een uitbesteed ICT-proces betekent dit dat er tussen klant en leverancier afspraken moeten bestaan over de beveiligingsnormen en de getroffen maatregelen. De handhaving van deze normen is evenzeer een verantwoordelijkheid van de klant als van de leverancier.

Uitgangspunt 3: taken Uitbesteding leidt in eerste instantie tot een reductie van ICT-processen en de daaraan verbonden werkzaamheden. De totstandkoming van een uitbestedingsrelatie tussen klant en leverancier leidt echter ook tot het ontstaan van nieuwe beheertaken.
De uitbesteding van een ICT-proces zal er in ieder geval toe leiden

dat de directe operationele werkzaamheden rond het proces op de leverancier zullen overgaan. In het verlengde daarvan zal er echter een beheerorganisatie ingericht moeten worden om enerzijds in de communicatie met de leverancier te kunnen voorzien en anderzijds het door de leverancier toegezegde normniveau te controleren. Zeker als een organisatie meer delen van het ICT-proces aan verschillende leveranciers heeft uitbesteed, is een versterkte vorm van Service Level Management beslist noodzakelijk.

Uitgangspunt 4: beveiligingsniveau De uitbesteding van ICT-processen mag niet leiden tot een aantasting van het bestaande beveiligingsniveau.
Het besluit om de ICT-processen te gaan uitbesteden komt vaak voort uit een bedrijfseconomische afweging. De uitbesteding zal ertoe moeten leiden dat de bedrijfsprocessen beter of goedkoper gaan functioneren. Beveiligingsaspecten spelen in deze beslissing nauwelijks een rol. Een (negatieve) bevestiging hiervan blijkt uit het feit dat organisaties die wel grote nadruk leggen op beveiligingsaspecten vaak besluiten om juist niet uit te besteden.
Uitgaand van het feit dat voorafgaand aan de uitbesteding reeds een passend beveiligingsniveau bestond, zal dit niveau ook na de uitbesteding voortgezet moeten worden. Uiteraard is het geen enkel probleem als de uitbesteding tot een andere of een efficiëntere uitvoering van de beveiliging leidt.

Uitgangspunt 5: ITIL Voor zover sprake is van beheerprocessen zal zo veel mogelijk aansluiting worden gezocht bij de methodiek en terminologie van ITIL.
Het gedachtegoed dat aan de ITIL-methodiek ten grondslag ligt, heeft inmiddels een brede verspreiding gevonden. Een groot aantal organisaties is ertoe overgegaan om het beheer van de ICT-processen voortaan conform ITIL te structureren. Door zo veel mogelijk gebruik te maken van de ITIL-terminologie kunnen begripsverwarring en misverstanden worden voorkomen. Door de brede toepassing van ITIL zal ook beter aangesloten kunnen worden bij reeds bestaande praktijksituaties.

Uitgangspunt 6: bedreigingen De bedreigingen die rond het ICT-proces manifest kunnen worden zijn verdeeld over vier hoofdgroepen: menselijke bedreigingen, systeemtechnische bedreigingen, infrastructurele bedreigingen en organisatorische bedreigingen.
Om een uitspraak te kunnen doen over beveiligingsmaatregelen is het noodzakelijk om eerst de bedreigingen te kennen die bij de uitbesteding van het ICT-proces kunnen optreden. Daarbij is geen

onderscheid gemaakt naar bedreigingen die altijd al verbonden waren aan een bepaald ICT-proces en bedreigingen die specifiek voortkomen uit het proces van uitbesteding van een uitbestedingsobject.
De grootste en waarschijnlijk ook de meeste bedreigingen komen voort uit al dan niet opzettelijk menselijk falen. Daarnaast kunnen problemen optreden in de kwaliteit van de verschillende systeemcomponenten, zoals de gebruikte hardware, software en gegevensverzamelingen. Ook de infrastructuur die ondersteuning biedt aan de informatiesystemen, kan defect raken. Ten slotte zijn organisatorische onvolkomenheden vaak de oorzaak van het niet tijdig kunnen voorkomen of onderkennen van potentiële bedreigingen, waardoor deze alsnog manifest kunnen worden.
Met name de organisatorische bedreigingen kunnen een aanzienlijk risico vormen dat vaak slechts met grote moeite kan worden ondervangen. Aan het element van de organisatorische bedreigingen en de bijbehorende compenserende maatregelen, zal in deze studie dan ook in ruime mate aandacht geschonken worden.

Uitgangspunt 7: beveiligingsnormen Bij het bepalen van de beveiligingsnormen die aan de uitbesteding van ICT-processen moeten worden gesteld, is niet zozeer gelet op de subjectieve wensen van de klant, maar is veeleer uitgegaan van de praktische maatregelen die door de leverancier getroffen kunnen worden.
Het uiteindelijke beveiligingsniveau van de ICT-processen bij de klant moet voorop staan. Echter, voor de wijze waarop dit niveau is bepaald, is gebruiktgemaakt van de concrete beveiligingsmaatregelen die de leverancier zou kunnen, en vaak zelfs zou moeten, treffen. Het is immers de leverancier die uiteindelijk bepaald of een beveiligingsmaatregel technisch uitvoerbaar of economisch haalbaar is. Als dit niet het geval is, zal de leverancier het betreffende beveiligingsniveau niet of alleen tegen onevenredige kosten kunnen leveren, hetgeen uiteindelijk ook in het nadeel van de klant zal zijn. In deze studie wordt dan ook alleen uitgegaan van bestaande en reële beveiligingsmechanismen.

Uitgangspunt 8: belang van de klant Bij het formuleren van de per uitbestedingsobject te hanteren beveiligingsnormen prevaleert steeds het belang van de klant.
Aan de zijde van de leverancier zullen de beveiligingsmaatregelen zich vooral concentreren op de continuïteit in het algemeen en de kwaliteit van de operationele processen in het bijzonder. Voor de klant liggen het niveau en de omvang van het door hem gewenste beveiligingsniveau een stuk hoger. Zo zullen de aspecten integriteit,

exclusiviteit en controleerbaarheid voor de klant van wezenlijk meer belang zijn dan voor de leverancier.
Om het klantbelang nog verder te benadrukken is gebruik gemaakt van de Code voor Informatiebeveiliging, waarin een aantal belangrijke ICT-gebruikers- en belangenverenigingen de door hun gestelde beveiligingseisen hebben gebundeld.

Doelstelling en scope van dit boek Het proces van uitbesteding, waar gewoonlijk in korte tijd op basis van vaak onvolledige informatie soms vergaande beslissingen worden genomen, is vaak een hectisch traject. Daarbij bestaat het gevaar dat belangrijke aspecten over het hoofd worden gezien of onvoldoende uitgewerkt. In de praktijk blijkt dit helaas ook te gelden voor een belangrijk kwaliteitsaspect als beveiliging. Deze studie is dan ook gericht op een tweetal doelstellingen:

METHODIEK Allereerst wordt het thema uitbesteding en de bijzondere plaats die beveiliging daarbinnen dient te hebben, op een strikt methodische wijze behandeld. Er wordt een aantal structuren geschetst die niet alleen specifiek gelden voor het beveiligingsaspect, maar ook voor het uitbestedingstraject als geheel. Aldus wordt een aantal handvatten geboden bij het uitbestedingstraject, die aan de concrete situatie kunnen worden aangepast.

VOLLEDIGHEID Door te kiezen voor een bottom-up benadering van de beveiligingsaspecten, waarbij in eerste instantie wordt uitgegaan van concrete bedreigingen, is ernaar gestreefd om op hoofdlijnen tot een zo volledig mogelijk beeld te komen. Tevens wordt voorkomen dat er in de SLA normen worden opgenomen die in de dagelijkse uitvoerende processen niet voorkomen, of nog erger, dat er in de SLA normen worden vergeten die in de reguliere processen wel degelijk van belang zijn. De SLA zal steeds een directe afspiegeling moeten zijn van de kwaliteits- en beveiligingsnormen die in de dagelijkse praktijk worden gehandhaafd.

Dit boek is vooral bedoeld om vanuit een brede verzameling concrete bedreigingen te komen tot een samenhangend geheel van een beperkt aantal van de belangrijkste beveiligingsnormen. Het detailniveau van deze normen is zodanig dat een directe vertaling gemaakt kan worden naar de in een SLA op te nemen bepalingen. Het uitbestedingscontract, dat hier zal worden beschouwd als aparte entiteit naast de SLA, is in feite de vastlegging van afspraken op een hoger hiërarchische niveau. De in het contract opgenomen normen zijn dan ook vaak van een hoger abstractieniveau. Wel zal een directe relatie moeten bestaan tussen de contractuele normen en de normen

die in de SLA worden gehanteerd en in feite een nadere concretisering zijn van de contractuele normen.
Dit boek is uitsluitend gericht op de beveiligingsaspecten in SLA's. Aan de inrichting van uitbestedingscontracten of de normen die daarin opgenomen zouden moeten worden, wordt vooralsnog voorbij gegaan.

Opzet van dit boek Dit boek is in feite opgebouwd uit twee delen. In hoofdstuk 2 wordt geschetst op welke wijze de uitbesteding in het algemeen en beveiligingaspecten in het bijzonder in een structuur kunnen worden geplaatst. De vier belangrijkste ICT-objecten die daaruit naar voren komen, worden in de hoofdstukken 3 tot en met 6 nader uitgewerkt. Het gaat daarbij om rekencentrumprocessen, netwerkprocessen, werkplekprocessen en systeemontwikkelingsprocessen. Van elk ICT-object worden aan de hand van de belangrijkste bedreigingen de daaraan verbonden beveiligingsmaatregelen nader toegelicht. Vervolgens wordt aangegeven welke beveiligingseisen en welke daaraan gekoppelde beveiligingsnorm de klant in de onderhandeling met zijn leverancier zal moet stellen om er zeker van te zijn dat de juiste beveiligingsmaatregelen door de leverancier geïmplementeerd worden. Hoofdstuk 7 biedt enkele conclusies en een matrix met de belangrijkste bedreigingen en maatregelen die per ICT-object kunnen voorkomen.

2 Grondslagen van uitbesteding

Zolang er automatiseringsdiensten worden verleend, bestaat ook de wens om deze dienstverlening in samenwerking met derden tot stand te brengen. De redenen hiervoor zijn zeer divers, maar zijn in principe altijd terug te voeren op de wens om de kwaliteit van de bestaande ICT-dienstverlening te verbeteren en de daarvoor aan te wenden middelen, met name de kosten, te beperken. Een van de oudste en meest bekende van deze vormen is de uitbesteding.
Uitbesteding is erop gericht om specifieke taken binnen de eigen dienstverlening te isoleren en vervolgens aan een zelfstandig te identificeren organisatie over te dragen. Dit kan zijn een andere afdeling binnen de eigen organisatie, maar ook een externe organisatie die in uitbesteding is gespecialiseerd. In alle gevallen ontstaat echter steeds een klant-leverancierrelatie.
De populariteit van uitbesteding neemt nog steeds toe. Hiervoor valt een groot aantal redenen te geven maar de belangrijkste zijn wel: de voortdurende vernieuwing en toenemende complexiteit van de ICT die steeds hogere eisen stelt aan de beheersing daarvan, de vaak hoge kosten versus de moeilijk te kwantificeren voordelen van de ICT, de groeiende schaarste aan deskundigheid en de toenemende bekendheid en ervaring met uitbesteding, die over het algemeen positief is te noemen.

Een aspect dat bijzondere aandacht verdient bij ICT-uitbesteding is de beveiliging. Wanneer een klant een deel van zijn automatisering door een derde partij laat uitvoeren, wil hij de zekerheid hebben dat de betrouwbaarheid van zijn informatievoorziening gehandhaafd blijft. Hij zal van de leverancier verlangen dat deze aantoonbaar aan de gestelde beveiligingseisen kan voldoen. De leverancier, die meestal meerdere klanten heeft, ziet zich voor de taak gesteld om voor elk van zijn klanten verschillende beveiligingseisen te realiseren. Deze studie geeft een overzicht van de risico's die spelen bij ICT-uitbesteding en van de beveiligingsmaatregelen waarmee deze risico's beheerst kunnen worden. Omdat de inhoud en de organisatievorm van ICT-uitbesteding per geval sterk verschillen, is het niet mogelijk om een algemeen geldend voorschrift voor beveiliging van ICT-uitbesteding te formuleren. In plaats daarvan geeft dit boek een

methode waarmee voor elke situatie de bedreigingen plus de bijbehorende beveiligingsmaatregelen gevonden kunnen worden. Ter illustratie is van de ICT-dienstenpakketten die veelal voorkomen, een overzicht van de belangrijkste bedreigingen en de daarbij passende maatregelen beschreven.
Ter inleiding wordt in het onderstaande eerst een beschrijving van de gebruikte termen en begrippen gegeven, niet alleen voor de uitbesteding maar ook voor de beveiligingsaspecten. Daarna volgt een beschrijving van de methode om bedreigingen en maatregelen voor elke situatie te kunnen bepalen. In de paragrafen die daarop volgen staan de belangrijkste bedreigingen en maatregelen beschreven die voor de uitbesteding van de verschillende ICT-objecten van toepassing zijn.

2.1 ICT-UITBESTEDING, TERMEN EN BEGRIPPEN

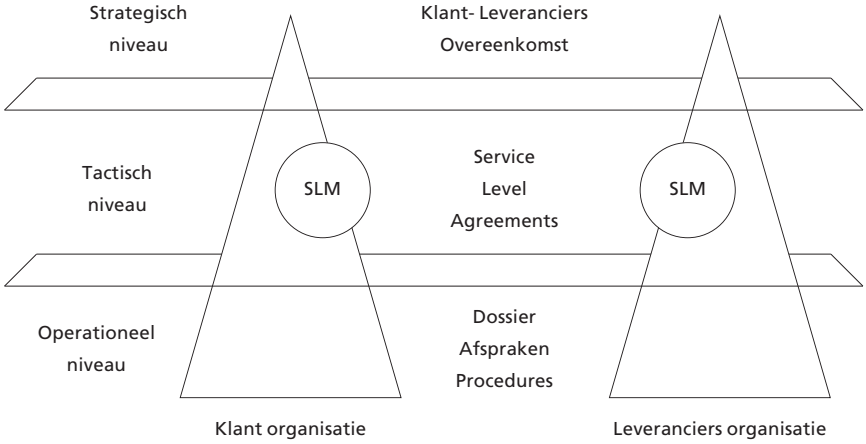
Onder ICT-uitbesteding wordt verstaan: het laten uitvoeren van (delen van) de informatievoorziening ten behoeve van een organisatie door een apart daarvoor ingerichte organisatie.
Een ander belangrijk begrip is de 'klant-leverancierrelatie'. Dit begrip is nauw verwant aan ICT-uitbesteding en duidt op de overdracht van de uitvoering van diensten aan een derde partij. Veelal wordt het begrip klant-leverancierrelatie uitsluitend gebruikt voor situaties waarin de dienstverlening door een extern bedrijf wordt verzorgd. Hier wordt deze situatie als een bijzonder geval van ICT-uitbesteding gezien. Ook wanneer de dienst wordt geleverd door een aparte afdeling binnen de eigen organisatie is sprake van klant-leverancierrelatie.
De omvang en diepgang van de ICT-uitbesteding kunnen van geval tot geval verschillen. Echter, ook in het meest minimale geval van ICT-uitbesteding zullen naast uitvoerende werkzaamheden eveneens beheersactiviteiten worden overgedragen. Aan de andere kant zijn er ook grenzen aan de maximale omvang en diepgang van de klant-leverancierrelatie. Zo is het voor de klant niet mogelijk om activiteiten uit te besteden die zuiver functioneel van aard zijn, of direct raken aan de strategische beleidsvorming binnen de eigen organisatie. Geconstateerd moet worden dat ICT-dienstverlening ondanks zijn vele verschijningsvormen een duidelijke onder- en bovengrens heeft.
Bij de klant-leverancierrelatie zijn minimaal twee partijen betrokken. Enerzijds is er de klant die (een deel van) de uitvoering en het beheer van zijn ICT-proces heeft uitbesteed aan een derde partij.

Anderzijds is er de leverancier die bereid is de uit te besteden taken en verantwoordelijkheden op zich te nemen. De relatie tussen de klant en de leverancier is op enigerlei wijze geformaliseerd in een klant-leverancierovereenkomst waarvan de vorm afhankelijk is van de aard van de relatie. De overeenkomst kan bijvoorbeeld in de vorm van een rechtsgeldig raamcontract zijn opgesteld, maar kan ook bestaan uit een beleidsuitspraak die stelt dat gemeenschappelijke ICT-voorzieningen geleverd dienen te worden door een aparte afdeling binnen het bedrijf.

Naast de aard van de klant-leverancierrelatie dienen ook afspraken omtrent de inhoud en kwaliteit van de dienstverlening te worden vastgelegd. Veelal gebeurt dit in een apart document, de Service Level Agreement (SLA). De procedures waarmee klant- en leveranciersorganisaties de activiteiten coördineren zijn veelal vastgelegd in een Dossier Afspraken en Procedures (DAP) of ook wel aangeduid als Operational Level Agreement.
De klant-leverancierrelatie is van groot belang, omdat het zowel inhoud geeft aan de communicatie tussen de klant en de leverancier als aan de structuur die daaraan ten grondslag ligt. De klant-leverancierrelatie raakt alle niveaus van de betrokken organisaties en is dan ook werkzaam op zowel strategisch niveau, waar klant-leverancierovereenkomsten (bijvoorbeeld uitbestedingsovereenkomsten met externe leveranciers) worden gesloten, als op tactisch niveau, waar de SLA's tot stand komen, als op operationeel niveau, waar de DAP's van toepassing zijn.
De klant-leverancierrelatie van ICT-uitbesteding zal er bij de klant niet alleen toe leiden dat (delen van) de ICT-beheersorganisatie verdwijnen, maar ook dat er nieuwe organisatorische structuren ontstaan. Om de klant-leverancierrelatie te kunnen sturen en beheersen, zal de klant een zogenaamde Service Requirement Management (SRM) organisatie moeten inrichten. Het Service Delivery Management (SDM) is het evenbeeld hiervan, maar dan aan de zijde van de leverancier. Tussen het SRM en SDM vindt een nadere invulling plaats van alle normen en afspraken die in het contract slechts op hoofdlijnen zijn vastgelegd. Daarnaast verloopt een belangrijk deel van de communicatie tussen klant en leverancier via de SRM en SDM (in de literatuur wordt vaak in dit verband gesproken van 'Smart Buyership').
Het Service Level Management (SLM) heeft tot taak te controleren of de gemaakte normen en afspraken ook daadwerkelijk worden nagekomen. Het vormt een onderdeel van het SRM voor het bewaken van de klantnormen en tevens de SDM voor het bewaken van de normen van de leverancier. Het SLM vormt de borging van de

tussen partijen afgesproken kwaliteit van de ICT-dienstverlening. De verschillende elementen van de klant-leverancierrelatie zijn samengevat in figuur 2.

FIGUUR 2



Service Management.

2.2 BEVEILIGINGSASPECTEN

In het ICT-proces speelt beveiliging een belangrijke rol. Ten aanzien van het begrip beveiliging kan daarbij onderscheid worden gemaakt in beveiliging in engere zin, waarbij alleen gekeken wordt naar het afschermen van gegevens en systemen inclusief de fysieke beveiliging daarvan, en beveiliging in bredere zin, waarbij ook andere aspecten worden betrokken, zodat een completer beeld wordt verkregen van de algemene kwaliteit van het ICT-proces.
In de loop der jaren zijn veelvuldig pogingen gedaan om overzichten van beveiligingsaspecten te maken, al dan niet gerelateerd aan onderdelen van en/of specifieke diensten binnen het ICT-proces. Een bekend voorbeeld is de Code voor Informatiebeveiliging [Code], die is voortgekomen uit een bundeling van de wensen en ervaringen van een aantal deskundigen van bekende Nederlandse bedrijven. De Code is inmiddels uitgegroeid tot een de facto standaard voor informatiebeveiliging. Uitgegaan wordt van beveiliging in ruime zin welke gebaseerd is op de basisprincipes:

– vertrouwelijkheid, het afschermen van systemen en gegevens tegen onbevoegde toegang en kennisname, ook wel aangeduid met het begrip exclusiviteit;

– integriteit, het waarborgen van de juistheid, volledigheid en tijdigheid van de gegevens en de verwerking daarvan;
– beschikbaarheid, het zeker stellen dat systemen naar behoren functioneren en de benodigde gegevens beschikbaar zijn, ook wel aangeduid als continuïteit.

Ook wordt controleerbaarheid wel als een apart beveiligingsaspect genoemd. Dit is echter niet noodzakelijk, omdat het meer een middel is om de andere beveiligingsaspecten zichtbaar te maken. In hoeverre effectiviteit en efficiëntie als beveiligingsaspecten beschouwd moeten worden, staat ter discussie. Vooralsnog worden deze eerder beschouwd als randvoorwaarden. Dit neemt echter niet weg dat deze aspecten in de SLA als geheel wel geadresseerd dienen te worden. Deze aspecten vallen echter buiten het huidige bestek.

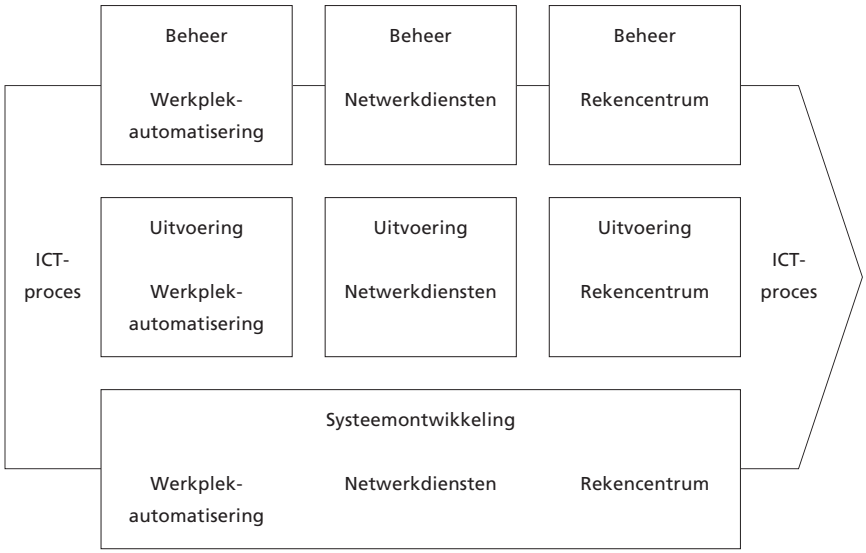
2.3 AANPAK VAN HET UITBESTEDINGSPROCES

De sleutelbegrippen in het uitbestedingsproces zijn het zogenaamde 'ICT-object' en de reeds eerder genoemde 'klant-leverancierrelatie'. Voor de structurering van de beveiligingsaspecten zal worden uitgegaan van de mogelijke bedreigingen, de gangbare beveiligingsmaatregelen die daarvoor getroffen moeten worden en de specifieke beveiligingseisen die tussen partijen worden vastgelegd om deze noodzakelijke maatregelen af te dwingen.

ICT-object Om in de complexe wereld van de klant-leverancierrelatie enige ordening aan te brengen is teruggegrepen op het ICT-proces in zijn meest elementaire vorm. In feite bestaat dit slechts uit de volgende onderdelen:
– De gebruikersinterface is het deel van het ICT-proces waarbij een interactie met de gebruiker plaatsvindt. Dit zijn gewoonlijk de werkstations of desktops met de bijbehorende randapparatuur. Ook de in deze apparatuur gebruikte besturings-, en applicatiesoftware valt hieronder.
– Het datatransport en -communicatie vormt de verbinding tussen de verschillende centrale en decentrale systemen. Deze verbindingen bestaan niet alleen uit kabels en een groot aantal fysieke netwerkcomponenten, zoals servers, routers en switches, maar ook uit netwerkbesturings- en beheerssoftware. Netwerken kunnen in aard en omvang sterk uiteenlopen.
– De centrale gegevensverwerking vindt plaats binnen rekencentra. Met behulp van mainframes vindt een grootschalige en daardoor goedkope verwerking en opslag van gegevens plaats.

Om het ICT-proces naar behoren te laten verlopen zal – voor elk van de onderdelen – tevens sprake moeten zijn van enige vorm van beheer, uitvoering en ontwikkeling. Aldus ontstaan er negen objecten die elk voor zich of in combinatie vatbaar zijn voor uitbesteding. In de praktijk blijkt dat binnen deze ICT-objecten een nadere opdeling wordt gemaakt in verschillende diensten. Het ontstaan van nieuwe diensten is sterk afhankelijk van ontwikkelingen in de markt en de technologie. Over de naamgeving en invulling van specifieke diensten bestaat dan ook vaak onduidelijkheid. Een overzicht wordt geboden in figuur 3.

FIGUUR 3



ICT-objecten.

In het vervolg zullen niet alle negen ICT-objecten afzonderlijk worden behandeld. De objecten beheer en uitvoering worden als dermate belangrijk beschouwd voor het goed functioneren van de verschillende procesonderdelen dat zij als een integraal onderdeel daarvan gezien worden. Aan de andere kant zal er voor wat betreft het object systeemontwikkeling per procesonderdeel weinig verschil bestaan. Dit resulteert in de volgende te onderscheiden ICT-objecten:

– werkplekautomatisering (gebruikersinterface, inclusief uitvoering en beheer);

– netwerkdiensten (datatransport, inclusief uitvoering en beheer);
– rekencentrum (centrale verwerking, inclusief uitvoering en beheer);
– systeemontwikkeling (binnen de werkplekautomatisering, de netwerkdiensten en het rekencentrum).

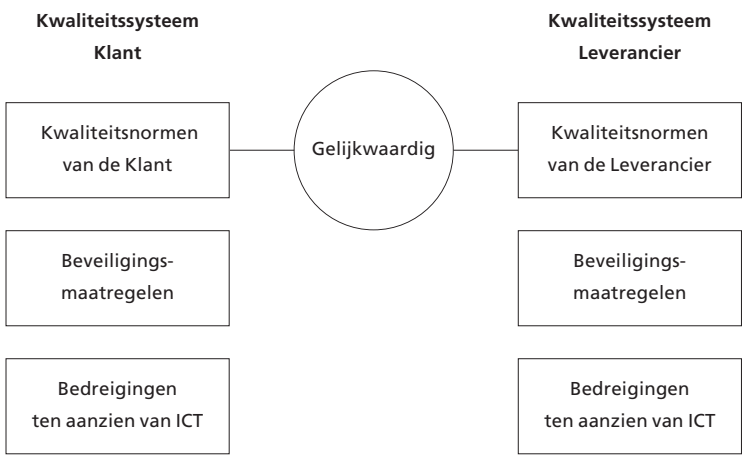
Klant-leverancierrelatie De overdracht van een ICT-object door de klant heeft tot gevolg dat (een deel van) de verantwoordelijkheid voor de operationele en beheerstaken overgaat op de leverancier. Daarentegen zullen de functionele verantwoordelijkheden alsmede de eindverantwoordelijkheid nimmer overgedragen kunnen worden.
Om de invulling en wederzijdse afstemming van deze verantwoordelijkheden goed te laten verlopen zal tussen de klant en leverancier een intermediaire organisatie gevormd worden, het eerder genoemde SLM. Hierbij wordt opgemerkt dat de werkzaamheden van het SLM zich gewoonlijk niet beperken tot het uitvoeren en bewaken van SLA's maar zich ook uitstrekken tot de andere niveaus van de klant-leverancierrelatie. Zo zal vanuit het SLM de aansturing van de DAP's plaatsvinden. Ervaringen met de klant-leverancierrelatie op tactisch en operationeel niveau zullen vanuit het SLM worden teruggekoppeld aan het strategische niveau, waardoor tot een bijstelling gekomen kan worden van de klant-leverancierovereenkomst. De gelaagde structuur van contracten, SLA's en DAP's, zorgt voor de noodzakelijk flexibiliteit binnen de vaste kaders van deze overeenkomst.
Gezien de sterke invloed van situationele omstandigheden zal het DAP hier buiten beschouwing blijven. De klant-leveranciercontracten en de SLA's zullen wel, zij het in meer algemene zin, worden behandeld.

Beveiligingsaspecten Om te komen tot de formulering van de noodzakelijke beveiligingseisen die in een klant-leverancierrelatie getroffen moeten worden, is in eerste instantie uitgegaan van de meest voor de hand liggende bedreigingen. Per ICT-object is een groepering gemaakt van bedreigingen die voortkomen uit menselijk falen, systeemtechnisch falen, infrastructureel falen en organisatorisch falen. Bij menselijk falen kan niet alleen worden gedacht aan fouten door onoplettendheid of onvoldoende kennis, maar ook aan bewust misbruik. Systeemtechnisch falen heeft betrekking op de gevolgen van het niet goed functioneren van de hard- en software. Infrastructureel falen wordt veroorzaakt door problemen in de directe omgeving van de systemen, zoals brand, oververhitting, stroomuitval, enzovoort. Organisatorisch falen is een relatief breed begrip en ver-

wijst naar problemen in het functioneren van de beheersorganisatie die van directe invloed zijn op de werking van de ICT.

Uitgaande van de bedreigingen wordt gekeken welke beveiligingsmaatregelen hiertegen gewoonlijk kunnen worden getroffen. Omdat sprake is van sterk operationele maatregelen en er daarnaast steeds is uitgegaan van een klant-leverancierrelatie, is in eerste instantie gekeken welke beveiligingsmaatregelen door de leverancier moeten worden getroffen om tot een acceptabel beveiligingsniveau te komen. Daarbij heeft tevens meegespeeld dat in de praktijk vaak de leverancier bepaalt wat het beveiligingsniveau zal zijn binnen de aangeboden klant-leverancierrelatie.
Formeel dient de klant van elk ICT-object, ongeacht of dit wordt uitbesteed of niet, een voor hem acceptabel beveiligingsniveau vast te stellen. Dit beveiligingsniveau laat zich vertalen in een stelsel van normen en maatregelen die noodzakelijk zijn om dit beveiligingsniveau te kunnen waarborgen. Door een ICT-object uit te besteden zal de verantwoordelijkheid voor de implementatie voor een belangrijk deel van de beveiligingsmaatregelen naar de leverancier overgaan. Wel zal de klant dienen aan te geven welke beveiligingsnormen de leverancier moet aanleggen. In de praktijk zal het er vaak op neerkomen dat de klant aangeeft op welke punten afgeweken wordt van het reeds bij de leverancier gehanteerde normenstelsel.
Een essentieel onderdeel van de keuze van een leverancier zal steeds gericht moeten zijn op een vergelijking van de aard en het niveau

FIGUUR 4



Matching van kwaliteitssystemen.

van het kwaliteitssysteem van de leverancier met het eigen kwaliteitssysteem (zie figuur 4). Let wel: beveiligingseisen hebben een specifiek karakter. Per eis zal bekeken moeten worden of de manier waarop de leverancier aan de eis invulling geeft, voor de specifieke klantsituatie de juiste is.

2.4 RAPPORTAGE EN CONTROLE

Controle op de juiste uitvoering van de beveiligingsmaatregelen is in eerste instantie een taak van het SLM, dat door middel van vooraf gedefinieerde rapportages inzicht heeft in de door de leverancier tot uitvoering gebrachte beveiligingsmaatregelen. Het afspreken van een goede rapportagestructuur is belangrijk voor het kunnen controleren van de kwaliteit en kwantiteit van de geleverde diensten.
Hoewel het afspreken van onderwerpen waarover gerapporteerd dient te worden niet moeilijk lijkt, blijkt in de praktijk toch vaak de verkeerde rapportage te worden gehanteerd. Enkele valkuilen hierbij zijn:

- Een overvloed aan rapportages, waardoor de essentiële items worden gemist. Een voorbeeld is het verstrekken van rapportage over de beschikbaarheid van alle applicaties en computers per dag en dat in een maandelijks rapport. De klant moet uit al die rapporten zelf samenstellen wanneer er uitval van zijn diensten is geweest en controleren of dat binnen de gemaakte afspraken valt. Dit is op zijn minst veel werk en vereist van de klant deskundigheid die niet relevant is voor zijn eigen business.
- Rapportages over irrelevante onderwerpen. Niet alle rapportage die kan worden verstrekt aan de klant is voor die klant relevant. Slechts die onderwerpen die de klant zelf kan begrijpen en constateren zijn van belang. Een voorbeeld is het verstrekken van overzichten over de gebruikte schijfruimte, terwijl de klant is geïnteresseerd in het feit of de gegevens op deze schijf door ongeautoriseerd personeel zijn benaderd.
- Een tekort aan rapportages, waardoor inzicht in de kwaliteit en kwantiteit van de geleverde diensten ontbreekt.

Het is dus zaak de balans te vinden tussen gerapporteerd worden over essentiële zaken zonder daarmee het totaalbeeld van de kwaliteit van de geleverde diensten te verliezen.

Een goede rapportage bestaat uit:

- Rapportage over afwijkingen van de afgesproken norm, bijvoorbeeld het uitvallen van een dienst langer dan de afgesproken normtijd.

- Rapportage over onderwerpen die voor de klant relevant zijn en begrepen kunnen worden zoals beschikbaarheid van de dienst voor de klant. De leverancier moet de vertaling maken van de beschikbaarheid van alle relevante componenten die de dienst vormen naar een totale beschikbaarheid voor de klant. Voorbeeld: een client-servertoepassing is beschikbaar als én de client-applicatie én het netwerk én de server beschikbaar zijn.
- Rapportage over het juist, volledig en tijdig (ofwel betrouwbaar) afhandelen van productieopdrachten, zoals het maandelijks draaien van de opdracht tot uitbetaling van salarissen.
- Rapportage over eventuele incidenten, zoals het ongeautoriseerd verwijderen van bestanden.
- Rapportage over verwachte gebeurtenissen die voor de klant belangrijk zijn, zoals gepland onderhoud, een grote interne verhuizing bij de leverancier waardoor de continuïteit van de dienstverlening in gevaar zou kunnen komen, enzovoort.
- De mogelijkheid om ad hoc rapportage op te vragen, bijvoorbeeld een overzicht van de beveiligingsincidenten van het afgelopen kwartaal. Hierover worden vooraf wel afspraken gemaakt, maar er wordt geen periodieke rapportage verstrekt. Op deze wijze kan de klant de aangeboden rapportage naar behoefte zelf regelen.

Daarnaast kan ook afgesproken worden dat de leverancier periodiek een onderzoek naar de kwaliteit van de beveiliging laat doen door een onafhankelijke derde. Dergelijk afspraken worden in de klant-leverancierovereenkomst vastgelegd, waarbij bepaald wordt dat jaarlijks een externe EDP-auditor de opdracht krijgt een zogenaamde third party-mededeling (TPM) op te stellen. De TPM bevat een oordeel over de kwaliteit van het stelsel van maatregelen van interne controle en beveiliging bij de leverancier en biedt de klant de garantie dat de leverancier zijn contractuele beveiligingsafspraken is nagekomen.

3 Uitbesteding van rekencentrumprocessen

Binnen het complex van geautomatiseerde bedrijfsprocessen van met name middelgrote en grote organisaties neemt het rekencentrum een centrale plaats in. Het rekencentrum omvat vaak meerdere mainframes en midrange systemen voor het uitvoeren van real-time en batchverwerking. Het rekencentrum dient gezien te worden als het geheel aan activiteiten gericht op de grootschalige exploitatie van de geautomatiseerde gegevensverwerking alsmede de beheersactiviteiten ten behoeve van de handhaving van de kwaliteit van de dienstverlening. Veel voorkomende synoniemen van het rekencentrum zijn data centre en computercentrum.
Gezien de centrale rol van rekencentra bij de verzorging van de geautomatiseerde informatievoorziening binnen bedrijven zijn deze omgeven met bijzondere beveiligingsmaatregelen. De concentratie van alle ICT-middelen rond één locatie vereenvoudigt het nemen van fysieke beveiligingsmaatregelen. Rekencentra zijn dan ook apart gelokaliseerd, niet openbaar toegankelijk en bovendien voorzien van extra infrastructurele voorzieningen tegen onder meer stroomstoring en brand.

Beveiliging is steeds gericht op het voorkomen of inperken van risico's en bedreigingen die de kwaliteit van de dienstverlening van het rekencentrum kunnen aantasten. Uit het spectrum van de kwaliteitsaspecten van informatiebeveiliging (continuïteit, vertrouwelijkheid en integriteit) is binnen het rekencentrum de waarborging van de continuïteit veruit het belangrijkste element. Het wegvallen van zelfs maar delen van de centrale geautomatiseerde gegevensverwerking zal direct gevolgen hebben voor het functioneren van de gehele informatievoorziening en daarmee ook de bedrijfsvoering in het algemeen. Op soms al korte termijn kan dit ernstige gevolgen hebben voor het imago en zelfs het voortbestaan van de onderneming.
De kwaliteitsaspecten vertrouwelijkheid en integriteit zijn weliswaar ook van belang, maar spelen in vergelijking met continuïteit een minder zwaarwegende rol. Dit mede vanwege het centrale en besloten karakter van het rekencentrum.
De belangrijkste kwaliteitseisen die aan de dienstverlening van het rekencentrum gesteld worden, zullen bij een eventuele uitbesteding

ervan ook nadrukkelijk naar voren moeten komen. Zowel in de uitbestedingsovereenkomst, maar meer nog in de SLA's zal aandacht besteed moeten worden aan continuïteitsbedreigingen en de beveiligingsmaatregelen die daartegen genomen moeten worden.

3.1 INBRAAK

Inbraak is een verzamelnaam voor een reeks van activiteiten waarbij ongeautoriseerde personen zich toegang verschaffen tot een object of een locatie, zoals een rekencentrum. Beveiligingsmaatregelen ter voorkoming of ontdekking van inbraak vormen nog steeds een actueel beveiligingsthema. Dat blijkt onder meer uit een in maart 1998 door Datapro Information Services (Gartner Group, Inc) gepubliceerde enquête waar 28 procent van de respondenten zich bezorgd toonde ('Concern for Risk') over onbevoegd Internet Access en 26 procent over onbevoegd System Access.
Bij inbraak kan onderscheid worden gemaakt tussen fysieke beveiligingsmaatregelen die zich bijvoorbeeld richten tegen het onbevoegd binnendringen in een gebouw, en logische beveiligingsmaatregelen die zich bijvoorbeeld richten tegen het onbevoegd binnendringen in systemen en netwerken. Dit laatste zal bij de behandeling van het autorisatiebeheer (paragraaf 3.6) verder worden uitgewerkt.
Bij het treffen van maatregelen tegen fysieke inbraak wordt een verdere verdeling gemaakt in bedreigingen die van binnenuit en die van buitenaf komen. Onderzoeken hebben aangetoond dat de inbraak van binnenuit de grootste bedreiging vormt. De eisen voor inbraakbeveiliging zijn per bedrijf verschillend, afhankelijk van de omvang, de organisatie en de geografische ligging van het rekencentrum.

3.1.1 Normen en maatregelen

Basisnormen voor een goede beveiliging tegen inbraak zijn:

- De fysieke beveiliging dient te voldoen aan de in Nederland gehanteerde normen uitgegeven door het Nederlands Normalisatie Instituut (NNI), de Stichting BORG of volgens de door het VIP ontworpen risicoklasse-indeling.
- De logische toegangsbeveiliging biedt weerstand tegen eenvoudige en geavanceerde inbraakpogingen welke laatste zijn gepubliceerd door CERT/CC of door de leverancier van het betreffende systeem.

Er dienen zowel preventieve alsmede repressieve en maatregelen genomen ter voorkoming en beperking van (verdere) bedrijfsschade door inbraak in de locatie van het rekencentrum alsmede kritische

systemen en gegevensverzamelingen. Als belangrijke basismaatregelen tegen inbraak zijn te noemen:
- er bestaat een integraal systeem voor toegangsbeveiliging;
- ICT-objecten worden onderscheiden en gecompartimenteerd;
- gebruikers worden geïdentificeer;
- toegangsautorisaties worden beperkt toegekend;
- het functioneren van de toegangsbeveiliging wordt bewaakt;
- medewerkers tekenen een geheimhoudingsverklaring.

3.2 DISFUNCTIONEREN VAN SYSTEMEN EN OPERATIONELE PROCESSEN

Vanuit de buitenkant bezien is het rekencentrum een soort fabriek waar in een volcontinu productieproces in opdracht van een systeemeigenaar bepaalde invoergegevens via een groot aantal verwerkingsstappen worden omgevormd tot eindproduct (uitvoer). Deze uitvoering van productie dient nauwkeurig te worden begeleid, zodat de verwerkingsstappen op het juiste moment en onder de juiste voorwaarden plaatsvinden.
Wat alle processen in het rekencentrum gemeen hebben, is het belang van een continue en ongestoorde voortgang. Beveiligingsmaatregelen dienen er in ieder geval op gericht te zijn om het blijvende functioneren van de centrale verwerkingsprocessen alsmede de in- en uitvoer stromen daarvan te waarborgen. Verstoringen in de in- en uitvoer kunnen veroorzaakt worden door een hardwaredefect, bijvoorbeeld een disfunctionerende lees/schrijfeenheid. Ook kunnen er tijdens de verwerking problemen ontstaan als bijvoorbeeld de jobbesturingsprogrammatuur fouten bevat. Maatregelen hiertegen liggen vooral in de organisatorische en personele sfeer door de werkzaamheden beter te structureren en controleren. Aanvullend kan ook gebruikgemaakt worden van systeemtechnische controlemaatregelen, zoals systeemchecks en monitoring tools.
Een tweede categorie van bedreigingen wordt veroorzaakt door onjuist menselijk handelen of beter gezegd menselijk falen, bijvoorbeeld doordat een operator een verkeerd commando geeft of een verkeerde tape laadt. Ook hier liggen de maatregelen in het verbeteren van de inrichting van de werkzaamheden en het verhogen van het kennisniveau.

3.2.1 Normen en maatregelen

De belangrijkste norm voor een goed functioneren van systemen en operationele processen is:
- Er dienen zowel preventieve als repressieve maatregelen genomen te worden om een vertraging of uitval van belangrijke

verwerkingsprocessen, inclusief de daaraan gekoppelde in- en uitvoerstromen, binnen het rekencentrum te voorkomen of tot een aanvaardbaar minimum te beperken.

De beveiligingsmaatregelen die gericht zijn tegen het disfunctioneren of uitvallen van belangrijke verwerkingsprocessen inclusief de daaraan gekoppelde in- en uitvoerstromen, kunnen zowel menselijk, systeemtechnisch als organisatorisch van aard zijn. Als belangrijke basismaatregelen tegen het disfunctioneren van systemen en operationele processen kunnen worden genoemd:
- documentatie en ondersteuning zijn in orde;
- toezicht en controle zijn geregeld;
- opleidingen zijn adequaat geregeld;
- systeemchecks vinden plaats;
- geautomatiseerd toezicht en controle is geregeld;
- in productieplanning is voorzien;
- problemen en storingen worden tijdig gesignaleerd;
- start-, storings- en herstelprocedures bestaan en worden nageleefd;
- er zijn mogelijkheden voor uitwijk;
- het beheer van de productieomgeving is adequaat.

3.3 UITVAL VAN INFRASTRUCTURELE VOORZIENINGEN

De grote concentratie van computersystemen, vaak binnen één of enkele ruimten van het rekencentrum, leidt tot de noodzaak om bijzondere infrastructurele maatregelen te treffen, zoals klimaatbeheersing, koelwater- en stroomvoorziening. Het uitvallen van deze voorziening zal direct gevolgen hebben voor de werking van de computersystemen en dus voldoende beveiligd moeten worden.
Infrastructurele maatregelen die direct voortkomen uit de beveiliging van de centrale computerruimte zijn onder meer fysieke toegangsbeveiliging, brandpreventie en -blusmiddelen, voorzieningen tegen spanningspieken en -uitval en ten slotte maatregelen tegen stof en straling.
Infrastructurele maatregelen zijn naar hun aard ingrijpend en kostbaar en kunnen per rekencentrum sterk verschillen. Factoren die van invloed zijn op de omvang van de infrastructurele beveiligingsmaatregelen zijn het beveiligingsbeleid, de omgevingskarakteristieken van de apparatuur en het belang dat wordt gehecht aan een continuïteit van de dienstverlening.

3.3.1 Normen en maatregelen

Als norm voor de infrastructurele voorzieningen geldt:

– De voor het functioneren van het rekencentrum noodzakelijke infrastructurele voorzieningen dienen zodanig te worden beveiligd dat de kwaliteit van de dienstverlening van het rekencentrum niet wordt aangetast.

De beveiligingsmaatregelen zijn enerzijds gericht op het waarborgen van de minimale kwaliteit van de infrastructurele maatregelen die noodzakelijk zijn voor het functioneren van het rekencentrum. Daarnaast zijn er infrastructurele maatregelen met een meer preventief of repressief karakter welke voortkomen uit de wens om een bepaald beveiligingsniveau te handhaven. Als belangrijkste basismaatregelen tegen de uitval van infrastructurele voorzieningen kunnen worden genoemd:

– er bestaat voldoende klimaatbeheersing;
– aan eisen ten aanzien van brandpreventie en blusmiddelen wordt voldaan;
– er zijn maatregelen getroffen ter voorkoming van waterschade;
– er zijn maatregelen getroffen ter voorkoming van stroomuitval;
– spanningspieken worden opgevangen;
– elektromagnetische straling wordt afgevangen;
– toegangsbeveiliging is geregeld.

3.4 ONVOLDOENDE OPSLAGBEHEER EN AFSCHERMING VAN (OUTPUT)GEGEVENS

De centrale taak van het rekencentrum is het verwerken van gegevens. De grote hoeveelheid gegevens die hiervoor gebruikt wordt, moet gestuurd en opgeslagen worden. Voor de opslag van gegevensbestanden wordt van verschillende media gebruikgemaakt zoals schijfgeheugen (ook wel Direct Acces Storage Device, DASD genoemd), cassette of tape, papier, microfiche en tegenwoordig steeds vaker cd-rom.
Een van de belangrijkste aspecten van het opslagbeheer is het registreren welke gegevens zich op welke locatie bevinden, zodat deze relatief eenvoudig zijn terug te vinden. Door een nauwkeurige registratie alsmede kennis van de maximale aanwezige opslagcapaciteit, kan de nog beschikbare opslagcapaciteit worden bepaald. Capaciteitstekorten kunnen zodoende vroegtijdig worden gesignaleerd.
Om de gewenste fysieke kwaliteit van gegevensdragers te waarborgen dient er een geconditioneerde omgeving te zijn, waarin de temperatuur en luchtvochtigheid bepaalde grenswaarden niet mogen

overschrijden. Daarnaast dienen de gegevensdragers, met name de magnetische tapes, periodiek te worden vervangen in verband met slijtage door veelvuldig gebruik. Dit betekent in de praktijk dat ieder gebruik van een tape dient te worden geregistreerd en geteld. De fabrikant van de tape stelt hierbij de richtlijnen op voor het vereiste moment van vervanging. Indien dit niet (op tijd) gebeurt, is het mogelijk dat lees- en schrijffouten optreden.
Logisch opslagbeheer heeft tot doel het realiseren van een zo effectief en efficiënt mogelijk gebruik van gegevensdragers. Dit vertaalt zich in een optimale bezetting van de gegevensdragers zonder dat de performance of opslagcapaciteit in gevaar komt.

Gegevens kunnen niet eeuwig op dezelfde gegevensdrager bewaard worden. Op een gegeven moment zullen deze vernietigd of op een andere gegevensdrager overgezet moeten worden. Voor de vernietiging van de gegevens zijn verschillende mogelijkheden aanwezig, zoals het fysiek onleesbaar of onwerkbaar maken van de gegevensdrager of het overschrijven van de gegevens met nullen of blanks.
Gegevensbestanden zijn vaak in klare, niet-vercijferde tekst opgeslagen op de gegevensdrager en zijn daardoor voor een derde vrij gemakkelijk toegankelijk. Om het ongeoorloofd gebruik van gegevens tegen te gaan zijn meerdere maatregelen noodzakelijk. Deze strekken zich uit over verschillende verantwoordelijkheidsgebieden waaronder fysieke toegangsbeveiliging, logisch toegangsbeheer, autorisatiebeheer en fysieke gegevens- en opslagbeheer.
Generiek gelden bij de definitie en implementatie van maatregelen de volgende principes:
- fysiek toegang tot het rekencentrum uitsluitend tot ruimten op basis van het principe 'need-to-be';
- logische toegang tot gegevens en programma's binnen het rekencentrum uitsluitend op basis van het principe 'need-to-know'.

3.4.1 Normen en maatregelen

Als normen gelden:
- Het rekencentrum dient enerzijds over voldoende opslagcapaciteit te beschikken, zodat gegevens altijd kunnen worden opgeslagen, en anderzijds over afdoende registratiesysteem, zodat gegevens snel weer teruggevonden kunnen worden.
- Gedurende de aanwezigheid van de gegevens binnen het rekencentrum zal de kwaliteit daarvan bewaakt moeten worden en zullen deze tegen onbevoegde gebruik afgeschermd moeten worden.

De beveiligingsmaatregelen zijn zowel gericht tegen menselijk falen, tegen systeemtechnisch falen als tegen organisatorische tekortkomin-

gen. Als belangrijkste basismaatregelen tegen onvoldoende afscherming van (output)gegevens en onvoldoende opslagbeheer kunnen worden genoemd:
- Er bestaat fysieke toegangsbeveiliging tot gegevensdragers en opslagruimten.
- Er bestaat logische toegangsbeveiliging van gegevensbestanden.
- Opgeslagen bestanden worden geregistreerd.
- Er is sprake van adequaat capaciteitsbeheer.
- Gegevensbestanden worden tijdig gemigreerd en opgeschoond.
- Afvoer en vernietiging van gegevensdragers is duidelijk geregeld.

3.5 ONVOLDOENDE BORGING VAN DE BEHEERSPROCESSEN

Om de voortgang van de door het rekencentrum geleverde diensten te kunnen waarborgen, is het noodzakelijk de operationele werkzaamheden in voldoende mate te coördineren en beheersen. Uiteraard geldt dit niet alleen voor de continuïteit van de dienstverlening, maar evenzeer voor de andere kwaliteitsaspecten (vertrouwelijkheid en integriteit), alsook voor de effectiviteit en efficiëntie van de bedrijfsvoering binnen het rekencentrum.
Bij het benoemen van de belangrijkste beheerscomponenten wordt gebruikgemaakt van de ITIL-methodiek. De Information Technology Infrastructure Library (ITIL) kan beschouwd worden als de beschrijving van een op de exploitatie van de ICT-structuur toegepast kwaliteitssysteem. Ten behoeve van de ICT-dienstverlening wordt binnen ITIL onderscheid gemaakt in een verzameling service support processen en een verzameling service delivery processen. De service support beheersprocessen liggen dicht tegen het operationele proces aan en omvatten configuration management, help desk, problem management, change management en software control & distribution. De service delivery beheersprocessen zijn evenzeer noodzakelijk voor een goede beheersing van de operationele processen binnen het rekencentrum, maar hebben een meer coördinerende functie. Service delivery omvat de beheersprocessen service level management, capacity management, contingency planning, availability management, cost management en security management.

In de communicatie tussen de klant en het rekencentrum zijn vooral de zogenaamde front-officeprocessen helpdesk en service level management van belang. De helpdesk zorgt voor de directe ondersteuning van de gebruiker, terwijl het service level management tot taak heeft om het kwaliteitsniveau van de dienstverlening te bewa-

ken. De overige ITIL-componenten behoren tot de back-office en zijn er volledig op gericht de interne verwerkingsprocessen van het rekencentrum te coördineren.
Indien binnen het rekencentrum onvoldoende aandacht wordt besteed aan de beheersing van de operationele processen, kan dit tot ernstige risico's voor de kwaliteit en met name de voortgang van de dienstverlening leiden. Er zullen zeer zeker beveiligingsmaatregelen tegen een dergelijk organisatorisch falen genomen moeten worden.

3.5.1 Normen en maatregelen

Als norm voor deugdelijke beheersprocessen geldt:

– Binnen het rekencentrum dienen de verwerkingsprocessen op een zodanige wijze te worden beheerst dat de kwaliteit van de dienstverlening kan worden gewaarborgd. Dit betekent dat er zowel sprake moet zijn van een duidelijke interne (ITIL) beheersstructuur, alsmede een goede communicatie met de klant.

Er dienen maatregelen genomen te worden tegen een organisatorisch falen van de rekencentrumorganisatie, zowel ten aanzien van de structurering van de interne beheersprocessen alsmede de wijze waarop met de klant wordt gecommuniceerd. Als belangrijke basismaatregelen tegen de onvoldoende borging van de beheersprocessen kunnen worden genoemd:

– Er dient sprake te zijn van:
  • duidelijke organisatiestructuur;
  • voldoende communicatie met de klant en gebruikers;
  • adequaat productiebeheer;
  • adequaat opslagbeheer.
– Directe ondersteuning van gebruikers is aanwezig.
– Incidenten en problemen worden adequaat opgelost.
– Er dient voldoende beheer te zijn van:
  • uitwijkprocedures en middelen;
  • configuratie;
  • capaciteit;
  • wijzigingen;
  • autorisaties.

3.6 ONVOLDOENDE AUTORISATIEBEHEER

De logische beveiliging van bedrijfsprocessen is niet alleen van belang voor de continuïteit, maar ook voor exclusiviteit en integriteit van die processen. De afscherming van processen en de daarbinnen voorkomende gegevensverzamelingen heeft vooral ten doel om

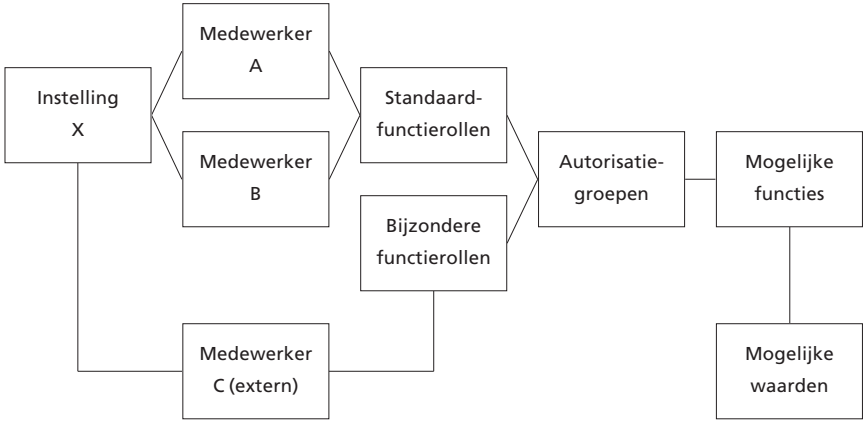
ervoor te zorgen dat alleen een beperkt aantal daartoe gerechtigde personen bepaalde gegevens mag opvragen en bewerken. De logische toegangsbeveiliging kan er tevens zorg voor dragen dat alleen voldoende deskundige personen toegang tot systemen en systeeminstellingen hebben en daarmee de kans op storingen voorkomen.

Functiescheidingen worden binnen organisaties veelvuldig toegepast. Door taken op te dragen aan verschillende personen met een tegengesteld belang wordt de kans op fouten (en ook fraude) sterk gereduceerd. Deze functiescheidingen kunnen met behulp van een systeem van logische toegangsbeveiliging ook in de aanwezige geautomatiseerde informatiesystemen worden geïmplementeerd.
Autorisatiebeheer is het toekennen, wijzigen en verwijderen van rechten in een systeem of applicatie. Voordat een gebruiker gebruik kan maken van de hem toegekende rechten, dient hij eerst te zijn ingelogd, dat wil zeggen, door het systeem te zijn geïdentificeerd (op basis van zijn gebruikersnaam) en geauthenticeerd (middels zijn persoonlijke wachtwoord). Een correct functionerend autorisatiebeheer is van essentieel belang. Het begrenst immers de mogelijkheden van de gebruiker en biedt zo bescherming tegen ongewenste inbreuk op de overige componenten van het systeem. Zo heeft een gebruiker bijvoorbeeld de mogelijkheid (via het hem toegekende recht) om bepaalde bestanden te lezen, gegevens te wijzigen of te verwijderen en programma's te starten.
Rechten worden toegekend aan diverse objecten. Dit kunnen zowel gebruikersnamen (user-id's) als (systeem)programma's zijn. Het toekennen gebeurt meestal direct bij het definiëren van het object door een systeembeheerder of beveiligingsmedewerker (security administrator). Hierbij wordt vaak gebruikgemaakt van speciale, ondersteunende programmatuur of in het systeem geïntegreerde hulpmiddelen, zoals panels voor het definiëren van Access Control Lists.
Autorisatierechten op zichzelf zijn geen starre, statische gegevens. Immers, functies in een organisatie zijn aan verandering onderhevig. Bovendien kunnen medewerkers van functie veranderen of ontslag nemen. Al deze aspecten dienen te leiden tot een herziening en/of wijziging van de toegekende rechten. Vaak worden de rechten toegekend op basis van een functierol (zie figuur 5).
De functierol is een clustering van medewerkers die (min of meer) gelijke taken uitvoeren binnen een bedrijfsproces. Functierollen worden mede gedefinieerd op basis van de behoefte tot het scheiden van de aanwezige functies en de daarmee samenhangende werkzaamheden. De functierol van bijvoorbeeld een baliemedewerker kent andere taken en bevoegdheden dan de functierol van de medewerker interne controle. De functierol wordt daarbij als het ware

'vertaald' naar systeem- of applicatierechten middels zogeheten autorisatiegroepen, waarbij soms per functierol verschillende waarden kunnen worden toegekend. Voorbeeld: bank X onderkent slechts één functierol van bankbaliemedewerker. Deze functierol is onder meer geautoriseerd voor het overboeken van geldbedragen tussen lopende betaalrekeningen bij die bank. Hierbij kan de bank bijvoorbeeld per medewerker waarden hanteren van (maximaal) *f*. 5000,-, *f*. 25.000,- of *f*. 1000.000,- per overboeking.

Ook binnen het rekencentrum is autorisatiebeheer een belangrijk aspect. Het takenpakket van veel rekencentrummedewerkers vereist soms vergaande rechten. Zo zal bijvoorbeeld een systeembeheerder hoge systeemrechten moeten hebben om systeemstoringen te kunnen analyseren en op te lossen. Middels die hoge rechten is hij vaak in staat om toegekende rechten aan anderen te 'overrulen'. Vanuit het oogpunt van 'need-to-know' en 'need-to-use' zal ernaar worden gestreefd om het aantal speciale rechten minimaal te houden. Om het dilemma van '(te) hoge systeemrechten' enerzijds en 'functienoodzaak' anderzijds verder te verminderen wordt meestal het principe van functiescheiding toegepast, waarbij de uitvoerende taken en de controlerende taken niet in handen van dezelfde persoon mogen liggen. Voor een rekencentrum betekent dit dat de werkzaamheden van bijvoorbeeld een systeembeheerder of operator nauwkeurig vastgelegd en gecontroleerd moeten worden, eventueel aangevuld met verbijzonderde controle door een medewerker van de interne controle afdeling.

FIGUUR 5



Functierollen.

Kort samengevat maakt het autorisatiebeheer gebruik van de elementen:
- onderhouden van een overzicht van beveiligde objecten;
- onderhouden van een overzicht van geautoriseerde gebruikers;
- onderhouden van een overzicht van functierollen;
- koppelen van rechten op ICT-objecten aan individuele gebruikers en hun functierol.

De bronnenregistraties die aan deze overzichten ten grondslag liggen, worden binnen andere afdelingen bijgehouden, bijvoorbeeld personeelszaken. Een mutatie in het personeelsbestand zal automatisch tot een signaal aan het autorisatiebeheer moeten leiden, waarna de bestaande overzichten worden aangepast.

3.6.1 Normen en maatregelen

Normen voor een adequaat autorisatiebeheer zijn:
- Het toekennen van rechten op ICT-objecten aan individuele personen, kortweg de toekenning van autorisaties, dient in overeenstemming te zijn met de onderkende functierollen en daarmee de functiescheiding binnen de bedrijfsprocessen te ondersteunen.
- Het beheer van de autorisaties en de onderliggende overzichten dient up-to-date te zijn.

Het autorisatiebeheer binnen het rekencentrum dient met behulp van een integraal systeem van toegangsbeveiliging te worden gewaarborgd. Bijgehouden moet worden welke functierollen er aanwezig zijn en welke medewerkers daartoe behoren. De functierollen dienen zodanig te zijn gekozen dat de functiescheiding optimaal wordt ondersteund. Als belangrijke basismaatregelen tegen onvoldoende autorisatiebeheer kunnen worden genoemd:
- Ongeoorloofde toegang tot en gebruik van systemen en programma's moet worden voorkomen.
- Ongeoorloofde toegang tot en gebruik van gegevens en output moet worden voorkomen.
- Ongeautoriseerde bewerkingen moeten worden voorkomen.
- Er dient adequaat autorisatiebeheer te zijn.

3.7 ONVOLDOENDE SCHEIDING TUSSEN ONTWIKKEL-, ACCEPTATIE- EN PRODUCTIEOMGEVING

Voor de continuïteit van de dienstverlening door het rekencentrum is het ongestoord functioneren van de productieomgeving van groot belang. Door middel van verschillende beheersfuncties wordt het functioneren van de productieomgeving voortdurend bewaakt en verbeterd. Daarnaast zal de productieomgeving afgeschermd worden tegen ongewenste externe invloeden die mogelijk tot een verstoring zouden kunnen leiden.
Naast de productieomgeving kent een rekencentrum ook andere omgevingen voor het ontwikkelen, testen en accepteren van programmatuur, alsmede voor specifieke herstel- en uitwijkoperaties. Ook deze omgevingen worden met zorg ingericht en voortdurend verbeterd. Niet alleen ongewenste externe invloeden, maar ook een ongewenste wisselwerking tussen de omgevingen zal zo veel mogelijk voorkomen moeten worden middels een stringente afscherming. Afscherming van de verschillende omgevingen zal in eerste instantie door middel van fysieke of logische inrichtingsmaatregelen tot stand gebracht worden. Daarnaast is reeds gewezen op het belang van fysieke en logische beveiliging, die ook hier bij de afscherming belangrijke instrumenten zijn.
Voor zover het noodzakelijk is in een van de bestaande omgevingen een wijziging aan te brengen, zal dit via duidelijke procedures dienen te verlopen. Change management zorgt ervoor dat het wijzigingsproces op een gestructureerde manier wordt doorlopen, inclusief de noodzakelijke maatregelen van functiescheiding en controle. Doordat binnen het change management veel aandacht wordt besteed aan het registratieve aspect, kunnen wijzigingen die onverhoopt tot problemen hebben geleid, achteraf gemakkelijk geëvalueerd worden.

3.7.1 Normen en maatregelen

Als normen gelden:

- Er dient een adequate logische en fysieke scheiding te zijn tussen de ontwikkel-, acceptatie-, en productieomgeving. Elk van de omgevingen worden afgeschermd door een systeem van toegangsbeveiliging.
- Zowel het doorvoeren van wijzigingen binnen een omgeving als het transport tussen de verschillende omgevingen, dient volgens vaste wijzigingsprocedures te verlopen.

Om de ongestoorde dienstverlening van het rekencentrum te waarborgen dient de productieomgeving afgeschermd te worden van verstorende externe invloeden. Wijzigingen mogen alleen via een

vaste procedure worden doorgevoerd. Als belangrijke basismaatregelen tegen een onvoldoende scheiding van de ontwikkel-, acceptatie- en productieomgeving kunnen worden genoemd:
- De productieomgeving dient volledig afgescheiden te zijn.
- De productieomgeving dient vrij te zijn van ontwikkeltools.
- Wijzigingen in de productieomgeving kunnen alleen via eenduidige procedures plaatsvinden.
- (Ongeoorloofde) wijzigingen dienen gesignaleerd en geregistreerd te worden.
- Er moet change management ingericht zijn.

3.8 AANDACHTSPUNTEN IN DE SLA

De kwaliteit van de werkzaamheden door het rekencentrum wordt zowel bepaald door de wijze waarop de verwerkingsprocessen ingericht en beheerst worden, alsmede door de wijze waarop de communicatie tussen het rekencentrum en de klant verloopt. Gewoonlijk wordt deze tweedeling binnen het rekencentrum tot uiting gebracht door een onderscheid te maken tussen front- en back-officeprocessen.
Deze tweedeling is ook van invloed op de SLA en de daarin opgenomen vereisten ten aanzien van de beveiligingsafspraken. Daar waar bij front-officeprocessen sprake is van een directe communicatie met het rekencentrum, zal de klant ook directe eisen kunnen stellen. Een bekend voorbeeld zijn de beschikbaarheidseisen die in een SLA gesteld worden aan de bereikbaarheid van de helpdesk.
De back-officeprocessen daarentegen zullen voor de klant grotendeels 'verborgen' blijven. De klant zal dan ook slechts een indirecte invloed kunnen uitoefenen op het functioneren en de beveiliging van deze processen. Om bijvoorbeeld vast te kunnen stellen of het change management en andere onderdelen van de beheersorganisatie naar behoren hebben gefunctioneerd, zal een beroep worden gedaan op een onafhankelijk EDP-auditor die hierover na onderzoek een 'third party'-verklaring afgeeft. In de SLA kan worden volstaan met de afspraak dat jaarlijks een onafhankelijke audit zal worden uitgevoerd.

De klant zal in de SLA die hij met de leverancier sluit een afweging moeten maken over te nemen beveiligingsmaatregelen, alsmede de aard en omvang van die beveiligingsmaatregelen. Normaliter bestaat binnen het rekencentrum van de leverancier al een bepaalde standaard voor het minimum beveiligingsniveau, de zogenaamde base-level security.

De specifieke waarde van de SLA ligt niet alleen in de expliciete vastlegging van het bestaande beveiligingsniveau. Ook kan het gebruikt worden om aanvullende beveiligingseisen in op te nemen. De SLA is de formalisering van het door de leverancier binnen het rekencentrum te hanteren beveiligingsniveau. Aan de hand van de eerder onderscheiden bedreigingen zal een nader overzicht gegeven worden van de elementen die in een SLA opgenomen kunnen worden. In de voorgaande paragrafen is een overzicht gegeven van de belangrijkste bedreigingen die binnen het rekencentrum kunnen voorkomen, alsmede de maatregelen die tegen deze bedreigingen genomen kunnen worden. Per onderwerp worden hierna de aandachtspunten voor de SLA genoemd.

Inbraak De beveiliging tegen inbraak is voornamelijk een verantwoordelijkheid van de back-office. Voor wat betreft de fysieke toegangsbeveiliging is het voldoende om in de SLA een algemene bepaling op te nemen. Ter controle kan door een onafhankelijke auditor periodiek (jaarlijks) een controle worden uitgevoerd naar de kwaliteit van de fysieke beveiliging. Ernstige gevallen van inbreuk zullen aan de klant gemeld moeten worden.
De logische toegangsbeveiliging vereist een directe betrokkenheid van de klant, echter alleen voor zover deze betrekking heeft op diens applicaties en gegevensbestanden. Hier wordt alleen gekeken naar de inrichting van de logische toegangsbeveiliging. Het beheer ervan zal nog nader ter sprake komen bij het autorisatiebeheer.
Eisen in de SLA betreffen:
- algemene eisen ten aanzien van fysieke toegangsbeveiliging;
- periodieke audit van de fysieke beveiliging;
- algemene eisen ten aanzien van logische toegangsbeveiliging;
- classificatie van systemen;
- periodieke audit van de logische beveiliging;
- rapportage bij ernstige inbreuk.

Aantasting van systemen en operationele processen De beveiliging tegen de aantasting van systemen en operationele processen is erop gericht om de voortgang van de verwerkingsprocessen binnen de back-office te waarborgen. De deskundigheid en kwaliteit van de operationele werkzaamheden zijn van directe invloed op de reputatie van de leverancier. Daarnaast kan door een onafhankelijk deskundige periodiek een oordeel gegeven worden over de algemene kwaliteit van de operationele processen.
Hoewel hier sprake is van back-officeprocessen dienen er in de SLA wel degelijk uitdrukkelijke eisen gesteld te worden aan de minimale beschikbaarheid, de verwerkingssnelheid, de capaciteit en de contro-

leerbaarheid daarvan. Ook is het van groot belang in de SLA aandacht te besteden aan de procedure die gevolgd wordt bij het uitvallen van de productie. De klant zal eisen moeten stellen aan de snelheid waarmee de productieomgeving wordt hersteld of tot uitwijk wordt overgegaan. De mate waarin recovery mogelijk is zal deels afhankelijk zijn van de door de klant gekozen back-up-methode.
Eisen in de SLA betreffen:
- reputatie leverancier;
- beschikbaarheid;
- verwerkingssnelheid;
- verwerkingscapaciteit;
- methode van back-up;
- methode van recovery;
- uitwijk;
- rapportage beveiligingseisen;
- periodieke audits.

Uitval van infrastructurele voorzieningen De wijze waarop de facilitaire voorzieningen zijn ingericht in en rond de computerzaal is een verantwoordelijkheid van de back-office van het rekencentrum. Voor de klant is alleen van belang dat er zodanige infrastructurele maatregelen zijn getroffen dat de voortgang en kwaliteit van de dienstverlening niet worden aangetast.
Eisen in de SLA betreffen:
- algemene beschikbaarheidseisen;
- algemene eisen ten aanzien van de kwaliteit van de infrastructurele voorzieningen;
- periodieke audit van het functioneren van de infrastructurele voorzieningen.

Onvoldoende opslagbeheer en afscherming van gegevens Het is voor de klant van groot belang om afspraken te maken over de wijze waarop met zijn gegevensbestanden wordt omgegaan. De beveiligingseisen zijn hier primair gericht op de exclusiviteit en in mindere mate de integriteit van de gebruikersgegevens. Zoals bij de beveiliging tegen inbraak is gesteld, zal van de leverancier geëist moeten worden dat zowel binnen de verwerkingsorganisatie als voor de afscherming van de applicatie gebruik wordt gemaakt van een afdoende systeem van logische toegangsbeveiliging. De deugdelijkheid van een dergelijk systeem dient jaarlijks door een deskundige en onafhankelijke auditor te worden gecontroleerd.
Aan de opslag en verwerking van de gebruikersgegevens kunnen

door de klant aanvullende eisen gesteld worden, bijvoorbeeld ten aanzien van de wijze van bewaren, de bewaartermijn en de wijze van vernietiging. Eventueel kunnen voor bijzonder vertrouwelijke of privacygevoelige gegevens aanvullende afspraken worden gemaakt.
Eisen in de SLA betreffen:
- integraal systeem van logische beveiliging;
- rapportage van inbreuken;
- periodieke audit van de logische toegangsbeveiliging;
- classificatie van gegevens;
- bewaartermijnen;
- migratieprocedures;
- vernietigingsprocedure.

Onvoldoende borging van de beheersprocessen Om de kwaliteit van de operationele exploitatieprocessen te kunnen waarborgen en daarmee tevens de garantie te kunnen bieden dat de beveiligingsmaatregelen ook daadwerkelijk functioneren, is een adequate beheersorganisatie noodzakelijk. De werkzaamheden binnen de beheersorganisatie zijn voor het grootste deel gericht op het intern sturen van de verwerkingsprocessen en zijn dan ook een onderdeel van de back-office. De werkzaamheden met betrekking tot de helpdesk en het service management zijn duidelijke gericht op de externe communicatie met de klant en behoren dan ook tot de front-office. Hierover zullen in de SLA dan ook afspraken gemaakt moeten worden.
Een belangrijke taak van de helpdesk is het ondersteunen van de gebruikers en het registreren van incidenten. Bij het formuleren van de beveiligingseisen spelen beschikbaarheid en deskundigheid van de helpdesk-werkzaamheden dan ook een grote rol.
Het service management verzorgt alle verdere contacten tussen klant en leverancier. Verzoeken van de klant worden of zelf afgehandeld of doorgesluisd naar de juiste instanties binnen de back-office. Tevens controleert het service management of de afgesproken service levels ook daadwerkelijk gehaald worden, het zogenaamde service level management.
Eisen in de SLA betreffen:
- algemene structuur en kwaliteit van de beheersorganisatie;
- periodieke audit van het functioneren van de beheersorganisatie;
- beschikbaarheid van de helpdesk;
- reikwijdte en deskundigheid van de helpdesk;
- afhandeling incidenten;
- afhandeling calamiteiten;
- rapportage van werkzaamheden van de helpdesk;
- procedures voor service management;
- rapportage van werkzaamheden service management;

– controle van toegezegde Service Levels;
– rapportage over kwaliteit van de dienstverlening.

Onvoldoende autorisatiebeheer Om na de uitbesteding het bestaande beveiligingsniveau te kunnen handhaven, is het noodzakelijk dat ook bij de leverancier een deugdelijk systeem van logische toegangsbeveiliging is geïmplementeerd. Een dergelijk systeem zal niet alleen bescherming moeten bieden aan de technische systemen binnen het rekencentrum, maar ook aan de applicatie van de gebruiker die nu binnen het rekencentrum functioneert. Daarbij valt het uit het oogpunt van efficiëntie te overwegen om een onderverdeling te maken naar verschillende beveiligingsniveaus, een zogenaamde classificatie.
Het autorisatiebeheer zorgt ervoor dat dit systeem optimaal functioneert door de initiële instellingen te bewaken, de autorisaties voortdurend te actualiseren en eventuele inbreuken direct te signaleren. Het autorisatiebeheer is weliswaar een volledig back-officeproces, maar de klant heeft hierop een aanzienlijke invloed.
Eisen in de SLA betreffen:
– algemene kwaliteit van de logische beveiliging;
– periodieke audit van de kwaliteit van de logische beveiliging;
– classificatie;
– beheren van user-id's en wachtwoorden;
– controleren en actualiseren van autorisaties;
– rapporteren van inbreuken.

Onvoldoende scheiding tussen ontwikkel-, test- en productieomgeving Het aanbrengen van scheiding tussen ontwikkel-, test- en productieomgeving is primair bedoeld om in ieder geval de productieomgeving zo veel mogelijk te isoleren van verstorende externe invloeden. Door middel van een deugdelijk change management en autorisatiebeheer kan deze scheiding verder in stand worden gehouden. Deze werkzaamheden gebeuren volledig in de back-office.
Eisen in de SLA betreffen:
– algemene kwaliteit infrastructuur;
– periodieke audit van de kwaliteit van de infrastructuur.

4 Uitbesteding van netwerkprocessen

Netwerken zijn meer dan alleen de verbinding tussen verschillende automatiseringscomponenten. Netwerken vormen steeds meer een integraal geheel met een groot aantal samenwerkende systemen en omgevingen. Het vervagen van de grenzen van het netwerk heeft tot gevolg dat het steeds moeilijker wordt om de taken en verantwoordelijkheden rond het gebruik en beheer van het netwerk eenduidig vast te stellen. Het diffuser wordende karakter van netwerken heeft tevens tot gevolg dat het nauwelijks meer mogelijk is om tot een sluitende definitie te komen voor het ICT-object netwerken.

4.1 OVERZICHT VAN NETWERKDIENSTEN

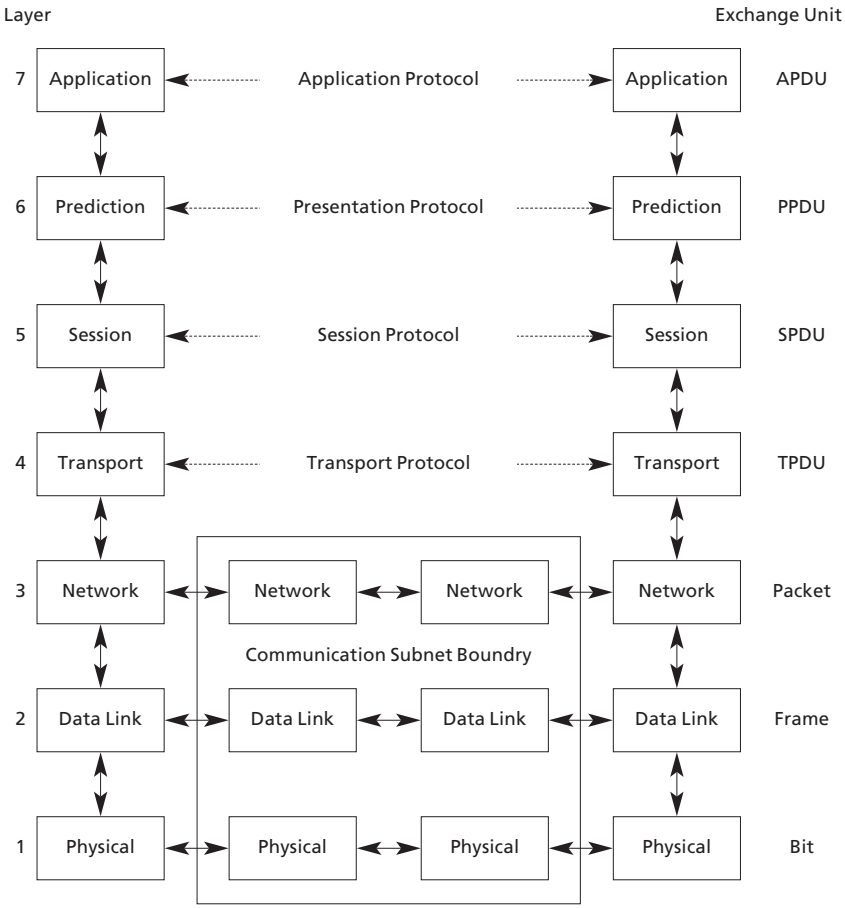
Bij de beschrijving van het ICT-object netwerkdiensten kan het best gebruikgemaakt worden van het algemeen aanvaarde OSI-referentiemodel, dat eind jaren zeventig tot stand kwam onder leiding van de International Organization for Standardization (ISO). Doel was om een internationaal erkend standaard netwerkprotocol te ontwikkelen en daarmee de wereldwijde (inter)connectie van netwerken mogelijk te maken. Het OSI-model (zie figuur 6) is opgebouwd uit zeven lagen:

- De physical layer (laag 1) bestaat uit de bekabeling en heeft ten doel het transport van de elektronische (of optische) pulsen te verzorgen. Op dit niveau zijn van belang: de soort kabel (UTP, fiber, coax), de netwerktopologie (star, ring, bus) en de soort transmissie (multiplexing en analoog/digitaaltransmissie).
- De datalink layer (laag 2) groepeert data in packets en zorgt voor de aansturing van de fysieke laag. In sommige gevallen vindt ook controle plaats op fouten in de verzending. Op dit niveau is vooral van belang of gebruikgemaakt wordt van een token ring of ethernet-netwerk.
- De network layer (laag 3) verzorgt de routering en adressering van de packets uit de datalink layer. Samen met de onderste twee lagen wordt het gehele feitelijke datatransport verzorgd. Bekende netwerkprotocollen zijn onder meer IP en IPX.
- De transport layer (laag 4) groepeert de ontvangen packets en

controleert of de ontvangen data volledig zijn en in de juiste volgorde staan. Eventueel kan de network layer om hernieuwde verzending verzoeken. Bekende transportprotocollen zijn onder meer TCP, NetBIOS/ NetBEUI en ATP.

– De session layer (laag 5) voert de regie bij het contact met andere netwerkcomponenten door het opzetten en onderhouden van een zogenaamde sessie. Deze laag voert controles uit en zet periodiek checkpoints ten behoeve van een eventuele recovery.
– De presentation layer (laag 6) wordt gebruikt voor de encryptie en de compressie van data. Dit onderdeel van de OSI-architectuur wordt niet in alle gevallen toegepast.

FIGUUR 6



Het OSI-model.

– De application layer (laag 7) vormt de directe verbinding met de gebruikersapplicaties. In deze laag worden de binnengekomen data ontdaan van alle tijdens de verzending toegevoegde routerings- en controle-informatie. Bekende protocollen zijn onder meer e-mail, FTP, Telnet en Finger.

Het OSI-model heeft vooral een theoretische betekenis. Met name de vanwege internet sterk opkomende TCP/IP-protocollen bleken moeilijk in het OSI-model inpasbaar. Desondanks is het model zeer bruikbaar als denkmodel. Maar door het samenvoegen van de verschillende lagen tot zogenaamde diensten die via het netwerk worden verleend, kan het OSI-model ook tot een praktisch bruikbaar model worden omgevormd. De volgende diensten kunnen daarbij onderscheiden worden:

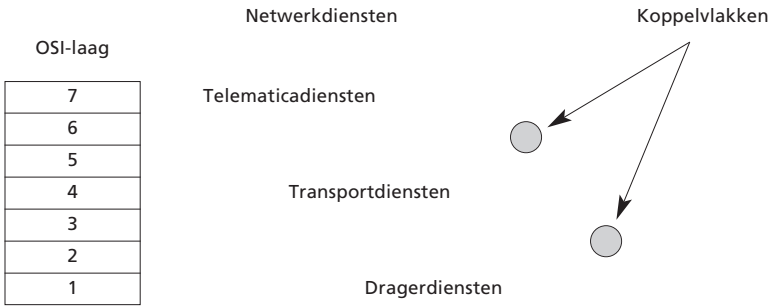
DRAGERDIENSTEN Het verzorgen van voldoende transmissiebandbreedte tussen twee punten op het netwerk. Dragerdiensten omvatten de eerste en tweede laag van het OSI model. Deze dienstverlening, die vooral een fysiek en infrastructureel karakter heeft, is vooral van belang bij netwerken die een grote afstand moeten overbruggen of waarover een intensief netwerkverkeer plaatsvindt. Te denken valt aan huurlijnen, frame-relay-koppelingen, ATM, SDH-transmissiecapaciteit. In het algemeen bieden de aanbieders van dragerdiensten naar keus een bepaalde bandbreedte aan waarover het de afnemer vrijstaat protocol-onafhankelijk informatie te versturen.

TRANSPORTDIENSTEN Het daadwerkelijk transporteren van informatie tussen twee of meer punten op het netwerk. De transportdiensten omvatten de derde en vierde laag van het OSI-model. Deze dienstverlening is gericht op de softwarematige netwerkbesturing van de gegevensstromen op het netwerk. Te denken valt aan TCP/IP-koppelingen, LAN-koppelingen en X.25-koppelingen (hoewel deze slechts aangrijpen op OSI-laag 3). Ook MPOA-of LANE-protocollen vallen hieronder, omdat deze immers zorgen voor de mogelijkheid om TCP/IP-protocollen te gebruiken over ATM. Ten slotte kan ook gedacht worden aan spraakdiensten zoals telefonie.

TELEMATICADIENSTEN Het aanbieden van toepassingen aan gebruikers waarbij het transport van gegevens over het netwerk noodzakelijk is. Transportdiensten omvatten de bovenste drie lagen van het OSI-model. Deze dienstverlening zorgt voor de specifieke functionaliteit die binnen de netwerkomgeving aan de gebruikers beschikbaar gesteld kan worden. Te denken valt aan bestandsoverdracht, koppelen van asynchrone terminals aan X.25-diensten (pad dienstverlening), e-mail, EDI, gateway-dienstverlening, video conferencing, databasekoppelingen, spraak (telefonie), PABX-koppelingen, enzovoort.

De verschillende diensten hebben elk een eigen karakter. Niet alleen ten aanzien van gebruik en beheer, maar ook ten aanzien van beveiligingsaspecten ligt het in de praktijk voor de hand om een onderscheid te maken in drager-, transport- en telematicadiensten. Het grensvlak tussen twee verschillende diensten wordt koppelvlak genoemd (zie figuur 7).

FIGUUR 7



Koppelvlakken.

De koppelvlakken vormen vaak een punt van discussie. Zeker wanneer de verantwoordelijkheid voor gebruik en beheer van de diensten over verschillende partijen is verdeeld, zal op de koppelvlakken een naadloze aansluiting moeten bestaan. Er mogen geen overlappingen of lacunes ontstaan. Met name het stelsel van beveiligingsmaatregelen dat rond het netwerk is ingericht, zal een consequent en sluitend geheel moeten vormen.
Om de koppelvlakken zo duidelijk mogelijk vast te leggen, wordt in de praktijk zo veel mogelijk aansluiting zocht bij een fysieke representatie. Het koppelvlak tussen telematica- en transportdiensten wordt gevormd door de wandcontactdoos in de kantoorruimten. De achterliggende bekabeling, hubs, switches, repeaters en dergelijke behoren tot de transportdiensten, terwijl de software voor het opzetten van de sessie en de toepassingssoftware voor bijvoorbeeld e-mail of encryptie op de individuele pc's zijn geïmplementeerd. De tussenliggende transportdiensten vormen deelgebieden in het geheel van dragerdiensten. Deze zijn opgebouwd uit fysieke componenten ,zoals routers, gateways of ATM-switches en worden aangestuurd door onder meer TCP/IP-protocollen.

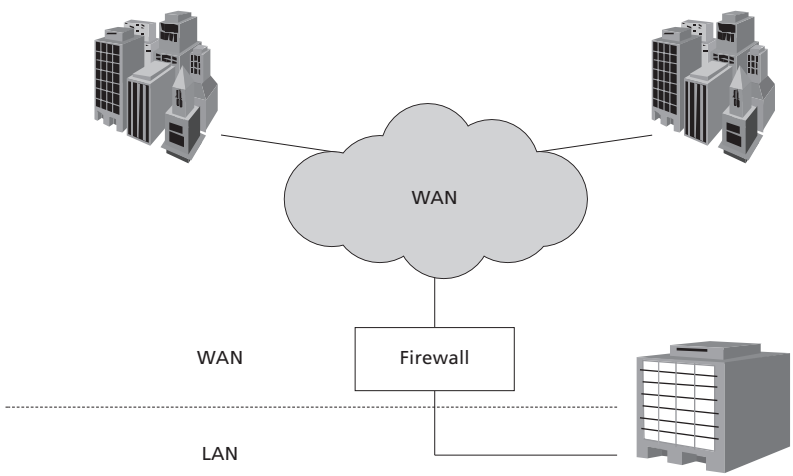
WAN en LAN Er bestaat een duidelijk verschil tussen zogenaamde Local Area Networks (LAN's) en Wide Area Networks (WAN's). Het LAN-netwerk omvat slechts een geografisch beperkt gebied, zodat de gehele dienstverlening rond het LAN-netwerk steeds plaatsvindt op de locatie en onder verantwoordelijkheid van de eigenaar van het netwerk. Het WAN-netwerk strekt zich over een fysiek veel groter gebied uit, waardoor vrijwel altijd van de dienstverlening van een derde partij gebruikgemaakt moet worden. Vaak betreft het voor derden toegankelijke netwerkonderdelen en steeds vaker ook openbaar toegankelijke netwerkonderdelen.
De dienstverlening van het WAN-netwerk is primair gericht op het beschikbaar stellen van dragerdiensten. Deze diensten zijn bij LAN-netwerken relatief minder belangrijk; hier ligt de nadruk juist op het verlenen van transport- en telematicadiensten. Zie ook tabel 1.

TABEL 1

Type dienstverlening	LAN	WAN
Telematicadienst	++	+/-
Transportdienst	++	+/-
Dragerdienst	+	++

Dienstverlening op WAN- en LAN-netwerken.

FIGUUR 8



Scheiding tussen LAN en WAN.

Uiteraard zijn de beveiligingseisen bij het gebruik en beheer van LAN-netwerken van een andere orde dan bij WAN-netwerken. Zo zal vertrouwelijke informatie over een (semi- of geheel openbaar) WAN-netwerk alleen versleuteld uitgewisseld mogen worden. Ook de aansluiting op een WAN-netwerk zal bijvoorbeeld door een speciale firewall extra beveiligd moeten worden. De overgang van het WAN-netwerk naar het LAN-netwerk vormt ook een koppelpunt (zie figuur 8).
De scheiding tussen het LAN en het WAN wordt in stand gehouden door een firewall. Er dient duidelijk afgesproken te worden of de firewall geheel of gedeeltelijk deel uitmaakt van de beheersorganisatie van het WAN- of het LAN-netwerk. Deze keuze is onder meer afhankelijk van de eisen die voortvloeien uit het informatiebeveiligingsbeleid.
Doorgaans is het functioneren van een LAN niet afhankelijk van een firewall. Zodra er WAN-dienstverlening wordt geboden, is bescherming van het LAN noodzakelijk. Zo geredeneerd behoort een firewall dus bij het WAN-domein. LAN-segmenten waarvoor verschillende beveiligingseisen gelden, worden doorgaans ook door middel van een firewall gekoppeld. Deze firewall-koppelingen behoren daarmee wel tot het LAN-beheersdomein.

4.2 INBRAAK

Inbraak op of gebruikmakend van netwerken is een dreiging waarover veel te doen is, zeker in het licht van internet (zie ook [Van Dam]). Onder inbraak vallen de volgende verschijnselen:
- Inbraak (zowel in- als extern), het daadwerkelijk zich ongeoorloofd toegang verschaffen tot een netwerk of delen daarvan.
- Afluisteren, een verschijnsel dat specifiek is voor netwerkbeveiliging en bij andere ICT-objecten niet voorkomt. Hoewel afluisteren van een verbinding niet als bedreiging in de Code voor Informatiebeveiliging staat vermeld, is dit toch een dreiging die voor kan komen. De benodigde middelen zijn niet duur en softwareprogramma's die afluisteren vanaf een gewone pc mogelijk maken, zijn eenvoudig toegankelijk.

Het grote verschil tussen afluisteren van een verbinding en inbraak op een netwerk is dat het eerste passief gebeurt. De schade blijft daarbij beperkt tot de informatie die bij niet-geautoriseerde personen bekend wordt. Inbraak gaat veel verder. Hier worden actief netwerkverbindingen gebruikt om:
- informatie te achterhalen op computers;

– te verhinderen dat verbindingen tot stand komen (denial of service attacks);
– misleidende informatie te verspreiden;
– informatie te corrumperen (aantasting van de integriteit), zowel informatie die wordt verzonden over het netwerk als informatie die in computers staat opgeslagen;
– virussen te verspreiden.

Wanneer bijvoorbeeld een dienst als e-mail wordt aangeboden, worden er vaak tijdelijk berichten op machines in het domein van de aanbieder opgeslagen. Deze berichten kunnen dan bekeken worden door onbevoegden. Dit is een geval van inbraak. Een e-mailserver is in beginsel gelijk aan een gewone server, maar met een bepaalde taak, namelijk het verzorgen van e-mailverkeer. Hiermee komt het apparaat in het domein van LAN/WAN dienstverlening. Tevens kunnen de instellingen van het netwerk worden gewijzigd door middel van inbraak, waardoor de continuïteit ernstig in gevaar kan komen.

Er bestaan verschillende instrumenten om inbraak (en afluisteren) tegen te gaan. Binnen een LAN kan gebruikgemaakt worden van een vaste beveiligde route, een netwerksegment waarbinnen het netwerkverkeer blijft, dat bij voorkeur niet toegankelijk is voor anderen. Een vaste beveiligde route houdt in het geval van WAN-diensten doorgaans in dat men geen gebruikmaakt van de openbare infrastructuur maar van vaste verbindingen waarvan de leverancier waarborgt dat deze niet gedeeld worden met anderen.
Onder PKI wordt een Public Key Infrastructuur verstaan. Dit omvat ook het gebruik van speciale protocollen ten behoeve van bancaire transacties (RSI met zeer grote vercijferingsleutels) en SET, PGP voor e-mail, enzovoort (zie [Damen]).

4.2.1 Normen en maatregelen

De normen voor goede beveiliging van netwerken tegen inbraak zijn weergegeven in tabel 2.

TABEL 2

Classificatie	Dragerdienst	Transportdienst	Telematicadienst
Ongeclassificeerd	Standaard protocol	Standaard	Standaard
Vertrouwelijk	Vaste beveiligde route	Vaste beveiligde route Speciale protocollen	Gescreend personeel
Geheim en verder	Public Key Infrastructuur (PKI)	PKI	Beperkt en gescreend personeel

Classificatie van gegevens en de bijbehorende beveiliging per dienst.

Basismaatregelen tegen inbraak zijn:
- Beveiligde routes (trusted path) worden toegepast.
- Personeel dat toegang heeft tot de netwerken wordt gescreend.

4.3 VERLIES VAN GEGEVENS

Door verstoringen kunnen gegevens tijdens het transport verloren gaan. Dit verlies van gegevens kan ertoe leiden dat de continuïteit en integriteit van de geautomatiseerde systemen in gevaar komen. De gebruikte protocollen zijn vaak wel in staat zelfstandig herstelacties uit te voeren, maar niet alle verstoringen kunnen door het protocol opgevangen worden. Bij totale uitval van het netwerk kunnen ongewenste situaties ontstaan. Wat moet er bijvoorbeeld gebeuren als halverwege een financiële transactie het netwerk uitvalt:moet de transactie bij herstel van de verbinding nog één maal worden verstuurd of juist niet meer of op aanvraag? Dit dilemma is slechts door goede afspraken op te lossen. Het netwerk speelt hierin een ondergeschikte rol.
Ook kan door een kwalitatief slechte verbinding (er moeten dan veel herstelacties worden uitgevoerd, waardoor de effectieve snelheid van het netwerk lager wordt) de performance van de netwerkdienstverlening sterk verminderen, waardoor gebruikers bijvoorbeeld een tragere responstijd ervaren.

4.3.1 Normen en maatregelen

Als normen gelden:
- Er treedt geen verlies van gegevens op.
- Hoewel er technische normen bestaan waarover afspraken te maken zijn, is het aan te bevelen de afspraken zodanig te maken dat beide partijen de inhoud ervan precies begrijpen.

Basismaatregelen zijn:
- Robuuste communicatieprotocollen zijn in gebruik.
- Daar waar aanvullende zekerheid nodig is, dient op applicatieniveau controle plaats te vinden op de betrouwbaarheid van de gegevensoverdracht.

4.4 TERUGLOPEN VAN DE TRANSPORTSNELHEID

De transportsnelheid of doorvoersnelheid van een netwerk kan door verschillende oorzaken teruglopen. De gebruiker kan dit merken aan de volgende gebeurtenissen:

– Er is minder respons van toepassingen, zoals terminals van mainframes die op afstand staan, terminal-emulatiepakketten, client/server-systemen.
– Het kan langer duren voor bestanden zijn overgedragen.
– Het kan langer duren voor transacties zijn geslaagd.
– Het kan zelfs voorkomen dat toepassingen zich afsluiten, als de netwerkcapaciteit onder een bepaalde waarde is gedaald.

De oorzaken van dit teruglopen van de transportsnelheid kunnen liggen in de belasting van het netwerk, uitval van (delen van) het netwerk, storing in de netwerkapparatuur of aanvallen van buiten (de zogenaamde denial-of-service aanvallen).
Naarmate de belasting van het netwerk toeneemt, kan de totale doorvoersnelheid van het netwerk teruglopen. Indien het netwerk goed beheerd wordt, ziet de netwerkbeheerder deze belasting oplopen en zal hij de klant tijdig informeren over een op handen zijnde daling van de performance van het netwerk (zie ook paragraaf 4.6: Capaciteitsbeheer). De klant kan er dan voor kiezen:
– het netwerk minder te belasten door het vermijden van piekgebruik;
– het netwerk minder te belasten door enkele toepassingen in de tijd te spreiden (bijvoorbeeld batches 's nachts te laten draaien);
– de capaciteit van het netwerk te laten verhogen.

4.4.1 Normen en maatregelen

Normering van deze service wordt als volgt aanbevolen:
– Zodra de gemiddelde belasting van een netwerk groter is dan veertig procent dient de klant daarover gerapporteerd te worden.
– Bij een gemiddelde belasting van het netwerk die groter is dan zestig procent, waarbij pieken boven de tachtig procent voorkomen, dient de klant daarover gerapporteerd worden.
– In geval van het incidenteel teruglopen van de transportsnelheid van het netwerk dient de klant hierover gerapporteerd te worden en dienen er afspraken gemaakt te worden over een zekere prioriteitstelling in het verkeer.

Om deze keuzes adequaat te maken zijn goede afspraken met de leverancier nodig over de wijze van rapporteren over de netwerkbelasting. Bij wijze van basismaatregelen moeten de volgende zaken geregeld worden:
– Er worden rapportages gemaakt over:
– het netwerkgebruik van afzonderlijke toepassingen;
– LAN- dan wel WAN-gebruik;

– aanbevelingen vanuit de leverancier.
– Er bestaan afspraken over drempelwaarden waarboven onverwijld rapportage wordt gevraagd.
– Er is een prioriteitstelling bij aanbod van verschillende te onderscheiden gegevensstromen.

4.5 ONVOLDOENDE CONFIGURATIEBEHEER EN KABELBEHEER

Het nauwgezet registreren van alle configuratie-items en hun onderlinge samenhang is essentieel voor een adequaat netwerkbeheer. Het is van belang de juiste kenmerken van alle apparatuur en verbindingen te registreren, zodat de beheerstaken goed uitgevoerd kunnen worden. Incidentbeheer is vrijwel onmogelijk zonder een goede configuratiedatabase. Bij het melden van een incident, in het bijzonder een beveiligingsincident, dient snel duidelijk te zijn wat er kan worden gedaan om de storing te beperken, wat de invloed is van een storing in het netwerk, wat de uitwijkroutes zijn, wat de invloed is op de performance, enzovoort. Een adequate configuratiedatabase is hiervoor noodzakelijk.

Het gebruik van bekabeling is typerend voor netwerken. Goede registratie hiervan, eigenlijk deel uitmakend van configuratiebeheer, is een voorwaarde om een netwerk adequaat te kunnen beheren. Het beveiligingsaspect van een goed kabelbeheer kan worden geïllustreerd door het feit dat kabels eigenschappen hebben die mede bepalend kunnen zijn voor het al dan niet geschikt zijn voor het transport van gegevens van een bepaald classificatieniveau. Denk daarbij aan de mate waarin afluisteren mogelijk is, het feit of bekabeling over niet-beveiligde ruimten of openbare wegen is gelegd, enzovoort.

4.5.1 Normen en maatregelen

Als normen gelden:
– De configuratiedatabase is van voldoende kwaliteit om de gevraagde beheerstaken te kunnen uitvoeren.
– Er kan van voldoende kabelbeheer gesproken worden als van alle aanwezige bekabeling de beveiligingeigenschappen adequaat zijn geregistreerd.

Als belangrijke basismaatregelen tegen onvoldoende configuratiebeheer kunnen worden genoemd:
– Er is een goede set beheersgereedschappen gekozen, waarin de geregistreerde elementen en hun onderlinge samenhang op een

inzichtelijke wijze kunnen worden beheerd. Het verdient aanbeveling regelmatig met behulp van 'discovery' tools te controleren welke netwerkcomponenten er aanwezig zijn.
- Er wordt zo veel mogelijk gebruikgemaakt van standaard beheersprotocollen om on line beheer van de componenten te kunnen uitvoeren. Protocollen die daarvoor in aanmerking komen, zijn SNMP (I en II) en CMIP.
- Een standaard componentindeling, zoals gedefinieerd in het TMN-model, is in gebruik.
- Licentiebeheer is geregeld. Dit is een vaak onderschat element, met name door de niet-uniforme wijze van opstellen van licentieovereenkomsten van de diverse leveranciers.
- De gehele levenscyclus, dus ook het afstoten van apparatuur en dergelijke, moet in beschouwing genomen worden.

Als belangrijke basismaatregelen tegen onvoldoende kabelbeheer kunnen worden genoemd:
- Van alle bekabeling moet een registratie van het type aangelegd worden (glas, koper volgens de standaard normering ISO Standaard bekabelingstructuur: ISO/IEC IS 50173).
- Alle bekabeling moet volgens een gecertificeerd systeem zijn aangelegd.

4.6 ONVOLDOENDE CAPACITEITSBEHEER

De capaciteit van het netwerk wordt bepaald door zowel de passieve componenten (bekabeling) als de actieve componenten. Hoewel een lijnverbinding snel kan zijn, bepaalt de apparatuur die de daadwerkelijke informatie daaroverheen verstuurt de communicatiesnelheid. Dit is te illustreren aan de hand van een telefoonaansluiting, waarover met de huidige stand van de techniek een snelheid van 8 Mbps mogelijk is. Het hangt dan van het modem af of deze snelheid ook gebruikt wordt.
Capaciteitsbeheer is daarmee meer dan alleen het bijhouden van de capaciteit van de diverse te onderscheiden elementen. Ook het geheel moet in beschouwing worden genomen, evenals de kosten die het leveren van de capaciteit met zich meebrengt. Teneinde goed capaciteitsbeheer te kunnen uitvoeren is veel en complexe informatie nodig.

4.6.1 Normen en maatregelen

De norm voor goed capaciteitsbeheer is:
- Het capaciteitsbeheer is zodanig geregeld dat de gevraagde

serviceniveaus gehaald en onderhouden kunnen worden tegen aanvaardbare kosten.

Als belangrijke basismaatregelen tegen onvoldoende capaciteitsbeheer kunnen worden genoemd:
- Er wordt goed netwerkbeheergereedschap gebruikt. Het is echter de kunst van alle componenten de goede parameters vast te leggen; met name het detailniveau is van wezenlijk belang. Ook de vertraging (latency) die iedere actieve netwerkcomponent introduceert is een belangrijke parameter die de totale capaciteit van het netwerk relevant kan beïnvloeden.
- Op mogelijke groei van de capaciteitsvraag wordt geanticipeerd.
- De specifieke capaciteitsbehoefte is per systeem vastgelegd.

4.7 ONVOLDOENDE WIJZIGINGSBEHEER

Wijzigingen in de configuratie van netwerken dienen uiterst zorgvuldig te worden uitgevoerd. Het geheel aan apparatuur en bekabeling dat tezamen een netwerk vormt, vereist een zorgvuldige instelling en configuratie van parameters, die vaak een complexe samenhang hebben, zeker daar waar het beveiligingsparameters betreft. Wijzigingen op dit geheel dienen volgens een goed uitgewerkt standaard plan te geschieden om verstoringen tot een minimum te beperken.

4.7.1 Normen en maatregelen

De norm voor goed wijzigingsbeheer is:
- Het vastgestelde beveiligingsniveau van een netwerk wordt niet nadelig beïnvloed door wijzigingen op het netwerk.

Basismaatregelen zijn:
- Een wijziging op een netwerk dient bij voorkeur op onderstaande wijze te geschieden:
- Stel vast, door test of simulatie, hoe een voorgenomen wijziging in de praktijk werkt.
- Stel vast, door inschakeling van deskundigen, dat de voorgenomen wijziging het vereiste beveiligingsniveau niet nadelig beïnvloedt.
- Documenteer en registreer de wijziging zorgvuldig.
- Maak een back-outplan dat voorziet in het teruggaan naar de oude situatie bij het ontdekken van storingen nadat de wijziging is geëffectueerd.
- Bepaal welke gegevens moeten worden gemonitord ter bepaling

van het correct functioneren van het netwerk en leg daar registraties van aan.
- De voortgang van de afhandeling van wijzigingsverzoeken wordt bewaakt.
- Zeker kort na de implementatie van een wijziging wordt de acceptatie van de wijziging door de netwerkbeheerder en de gebruiker bewaakt.
- Een onafhankelijke partij controleert periodiek het beveiligingsniveau, zodat kan worden vastgesteld of het gewenste niveau nog steeds wordt gehaald.

4.8 AANDACHTSPUNTEN IN DE SLA

De kwaliteit van de netwerkdiensten die de leverancier aan de klant levert, wordt in beginsel door twee elementen bepaald. Enerzijds de wijze waarop de leverancier zijn interne processen beheerst en daarmee de kwaliteit van het geleverde product kan bepalen, anderzijds de wijze waarop de leverancier met de klant communiceert en daardoor in staat is aan de wensen van de klant te voldoen. Een belangrijke exponent waarmee deze tweedeling wordt geconcretiseerd is het onderscheid tussen front- en back-officeprocessen. Bij de invulling van de baseline-beveiligingsafspraken in de SLA is het onderscheid in front-en back-officeprocessen zeer bruikbaar. In de SLA zal aan beide soorten processen zeker aandacht gegeven moeten worden, maar de wijze waarop zal sterk verschillen.
Voor front-officeprocessen, zoals de ondersteuning door de helpdesk, zullen gedetailleerde afspraken gemaakt moeten worden omtrent de kwaliteit van de dienstverlening, vertaald in bijvoorbeeld openstellingstijden, reactietijden, oplospercentages, enzovoort.
De back-officeprocessen behoren veel meer tot de verantwoordelijk van de leverancier. De klant kan bij deze processen in principe volstaan met het opstellen van algemeen geformuleerde normen. Op welke wijze bijvoorbeeld het probleembeheer is ingericht, is voor de klant niet van essentieel belang, wel dat de problemen (van een bepaalde categorie) binnen een bepaalde tijd worden opgelost. Of de leverancier voor het oplossen van het probleem eigen specialisten inschakelt, daarvoor gebruikmaakt van externen of misschien wel moet uitwijken naar een ander systeem, is voor de klant niet van doorslaggevend belang. Het belangrijkste is dat de in de SLA afgesproken continuïteitsnorm wordt gehandhaafd.
Uit het oogpunt van kwaliteitsborging is het van belang dat er in de SLA niet alleen beveiligingsnormen worden vastgelegd, maar ook dat deze normen worden gecontroleerd. De leverancier zal door

middel van rapportage moeten aantonen dat de in de SLA gemaakte afspraken ook zijn nagekomen. Zeker bij front-officeprocessen zal dit een effectief controlemiddel zijn. Voor back-officeprocessen, die minder zichtbaar zijn voor de klant, is het aan te bevelen om periodiek een onafhankelijke controle bij de leverancier uit te voeren naar de kwaliteit hiervan. In de praktijk wordt hierin door de leverancier voorzien, door jaarlijks aan een onafhankelijke EDP-auditor te vragen een zogenaamde third party-mededeling af te geven.

In de voorgaande paragrafen is een overzicht gegeven van de belangrijkste bedreigingen die zich kunnen voordoen bij de netwerkdienstverlening, alsmede enkele van de belangrijkste maatregelen om deze bedreigingen te compenseren. De klant zal steeds een afweging moeten maken tussen enerzijds de bestaande bedreigingen en anderzijds het gewenste beveiligingsniveau. In de SLA worden de bij het gewenste beveiligingsniveau horende normen nader uitgewerkt en vastgelegd. Hierbij dient nog te worden opgemerkt dat de leverancier vaak zelf al een intern baseline-beveiligingsniveau hanteert, waaraan ook de klant minimaal zal moeten voldoen.
Een belangrijke toegevoegde waarde van de SLA voor de klant is dat de waarschijnlijk al bestaande beveiligingsnormen nu duidelijk zichtbaar worden gemaakt. Door in het kader van de SLA te onderhandelen krijgt de klant tevens een goed inzicht in de baseline-beveiligingsnormen van de leverancier. Ten slotte is de SLA door het opnemen van duidelijke beveiligingsnormen en rapportageverplichtingen een goed controle-instrument voor zowel de klant als de leverancier.

Inbraak Het ongeoorloofd netwerkgebruik door derden wordt voorkomen door in de SLA normen op te nemen voor zowel de fysieke als de logische toegangsbeveiliging van de netwerkdienstverlening door de leverancier. Omdat dit in belangrijke mate back-officeprocessen zijn, zal de leverancier hiervoor nadere maatregelen moeten treffen, bijvoorbeeld door de implementatie en het beheer van een integraal systeem van toegangsbeveiliging. Om ook het ongeoorloofd netwerkgebruik binnen de organisatie van de leverancier af te dekken, kan de klant volstaan met het in de SLA opnemen van een algemene norm inzake de integriteit en deskundigheid van het personeel van de leverancier. Deze zal door bijvoorbeeld nadere opleiding, toezicht en boetebedingen hieraan zelf verdere invulling moeten geven.
Een belangrijk punt is dat ongeoorloofd gebruik, of pogingen daartoe, aan de klant wordt gemeld. Omdat netwerkbeveiliging een complex en dynamisch geheel is, zal er tussen klant en leverancier regelmatig overleg en afstemming moeten plaatsvinden, eventueel

ondersteund door externe deskundigen. In ieder geval zal de leverancier jaarlijks een zogenaamde third party-mededeling moeten kunnen overleggen.
Eisen in de SLA betreffen:
- algemene eisen ten aanzien van de fysieke toegangsbeveiliging;
- periodieke audit van de fysieke toegangsbeveiliging;
- algemene eisen ten aanzien van de logische toegangsbeveiliging;
- periodieke audit van de logische toegangsbeveiliging;
- rapportage van ernstige inbreuk.

Verlies van gegevens De klant zal in de SLA duidelijke normen opstellen voor de netwerkomgeving ten aanzien van de veilige verwerking van de klantgegevens. De integriteit van de klantgegevens zal tijdens het transport en de opslag zo veel mogelijk onaangetast dienen te blijven. In de praktijk is gebleken dat een hoge mate van beveiliging zeer goed haalbaar is. Een volledige garantie op dit punt is echter vrijwel onmogelijk en in ieder geval zeer kostbaar.
De handhaving van de netwerkintegriteit door middel van technische en organisatorische maatregelen is voornamelijk een back-officeproces. De klant kan in principe volstaan met het formuleren van een algemene integriteitnorm en de controle ervan door middel van rapportage en periodiek onafhankelijk onderzoek. Belangrijke inbreuken op de integriteit, zoals inbeuk door derden, verlies van gegevens, foutieve verzendingen en uitvallen van het interne controlesysteem, zullen direct bij de klant gemeld moeten worden.
Eisen in de SLA betreffen:
- algemene eisen ten aanzien van de wijze van transport van gegevens;
- afspraken over de verwijdering van gegevens;
- periodieke rapportage over het opvolgen van integriteitnormen;
- periodieke audit van het integriteitsysteem bij de leverancier;
- rapportage van ernstige inbreuken op de integriteit.

Teruglopen van de transportsnelheid Het is voor de klant van groot belang dat de continuïteit van de operationele netwerkprocessen is gewaarborgd. In de SLA zullen dan ook duidelijke normen opgesteld moeten worden voor de minimale beschikbaarheid en de verwerkingssnelheid van de netwerkdienstverlening. De technische en organisatorische maatregelen die hiervoor genoemd moeten worden, liggen met name in de back-office, zodat het volstaat om in de SLA een aantal algemene normen op te nemen. Zo zullen eisen geformuleerd moeten worden ten aanzien van de beschikbaarheid, de snelheid en de capaciteit van de netwerkverbinding. Ten aanzien van de controle van deze normen zal de leverancier regelmatig rapportage moeten

opleveren en jaarlijks een audit moeten laten uitvoeren van de wijze waarop deze normen binnen de organisatie van de leverancier zijn gewaarborgd.
Eisen in de SLA betreffen:
- beschikbaarheid van netwerkdiensten;
- snelheid van netwerkverbindingen;
- capaciteit van de netwerkverbindingen;
- piekbeheersing;
- periodieke rapportages;
- jaarlijkse audit.

Onvoldoende configuratiebeheer De geografische omvang van het netwerk gekoppeld aan de vaak snelle groei en verandering daarvan, leidt er toe dat het vaak moeilijk is om te kunnen bepalen welke componenten er op welk moment op welke plaats in gebruik zijn. Voor een effectieve dienstverlening inclusief een goede ondersteuning bij storingen is dit inzicht echter onmisbaar. Het configuratiebeheer waar al deze informatie over de verschillende netwerkcomponenten wordt bijgehouden, is dan ook een essentieel onderdeel van het netwerkbeheer.
Een actueel en eenduidig bestand met configuratie-items heeft tevens als voordeel dat exact bekend is welke onderdelen tot het netwerk behoren en welke mate van service aan de verschillende onderdelen zal worden verleend. Hiervoor is het wel noodzakelijk dat zowel klant als leverancier het eens zijn over de initiële inhoud en de wijze van onderhoud van de configuratiedatabase.
De gegevens van de configuratiedatabase vormen tevens een belangrijke input voor de andere onderdelen van de beheersorganisatie, ongeacht of deze nog door de klant worden gevoerd of aan de leverancier zijn uitbesteed.
Eisen in de SLA betreffen:
- overeenstemming over configuratie-items;
- verantwoordelijkheid voor en onderhoud van de configuratiedatabase;
- ter beschikking stellen van configuratiegegevens;
- periodieke rapportage;
- jaarlijkse audit van de kwaliteit van het configuratiemanagement.

Onvoldoende kabelbeheer De kabels vormen de fysieke verbinding tussen de netwerkcomponenten en zijn daarmee een essentieel onderdeel van het netwerk. Een netwerk van enige omvang bevat een grote hoeveelheid kabels, stekkers en andere onderdelen, die ieder voor zich een potentieel storingsrisico vormen. De aard van deze storingen leidt vaak tot een definitieve breuk in (een deel van)

de netwerkverbindingen en is alleen door de fysieke tussenkomst van een monteur te herstellen.
Kabelbeheer vereist niet alleen een gedetailleerde kennis van de topologie van het netwerk, maar tevens middelen voor een vergaande diagnostiek om exact te bepalen waar de storing zich voordoet. Zeker voor een netwerk dat over een geografisch groter gebied is verspreid, zal een team van monteurs beschikbaar moeten zijn om binnen de verschillende regio's relatief snel ondersteuning te kunnen bieden.
Kabelbeheer speelt ook belangrijke rol bij de vervanging en uitbreiding van de fysieke netwerkinfrastructuur. Er zal steeds een afweging gemaakt moeten worden tussen de gevraagde en de te voorziene capaciteitsuitbreiding, de technische mogelijkheden en de daaraan gekoppelde investeringskosten. Uiteraard zullen ook beveiligingseisen aanleiding kunnen geven tot additionele structurele aanpassingen.
Eisen in de SLA betreffen:
- inzicht in de netwerkcomponenten;
- de topologie van het netwerk;
- de capaciteit van netwerkcomponenten;
- de snelheid van storingsondersteuning;
- periodieke rapportage;
- invloed op de uitbreidingsmogelijkheden van het netwerk.

Onvoldoende capaciteitsbeheer Binnen vrijwel elk netwerk bestaat een voortdurende behoefte aan uitbreiding van de bestaande omvang en capaciteit en aan technische verbeteringen. Binnen deze groei zal een verdeling gemaakt moeten worden naar verschillende prioriteiten: welke uitbreidingen zijn absoluut noodzakelijk, dringend gewenst of wenselijk? Gezien de aanzienlijke kosten die hiermee gemoeid zijn, zal eveneens gekeken moeten worden naar de snelheid waarmee deze veranderingen kunnen worden ingevoerd. Met behulp van de informatie uit verschillende bronnen tracht het capaciteitsmanagement te komen tot een actueel advies over de doelmatigste vervanging en uitbreiding van de netwerkcomponenten en netwerkdiensten.
Eisen in de SLA betreffen:
- verantwoordelijkheid voor het capaciteitsmanagement;
- randvoorwaarden en prioriteiten binnen het capaciteitsmanagement;
- wijze van informatie-uitwisseling met het capaciteitsmanagement;
- periodieke rapportage;
- jaarlijkse audit van de kwaliteit van het capaciteitsmanagement.

Onvoldoende wijzigingsbeheer Het wijzigingsbeheer heeft tot taak om de voortdurende verandering en groei van het netwerk op een gecontroleerde manier te laten verlopen. Allereerst worden de binnengekomen wijzigingsverzoeken geregistreerd en bewaakt. Tevens wordt een selectie gemaakt naar prioriteit en wordt een planning voor de invoering gemaakt. Op initiatief van wijzigingsbeheer worden de wijzigingen vervolgens door het serviceteam tot uitvoering gebracht. Daarbij wordt tevens nauwkeurig vastgelegd wat er in de bestaande configuratie wordt gewijzigd. Dit is niet alleen van belang om een juist en actueel inzicht in het bestaande netwerk te houden. Ook kan bij problemen die naar aanleiding van de wijziging ontstaan, relatief gemakkelijk naar de oude situatie worden teruggekeerd.
Eisen in de SLA betreffen:
- verantwoordelijkheid voor het wijzigingsbeheer;
- randvoorwaarden en prioriteiten binnen het wijzigingsbeheer;
- wijze van informatie-uitwisseling met wijzigingsbeheer;
- periodieke rapportage;
- jaarlijkse audit van de kwaliteit van het wijzigingsbeheer.

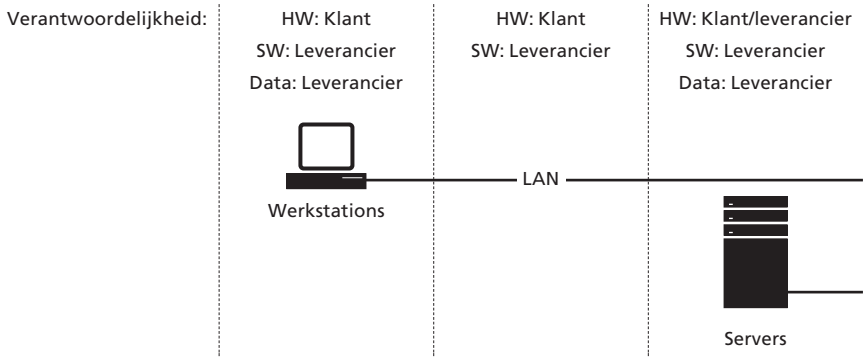
5 Uitbesteding van werkplekprocessen

Werkplekken zijn hét productiemiddel geworden van de jaren negentig. De penetratie van pc's binnen organisaties is in Europa genaderd tot tachtig procent per werkplek. In Nederland is dit percentage zelfs negentig procent. De diversiteit van de werkzaamheden is ook groter geworden. Was de pc eerst een vervanger van de typemachine, nu worden op de werkplek ook facturen gemaakt, planningen bijgehouden, managementinformatie gepresenteerd, intra- en internet informatie geraadpleegd, personeelsinformatie bijgehouden, enzovoort. De grote vlucht van ERP-systemen maakt dat men nog meer bedrijfsondersteunende en voor het primaire bedrijfsproces belangrijke zaken vanuit de werkplek bestuurt. De geautomatiseerde werkplek is daarmee een complex geheel geworden. Het onderhouden van deze werkplek wordt dan ook steeds belangrijker en duurder. Een gemiddelde werkplek kost tussen *f*. 20.000,- en *f*. 40.000,- per jaar aan onderhoud.

Het NGI hanteert de volgende definitie van een geautomatiseerde werkplek [Bautz1]: een elektronische werkplek is een plaats waar iemand gegevens verwerkt en daarbij gebruikmaakt van een pc, de daaraan aangesloten randapparatuur en de daarbij noodzakelijke infrastructuur.
Het NGI gaat ervan uit dat er drie categorieën werkplekken bestaan, namelijk de standalone-werkplek, de werkplek gekoppeld aan een netwerk en de mobiele werkplek. Voor elke categorie werkplek zijn verschillende beveiligingsmaatregelen te nemen. Bij het opstellen van een SLA dient daar rekening mee te worden gehouden. Indien van toepassing worden in de gegeven beschrijving voorbeelden aangehaald. Om het algemene karakter van deze publicatie te behouden wordt hier geen onderscheid naar de verschillende categorieën gemaakt.
Veelvoorkomende synoniemen voor de werkplek zijn: pc, thin client, netwerkcomputer en werkstation. In het vervolg van dit hoofdstuk wordt de term werkstation gehanteerd. Hiermee worden niet bedoeld de niet-intelligente terminals die uitsluitend als front-end voor mainframe-systemen functioneren. In figuur 9 staan de elementen afgebeeld die samen de werkplek vormen. Er ontstaat een

keten van diensten/producten. Elke schakel van de ketting moet in de SLA worden beschreven, en daarmee ook de beveiligingsaspecten. In grote lijnen kunnen de al beschreven diensten van netwerkprocessen en rekencentrumprocessen worden herkend als schakels van de ketting, die op de werkplek samenkomen.

FIGUUR 9



De elementen van een werkplek en bijbehorende verantwoordelijkheden.

Een werkplek bestaat niet alleen uit de werkstations op de werkplek van de gebruiker. Ook het LAN en de servers vormen een onderdeel daarvan. In dit hoofdstuk wordt echter niet ingegaan op het LAN, aangezien dit in hoofdstuk 4 reeds uitgebreid aan de orde kwam. Daarbij moet opgemerkt worden dat het bij het uitbesteden van werkplekbeheer belangrijk is om in de contracten aandacht te besteden aan de beveiligingsmaatregelen omtrent het LAN. In dit hoofdstuk worden dus uitsluitend beveiligingsmaatregelen opgenomen voor het domein van de werkstations en servers.
Werkstations zijn veelal goed toegankelijk: zij bevinden zich vaak op het bureau van werknemers, en beveiliging is daarmee een belangrijk element geworden. Dit geldt in verhoogde mate voor de portable werkstations, notebooks of laptops (palmtops en PDA's blijven buiten beschouwing). Het gebruik van portable werkstations neemt een hoge vlucht. Het wordt zo eenvoudiger personeel in de gelegenheid te stellen het werk op een andere locatie dan bij de werkgever uit te voeren, en daarmee ook thuis. Het gevaar bestaat dat het werkstation ook voor privé doeleinden gebruikt wordt. Immers: het aanschaffen van een privé-pc is duur en na drie jaar is de pc volledig verouderd. Het verdient aanbeveling het privé-gebruik van het portable werkstation te faciliteren. Het voordeel voor de werkgever is dat het

privé-gebruik van het werkstation daarmee gecontroleerd kan plaatsvinden, zodat er geen schade kan ontstaan aan de pc. Dit kan ondersteund worden door bijvoorbeeld een extra harde schijf ter beschikking te stellen die compleet geïnstalleerd wordt aangereikt en waarop men eigen programmatuur kan installeren. De werkgever eist in ruil hiervoor de discipline van de werknemer om bij privé-gebruik de harde schijf te verwisselen.

De verantwoordelijkheid voor de beschikbaarheid, integriteit en exclusiviteit van zowel de hardware, software als de gegevens ligt bij de klant. De klant voert immers de gegevens in en draagt zorg voor de inhoudelijke correctheid van deze gegevens.
In de volgende paragrafen zijn de belangrijkste elementen uit een reeks van dreigingen opgesomd. Deze elementen hebben een directe relatie met het kwaliteitsaspect continuïteit. De aangegeven basis-maatregelen zijn niet uitputtend.

5.1 DIEFSTAL

Een werkstation is gevoelig voor diefstal omdat dit vaak op een goed toegankelijke plaats staat. Diefstal is het geheel of gedeeltelijk meenemen van apparatuur, software en data door middel van onge-autoriseerde toegang tot een ruimte waarin zich deze componenten bevinden. Onderzoeken hebben aangetoond dat met name diefstal van binnenuit het meest voorkomt. Hiermee wordt zowel directe diefstal van gegevens en/of hardware bedoeld als meer indirecte diefstal: het voor derden mogelijk maken inbraken uit te voeren (openbaar maken van toegangscodes, openen van vensters, ontgren-delen van deuren, enzovoort).
Portable werkstations zijn zeer gevoelig voor diefstal. Daarvoor die-nen dan ook extra maatregelen te worden genomen. Voornamelijk zijn dit maatregelen die de klant (de gebruiker) zelf moet naleven en waarvoor de leverancier niet verantwoordelijk is, zoals het transport van een laptop. De leverancier dient wel dusdanige maatregelen te nemen dat bij verlies of diefstal van de laptop de opgeslagen gegevens en de programmatuur niet voor derden toegankelijk zijn, bijvoor-beeld door encryptie van de gegevens op de laptop. Dit moet op een zodanige wijze gebeuren dat ook bij het wegnemen van de harde schijf de gegevens hierop niet eenvoudig gebruikt kunnen worden. De leverancier is voor het samenstel van maatregelen verantwoorde-lijk, omdat deze maatregelen moeten passen in de totale dienst-verlening. De klant is verantwoordelijk voor het naleven van de gevraagde maatregelen aan de klantzijde, zoals het erop toezien dat

wachtwoorden niet openbaar worden gemaakt, het niet onnodig blootstellen van laptops aan gevaren (achterlaten in een auto, ongeoorloofd installeren van programmatuur, onbeveiligd gebruik van internet, enzovoort).
Het voorkomen van diefstal is voornamelijk de verantwoordelijkheid van de klant, aangezien (bijna) alle apparatuur op de locatie van de klant is gesitueerd. De klant dient zelf maatregelen te nemen, zoals een alarm, goedgekeurde sloten, camerabewaking, enzovoort. De leverancier is verantwoordelijk voor het beheer van de apparatuur, software en gegevens die op de locatie van de leverancier aanwezig zijn. Dit wil meestal zeggen dat de leverancier verantwoordelijk is voor het nemen van beveiligingsmaatregelen voor het beschermen van de servers. In figuur 9 zijn de verantwoordelijkheden van leverancier en klant weergegeven.

5.1.1 Normen en maatregelen

De basisnorm is:

– Er zijn afdoende logische en fysieke maatregelen genomen om inbraak en diefstal van hardware, software en data te voorkomen of tot een minimum te beperken en indien nodig te kunnen detecteren.

De basismaatregel luidt:

– Er worden zowel preventieve alsmede repressieve maatregelen genomen ter voorkoming en beperking van (verdere) bedrijfsschade door uitval of disfunctioneren van kritische operationele systemen. Enkele voorbeelden van maatregelen tegen diefstal zijn: een integraal systeem voor toegangsbeveiliging, zowel logisch als fysiek, en fysiek afgesloten ruimten voor servers en opslag van software.

5.2 VERLIES VAN GEGEVENS

De gebruikers van werkstations zijn afhankelijk van gegevens waarmee zij werken. Veelal zijn deze gegevens opgeslagen op een of meerdere servers in het netwerk of op locale schijven. Aangezien verlies van deze gegevens tot productieverlies kan leiden, kunnen eisen gesteld worden aan de beschikbaarheid van gegevens. Tevens moeten maatregelen genomen worden om verlies van gegevens tegen te gaan. Deze maatregelen betreffen vaak procedures voor back-up en restore van bestanden.
Van de aanbieder van de werkplekdienst kan gevraagd worden te voorzien in maatregelen om gegevensverlies te voorkomen op ser-

verniveau. Gegevensverlies kan bijvoorbeeld worden veroorzaakt door virusactiviteit. Met de leverancier van de dienst dienen afspraken gemaakt te worden ter voorkoming van virusinfecties. Ook hier speelt de discipline van de gebruiker een rol. Als een werkstation de mogelijkheid biedt om diskettes en/of andere media te gebruiken, dan kan dit een bron van virussen zijn. Hoewel de leverancier met behulp van antivirusprogrammatuur enige zekerheid kan bieden, wordt het risico verhoogd als gebruikers media gebruiken met daarop ongecontroleerde bestanden. Over dit risico dienen dan ook afspraken gemaakt te worden. Zie figuur 9 voor een overzicht van de verantwoordelijkheden.

5.2.1 Normen en maatregelen

De basisnorm is:

– Het beschikbaar zijn van gegevens is in overeenstemming met de beschikbaarheids- en integriteitseisen van de klant.

De basismaatregel is:

– Er moeten preventieve en correctieve maatregelen worden getroffen om bij verlies van gegevens deze zo snel mogelijk weer beschikbaar te hebben met zo min mogelijk verlies van de actuele gegevens. Enkele voorbeelden van maatregelen tegen het verlies van gegevens zijn: adequate back-up- en restore-voorzieningen treffen, in de SLA vastleggen wat de maximale tijd is dat gegevens verloren mogen zijn.

5.3 ONGEOORLOOFD GEBRUIK VAN PROGRAMMATUUR EN GEGEVENS/OUTPUT

Bij afwezigheid van de gebruiker van het werkstation is het voor onbevoegden fysiek goed mogelijk gebruik te maken van de programmatuur en gegevens op het werkstation. Dit heet ongeoorloofd gebruik. De overige apparatuur waarmee deze dienst wordt gevormd, zoals servers (zie figuur 9), is vaak in beter beveiligde ruimten geplaatst. Een voorbeeld van ongeoorloofd gebruik is het kopiëren van programmatuur waarvoor een licentie nodig is.
Aangezien het ongeoorloofd gebruik van de programmatuur en gegevens op het werkstation eenvoudig is en diverse partijen een rol spelen bij het treffen van adequate maatregelen, dient duidelijk te worden gemaakt wat de verantwoordelijkheden van de diverse partijen zijn.
De leverancier is verantwoordelijk voor het treffen van adequate technische voorzieningen om ongeoorloofd gebruik tegen te gaan

voor alle programmatuur, dus ook de programmatuur op de servers. De klant is verantwoordelijk voor het naleven van de beveiligingsprocedures door het eigen personeel.

5.3.1 Normen en maatregelen

De basisnorm is:

– De maatregelen ter voorkoming van ongeoorloofd gebruik van programmatuur en gegevens zijn in overeenstemming met de eisen ten aanzien van exclusiviteit die door de klant zijn gesteld in de SLA.

Voorbeelden van maatregelen tegen ongeoorloofd gebruik van programmatuur en gegevens/output zijn:

– De toegang tot het werkstation moet gecontroleerd worden (wachtwoord voor toegang, beveiligde screensavers, enzovoort).
– Er is gecontroleerde fysieke toegang tot ruimten waar apparatuur centraal staat opgesteld (de serverruimten, patchkasten, enzovoort – dus niet de ruimte waar het werkstation staat).

5.4 NIET KUNNEN WERKEN

Het is zinvol onderscheid te maken tussen het uitvallen van de complete dienstverlening en delen daarvan. Een werkstation dient vaak als basis voor het ontsluiten van andere meer specifieke toepassingen, zoals personeelsinformatiesystemen en financiële informatiesystemen. Om met bijvoorbeeld het financiële informatiesysteem te kunnen werken is het werkstation een voorwaarde, evenals het achterliggende netwerk en de server waarop de toepassing draait. Er is sprake van een keten. Een uitspraak over de beschikbaarheid van een werkplek zoals vastgelegd in de SLA, is daarmee een uitspraak over de beschikbaarheid van de gehele keten.
Aangezien per toepassing een aparte beschikbaarheid kan gelden en per werkstation een mix van deze toepassingen mogelijk is, kan een ingewikkelde situatie ontstaan. Daardoor kunnen per werkstation uiteenlopende beschikbaarheidseisen gelden. Het is zaak dit mechanisme te bewaken en de beschikbaarheid onder te brengen in een aantal verschillende 'standaard' niveaus van dienstverlening. In de praktijk wordt volstaan met drie niveaus: het basisniveau, het verhoogde beschikbaarheidsniveau en het hoge beschikbaarheidsniveau. Bij de inrichting van de werkplek kan hiermee rekening worden gehouden. De situatie blijft daarmee overzichtelijk en per werkplek kan de beschikbaarheid in de configuratie worden meegenomen. Indien verschillende delen van de keten aan onderaannemers zijn

toevertrouwd blijft de hoofdaannemer verantwoordelijk. De klant dient wel ingelicht te worden.

5.4.1 Normen en maatregelen

De basisnorm is:

– De beschikbaarheid van de werkplekken is een correcte afspiegeling van het gebruik ervan.

Voorbeelden van maatregelen zijn:

– Er bestaan adequate escalatieprocedures, ook met toeleveranciers van apparatuur en software.
– Er moet een uitwijkwerkplek beschikbaar zijn.

5.5 ONVOLDOENDE WERKPLEKBEHEER

Het correct functioneren van de werkplek wordt door het operationeel beheer gewaarborgd. Zo bezien is het hebben van operationeel beheer voorwaardelijk voor het bieden van welke dienst dan ook. Een goed ingericht operationeel beheer geeft signalen af als er zaken dreigen mis te lopen, voert herstelacties uit indien er zaken zijn misgelopen, installeert nieuwe apparatuur, installeert updates van antivirus-programmatuur, vervangt oude apparatuur, geeft bij storingen signalen naar de helpdesk (zodat deze de gebruikers kan inlichten over het mogelijk niet beschikbaar zijn van een of meerdere toepassingen), handhaaft de geïmplementeerde beveiligingsmaatregelen, enzovoort.
Alle afspraken met betrekking tot beschikbaarheid, integriteit en exclusiviteit kunnen worden geschaad indien het operationeel beheer onvoldoende is ingericht. Het operationele beheer is in zijn geheel de verantwoordelijkheid van de leverancier. Een klant zal in de praktijk geen inzicht krijgen in het functioneren van het operationeel beheer bij de leverancier. Er kunnen wel afspraken gemaakt worden om deze functie door een onafhankelijke derde partij te laten controleren.

5.5.1 Normen en maatregelen

De basisnorm luidt:

– Het operationeel beheer is zodanig ingericht dat (de eisen van) beschikbaarheid, integriteit en exclusiviteit zijn gewaarborgd.

Voorbeelden van maatregelen tegen onvoldoende werkplekbeheer zijn:

– Richt het operationeel beheer in met duidelijke procedures.
– Zorg voor goed opgeleid personeel.

5.6 INADEQUATE HELPDESK

De helpdesk is het loket waar de gebruiker zijn dagelijkse klachten en vragen kan indienen. De helpdesk heeft tot taak gebruikers zo snel mogelijk weer in de gelegenheid te stellen het werk uit te voeren. Mocht een klacht niet direct verholpen kunnen worden, dan wordt vanuit de helpdesk een beroep gedaan op een groep specialisten die gaat zorgen voor een oplossing. De helpdesk bewaakt deze activiteiten en informeert de gebruiker over de voortgang. In een SLA zijn vaak afspraken gemaakt over de openingstijden van de helpdesk, de gewenste beschikbaarheid van de systemen waarmee de gebruikers werken, alsmede de maximale duur van het niet operationeel zijn van de systemen. De helpdesk zal bij verstoringen de prioriteit die aan het oplossen daarvan wordt gegeven bepalen aan de hand van de in de SLA vastgelegde afspraken.
Behalve als loket ten behoeve van de gebruikers naar de organisatie toe, is de helpdesk vanuit de leverancier geredeneerd het loket waardoor hij kan communiceren met de gebruiker over op handen zijnde gebeurtenissen. Een goed werkende helpdesk kan als eerstelijns ondersteuning de beschikbaarheid van de werkstations enorm vergroten. Door het bijhouden van incidenten en de oplossingen ervan kunnen de meest voorkomende klachten snel door de helpdesk worden verholpen. Ten aanzien van beveiligingsincidenten moet de helpdesk over informatie beschikken waardoor onderscheid gemaakt kan worden tussen gewone incidenten en beveiligingsincidenten. Tevens dient een procedure te bestaan die de afhandeling van een beveiligingsincident beschrijft. Bij het afhandelen van een inbraakpoging op het netwerk wordt bijvoorbeeld de beveiligingsbeambte ingeschakeld, die buitenspel blijft als het gaat om de melding dat een toepassing niet functioneert.

5.6.1 Normen en maatregelen

De basisnorm is:

– De helpdesk biedt adequate ondersteuning aan de gebruikers.

Voorbeelden van maatregelen zijn:

– De helpdesk dient te kunnen beschikken over voldoende geschoold personeel.
– De helpdesk dient te beschikken over een goede, geautomatiseerde helpdesktool.

5.7 ONVOLDOENDE AUTORISATIEBEHEER

Autorisatiebeheer is het toekennen, wijzigen en verwijderen van rechten in een systeem of applicatie, veelal op basis van een functierol. Voordat een gebruiker gebruik kan maken van de hem toegekende rechten, dient hij te zijn ingelogd, dat wil zeggen door het systeem te zijn geïdentificeerd op basis van zijn gebruikersnaam en geauthenticeerd door middel van zijn persoonlijke wachtwoord. Een correct functionerend autorisatiebeheer is van essentieel belang. Het begrenst immers de mogelijkheden van de gebruiker en biedt bescherming tegen ongewenste inbreuk op de overige componenten van het systeem. Zo heeft een gebruiker bijvoorbeeld de mogelijkheid (via het hem toegekende recht) om bepaalde bestanden te lezen, gegevens te wijzigen of te verwijderen en programma's te starten. Onder autorisatiebeheer valt ook het al dan niet toestaan van door gebruikers geïnstalleerde screensavers en het downloaden van (kwaadaardige) programmatuur van buiten de organisatie.
Voor de juiste werking van het autorisatiebeheer is niet alleen de leverancier verantwoordelijk. Ook de klant speelt hierbij en rol. De klant is namelijk zelf verantwoordelijk voor het inrichten en aanleveren van de functieprofielen die de leverancier dient te hanteren bij het toekennen van autorisaties en het uitvoeren van het autorisatiebeheer. In de praktijk is het een goed gebruik dat er een samenspel ontstaat tussen de klant en de leverancier over het autorisatiebeheer.

5.7.1 Normen en maatregelen

De basisnorm is:

– De rechten met betrekking tot het gebruik van programma's en gegevens zijn op grond van functieprofielen correct toebedeeld aan de medewerkers in de organisatie en bij de leverancier, en worden als zodanig up-to-date beheerd.

Basismaatregelen zijn:

– Voor elke medewerker wordt door de organisatie vastgesteld en gewaarborgd welke (IT-)functies hij mag uitvoeren, voor welke gegevens en met welke programma's. Optioneel kan worden bepaald voor welke grenswaarden de medewerker is geautoriseerd.
– Door de invoering van functiescheiding tussen autorisatie, uitvoering en controle wordt een controlefunctie ingebouwd voor medewerkers met hoge systeemrechten.

Voorbeelden van maatregelen tegen onvoldoende autorisatiebeheer zijn: jaarlijkse controle op bevoegdheden, en periodiek doorgeven van wijzigingen in bevoegdheden (een verantwoordelijkheid van de klant).

5.8 ONVOLDOENDE CONFIGURATIEBEHEER

Geen organisatie kan efficiënt of effectief zijn zonder adequate zorg voor zijn middelen. Hoe essentiëler de middelen zijn voor de organisatie, hoe belangrijker de zorg wordt. Deze methode start met het aanleggen van een lijst van de middelen in een bestand. Met middelen worden hier niet alleen hardware- en softwarecomponenten bedoeld , maar ook de organisatiestructuur. Tot welk detailniveau er componenten onderscheiden worden, is afhankelijk van de situatie en vormt de grootste uitdaging van het configuratiebeheer. Het aanleggen en nauwgezet bijhouden van deze lijst wordt configuratiebeheer genoemd. Configuratiebeheer houdt tevens in dat er per te onderscheiden configuratie-item een verantwoordelijke wordt aangewezen.
De volgende gegevens worden veelal bijgehouden:
– locatie van de configuratie-items (geografische spreiding);
– aantal licenties;
– welke gebruiker gebruikmaakt van welke componenten;
– samenhang van de componenten;
– beveiligingsonderwerpen, zoals beschikbaarheidseisen, integriteitseisen en gewenste toegankelijkheid van de component.

De verantwoordelijkheid voor configuratiebeheer ligt voornamelijk bij de leverancier, maar de klant speelt ook een belangrijke rol. De klant is namelijk verantwoordelijk voor bijvoorbeeld het melden van verhuizingen van apparatuur. De klant stelt de beveiligingseisen vast die aan de diverse te onderscheiden componenten worden gesteld. De leverancier geeft garanties over het implementeren van de gerelateerde maatregelen.

5.8.1 Normen en maatregelen

De basisnorm is:
– Er zijn maatregelen genomen voor het dusdanig registreren van componenten dat voor de andere beheerprocessen voldoende gegevens beschikbaar zijn over de componenten die tezamen de werkplekautomatisering realiseren.

Voorbeelden van maatregelen tegen onvoldoende configuratiebeheer zijn:
– Er is een correcte registratie van alle in gebruik zijnde en nieuw in te kopen hardware en software.
– Er bestaat een periodieke controle op de volledigheid van de configuratiedatabase.

5.9 SOFTWARECONTROLE EN -DISTRIBUTIE

Het onder controle houden van alle software die op werkplekken wordt geïnstalleerd, inclusief de versies ervan, is een niet te onderschatten taak met grote invloed op de beschikbaarheid van de systemen. Het gaat hierbij niet slechts om de softwarecomponenten afzonderlijk maar juist in samenhang. Het vooraf goed testen van nieuwe softwarecomponenten op hun integreerbaarheid met de reeds aanwezige softwarecomponenten op een werkplek vormt een belangrijk element om de beschikbaarheid van het werkstation te garanderen. Het controleren van de aangeboden softwarecomponenten op de aanwezigheid van virussen is een maatregel om de integriteit te waarborgen.
Ten aanzien van beveiligingsaspecten spelen derhalve de volgende elementen een belangrijke rol:

- het controleren van de software componenten op virussen;
- het zeker stellen dat aangeboden softwarecomponenten niet conflicteren met andere componenten;
- het zeker stellen dat bij de overgang van een nieuwe versie van het operating systeem alle softwarecomponenten daarmee kunnen werken, en dat deze werking door de leveranciers wordt gegarandeerd;
- het zeker stellen dat bij de overgang naar een nieuwere versie van het databasesysteem de softwarecomponenten ook daarmee kunnen werken, dat deze werking door de leveranciers wordt gegarandeerd en dat de gegevens die in de database zijn opgeslagen correct worden gemigreerd naar de nieuwe versie van de database.

Zodra een nieuwe release van de software is uitgebracht, wordt dit de actuele release en moet hij worden opgenomen in de configuratiedatabase. Het actualiseren van de configuratiedatabase moet tegelijkertijd met het beschikbaar stellen van de release worden uitgevoerd. Op deze wijze wordt gegarandeerd dat storingen die zich daarna voordoen altijd worden onderzocht, gebruikmakend van de actuele gegevens.
Het bijhouden van historische gegevens over softwarereleases is een tweede belangrijke taak. De gegevens die moeten worden bijgehouden om op een later tijdstip nog gebruik te kunnen maken van oude software, zijn omvangrijk. Bij het niet adequaat bijhouden van deze gegevens bestaat het gevaar dat oude software of gegevens niet meer gebruikt kunnen worden, wat tot aanzienlijke schade kan leiden.
Gegevens die moeten worden bijgehouden zijn:

- softwarecomponenten van een release;
- het gebruikte operating systeem;

– het gebruikte databasemanagementsysteem;
– de gebruikte hardwareconfiguratie (let hierbij speciaal op het gebruik van randapparatuur).

Er zijn instellingen die een groot archief aan acht-inch-diskettes bezitten maar niet de apparatuur die deze diskettes kan lezen, noch de software die de bestanden kan verwerken.

5.9.1 Normen en maatregelen

De basisnorm is:
– Er bestaat een adequaat stelsel van afspraken met betrekking tot de softwarereleasestrategie, het softwaredistributiemechanisme en het historisch configuratiebeheer.

Voorbeelden van maatregelen tegen onvoldoende softwarecontrole en -distributie zijn:
– Er is gezorgd voor virusvrije verspreiding van software.
– Er is gezorgd voor een uitgebreide controle op de werking van softwarecomponenten in hun onderlinge samenhang.

5.10 AANDACHTSPUNTEN IN DE SLA

De kwaliteit van de dienstverlening die verbonden is aan het beschikbaar stellen van pc's en randapparatuur, wordt voor een belangrijk deel bepaald door de directe interactie met de klant die daarbij plaatsvindt. Naast deze front-office-activiteiten is het echter ook van groot belang dat op de achtergrond een aantal belangrijke organisatorische maatregelen wordt getroffen. Deze zogenaamde back-office-activiteiten zijn voor de kwaliteit van de dienstverlening van minstens even groot belang.
Werkplekondersteuning is sterk gericht op het direct ondersteunen van de gebruikers van de werkplekapparatuur, en is daarmee voor de klant een zeer zichtbaar proces. De snelheid en deskundigheid waarmee problemen op de werkplek worden opgelost, kan door iedere gebruiker vanuit de eerste hand worden vastgesteld. Om een oordeel te kunnen geven over het functioneren van de back-officeprocessen is het noodzakelijk dat er inzicht is in zowel de inrichting als de normering van deze processen. Voor de inrichting wordt veelal gebruikgemaakt van het gedachtegoed van ITIL, waarbij de te hanteren normen eenduidig in een SLA kunnen worden vastgelegd. Met name als besloten wordt tot uitbesteding van de werkplekondersteuning, zullen tussen klant en leverancier duidelijke afspraken gemaakt moeten worden over zowel de front- als de back-officeprocessen.

In de voorgaande paragrafen is een overzicht gegeven van de belangrijkste bedreigingen die binnen de werkplekdienstverlening kunnen optreden, alsmede de belangrijkste maatregelen die daartegen getroffen dienen te worden. Bij de uitbesteding van het werkplekbeheer zal met deze bedreigingen terdege rekening gehouden moeten worden. Elk van de genoemde bedreigingen zal in de SLA die tussen de klant en de leverancier gesloten wordt besproken dienen te worden, waarbij tevens aangeven zal moeten worden op welke wijze deze bedreigingen te compenseren zijn.
Ter borging van de afgesproken normen en maatregelen zal niet alleen op reguliere basis controle van het geleverde product plaats dienen te vinden, maar ook – op meer periodieke basis – een controle van de onderliggende structuur van het voortbrengingsproces. De reguliere controle van het geleverde product zal door de afdeling SLM worden verzorgd, waarbij gebruik wordt gemaakt van de door de leverancier aangeleverde rapportages. De verbijzonderde periodieke controle van het voortbrengingsproces (en van de betrouwbaarheid van de rapportages) is de taak van de EDP-auditor.
In het vervolg zullen de belangrijkste bedreigingen nader besproken die in de SLA een plaats zouden moeten krijgen. Hierbij wordt nog aangetekend dat zowel de klant als de leverancier binnen zijn eigen ICT-organisatie een eigen kwaliteits- en beveiligingsniveau hanteert. Bij het opstellen van een SLA zal getracht moeten worden deze niveaus bij elkaar te brengen.

Diefstal Om zo goed mogelijk toegankelijk te zijn voor de gebruikers, dienen pc's en randapparatuur op een groot aantal bureaus op vaak nog verschillende kantoorlocaties beschikbaar te zijn. De toegankelijkheid gekoppeld aan een vaak hoge verspreidingsgraad van apparatuur vergroot de kans op diefstal. Dit wordt nog versterkt door het steeds toenemende gebruik van mobiele systemen, zoals laptops. Mogelijkheden om diefstal van computer en randapparatuur tegen te gaan zullen vooral gezocht moeten worden in preventieve maatregelen. Dit kunnen zowel fysieke als logische maatregelen zijn. De effectiviteit van de maatregelen zal met name in combinatie met de klassieke fysieke beveiligingsmaatregelen, zoals toezicht op en bewaking van de omgeving waarin de apparatuur staat opgesteld, aanzienlijk verhoogd worden.
Eisen in de SLA betreffen:
- fysieke beveiliging van apparatuur;
- logische beveiliging van apparatuur;
- beveiliging en bewaking van kantoorlocaties;
- toewijzing en registratie van apparatuur;
- preventiebeleid;

– aangiftebeleid;
– rapportage.

Verlies van gegevens Het opslaan en verwerken van gegevens is een primaire taak van de pc en randapparatuur. Het is dan ook een inherent risico van dit proces dat het soms tot problemen leidt waarbij gegevens verloren gaan. In het overgrote deel van de gevallen ligt de oorzaak van gegevensverlies bij het onjuiste of ondeskundige gebruik van de apparatuur of software. Een goede back-upprocedure en het strikt naleven daarvan kan een hoop problemen voorkomen. Vaak zal vanuit een dataserver in het netwerk al automatisch worden gezorgd voor het maken van back-upsvf, zodat de gebruiker alleen nog zijn lokale data zal moeten veiligstellen. Het beheer van de dataserver is een onderdeel van het netwerkbeheer.
Gegevensverlies kan ook externe oorzaken hebben, zoals virussen en andere ongewenste programmatuur. Een goede virusscanner, voorzien van de recentste profielen van mogelijk-schadelijkprogramma's, kan een effectief middel zijn.
Ongeacht de oorzaak van het gegevensverlies moet een gebruiker zo spoedig mogelijk geholpen worden als hij problemen ondervindt met het gebruik van zijn pc of randapparatuur. In eerste instantie zal deze hulp van de helpdesk moeten komen. Is er echter ondersteuning ter plekke nodig, dan zal ook deze binnen redelijke termijn geboden moeten worden.
Eisen in de SLA betreffen:
– installatieprotectie voor programmatuur;
– een back-upprocedure voor (lokale) data;
– het opleiden van gebruikers;
– ondersteuning door de helpdesk;
– ondersteuning op de werkplek;
– rapportage.

Ongeoorloofd gebruik van programmatuur, gegevens en output Een aantal totaal verschillende situaties kan leiden tot het ongeoorloofd gebruik van programmatuur en gegevens. Een veelvoorkomende situatie is dat een reguliere gebruiker toegang krijgt tot programmatuur of gegevens die hij voor zijn taakuitoefening niet nodig heeft en waartoe hij niet is geautoriseerd. Te denken valt aan bepaalde (beheer of ontwikkel)tools die bij onjuist gebruik grote schade zouden kunnen aanrichten, of aan vertrouwelijke of privacygevoelige data. Ook uit het oogpunt van functiescheiding is het niet wenselijk dat toegang wordt verkregen tot bepaalde apparatuur of gegevens. Om deze reden is het noodzakelijk dat men beschikt over een adequaat sys-

teem van toegangsbeveiliging, waarin aan de juiste personen de juiste bevoegdheden zijn toegekend.
Een andere situatie is dat op de werkplek gebruik wordt gemaakt van programmatuur waarvoor geen licentierechten zijn verkregen, of apparatuur die illegaal is geïnstalleerd, waardoor problemen met andere reguliere onderdelen van de technische infrastructuur kunnen ontstaan. Zeker als de werkplek over een internetverbinding beschikt, is het downloaden van programma's en tools geen enkel probleem. Door regelmatig scans uit te voeren of speciale programmatuur te installeren, kan hiertegen opgetreden worden.
Ook kan het voorkomen dat een derde, niet-reguliere gebruiker, zich toegang verschaft tot apparatuur waartoe hij niet gerechtigd is, of gebruikmaakt van de rechten van een ander. Het gebruik van user-id's met strikt persoonlijke wachtwoorden kan dit voorkomen. Ook kan gebruikgemaakt worden van bijvoorbeeld screensavers om een gebruiker die even van zijn plek is te behoeden voor oneigenlijk gebruik van zijn pc.
Eisen in de SLA betreffen:
- een systeem van toegangsbeveiliging;
- actuele en veilige wachtwoorden;
- een duidelijke bevoegdhedenstructuur;
- geen illegale programmatuur;
- screensavers;
- rapportage van inbreuken.

Niet kunnen werken Het ICT-proces wordt steeds meer integraal onderdeel van de bedrijfsprocessen, zodat uitval direct gevolg heeft voor de continuïteit van de bedrijfsvoering. Gebruikers die niet meer kunnen beschikken over hun pc of randapparatuur kunnen hun werk niet meer doen. Zeker als een grotere groep van gebruikers tegelijkertijd niet meer kan werken, ontstaat een acuut probleem. Dit is dan ook een van de beveiligingsaspecten die meestal wel in een SLA zijn opgenomen in de vorm van een algemene beschikbaarheidseis. Het is echter wenselijk om naast deze algemene beschikbaarheidseis een aantal onderliggende beveiligingsaspecten te noemen die aan deze algemene eis nadere invulling geven.
Eisen in de SLA betreffen:
- normen voor beschikbaarheid;
- ondersteuning door de helpdesk;
- ondersteuning op de werkplek;
- testen en certificeren;
- vervangende apparatuur;
- een uitwijk;
- rapportage.

Onvoldoende werkplekbeheer Werkplekbeheer is de verzameling van activiteiten die nodig zijn om aan de gebruiker een werkplek ter beschikking te stellen conform de gemaakte afspraken. Een deel van deze activiteiten is voor de gebruiker direct zichtbaar. Er staat apparatuur voor hem klaar, hij kan een beroep doen op de helpdesk of een IT-loket en in geval van nood wordt hij op de werkplek ondersteund.
Daarnaast zal in de back-office een aantal ondersteunende activiteiten moeten worden ontplooid om ervoor te zorgen dat het werkplekbeheer ook voor langere tijd zonder problemen zal verlopen. Deze aan ITIL gerelateerde activiteiten, zoals de helpdesk, configuratiebeheer, softwarecontrole en -distributie, komen in het vervolg aan de orde.
Bij onvoldoende werkplekbeheer wordt in eerste instantie gedacht aan meer algemeen organisatorische aspecten, zoals het opstellen en bewaken van procedures, het zorgen voor deskundige en correct handelende medewerkers, communiceren met gebruikers, signaleren van structurele problemen en het rapporteren aan de opdrachtgever. Periodiek zal een audit worden uitgevoerd om meer inzicht te krijgen in de kwaliteit van de geboden ondersteuning, in de wijze waarop de werkzaamheden zijn ingericht en in de betrouwbaarheid van de rapportages.
Eisen in de SLA betreffen:
- deskundigheid;
- een gedragscode;
- het onderkennen van structurele problemen;
- rapportage;
- een periodieke audit.

Helpdesk Werkplekbeheer kent een intensieve relatie met de gebruikersorganisatie. De helpdesk, die er primair op gericht is om de gebruikers bij hun operationele problemen te helpen, speelt binnen werkplekbeheer dan ook een belangrijke rol. Binnenkomende incidenten worden door de helpdesk geregistreerd en in eerste instantie zo veel mogelijk op afstand opgelost. Als dit niet tot een oplossing leidt, wordt iemand naar de betreffende locatie gestuurd om de gebruiker hulp te bieden. Bij ernstige problemen kan eventueel voor vervangende apparatuur gezorgd worden. De voortgang en kwaliteit van dit proces wordt door de helpdesk bewaakt.
Gezien de directe relatie met de gebruikersorganisatie kan de helpdesk ook als algemeen meldpunt voor andere zaken dienen, bijvoorbeeld het melden van misbruik of van ongewenste situaties.
Eisen in de SLA betreffen:
- beschikbaarheid van de ondersteuning;

– omvang en duur van de ondersteuning;
– registratie van incidenten;
– voortgang (en doorverwijzing) van incidentafhandeling;
– een centraal meldpunt;
– rapportage.

Autorisatiebeheer Het gebruik van een betrouwbaar systeem van logische toegangsbeveiliging speelt een belangrijke rol bij de beveiliging van de werkplekken. De werking van een dergelijk systeem is in sterke mate afhankelijk van de wijze waarop inhoud wordt gegeven aan het beheer van de overzichten met gebruikers en hun individuele rechten op bepaalde objecten. Zeker bij een organisatie van enige omvang zal er niet alleen sprake zijn van een groot aantal gebruikers en objecten, maar ook van een frequente mutatie hiervan.
Aangezien het van groot belang is dat aan een individuele gebruiker een juiste autorisatie wordt verstrekt, zal de autorisatieverlening via een strikte procedure moeten worden toegekend. Daarbij zal niet alleen steeds van een bevoegde derde (lijnmanager/directeur/projectleider) toestemming verkregen moeten worden, maar ook zal bewaakt moeten worden of de verleende autorisaties passen in het grotere geheel van functiescheidingen.
In een systeem van logische toegangsbeveiliging is het mogelijk om een groot aantal parameters in te stellen om te komen tot een strengere of minder strenge verificatie van de gebruiker en de aan hem verleende autorisatie. De gebruiker kan meestal een aantal pogingen doen om in te loggen en zijn wachtwoord heeft een bepaalde levensduur. Er valt echter nog een groot aantal andere regels te definiëren. Zeker bij een strikt ingericht systeem van toegangsbeveiliging is het belangrijk dat de gebruiker kan terugvallen op een adequate ondersteuning door de helpdesk.
Naast het onderhouden van de gebruikersgegevens en objecten heeft het autorisatiebeheer ook tot taak om de werking van het systeem te bewaken en in een zo vroeg mogelijk stadium eventuele ongeautoriseerde pogingen om toegang te krijgen te signaleren en verijdelen.
Eisen in de SLA betreffen:
– een overzicht van managers die bevoegd zijn tot autorisatieverlening;
– eenoverzicht van functies en functiescheidingen;
– een overzicht van medewerkers;
– regels voor toegangsautorisatie;
– ondersteuning door de helpdesk;
– monitoring;
– het signaleren van inbraak en gewenste vervolgacties;
– rapportage.

Configuratiebeheer Het grote aantal componenten en de verspreiding daarvan over een groot aantal locaties stelt bijzondere eisen aan het beheer en dus ook aan de beveiliging daarvan. Nauwkeurig zal bijgehouden moeten worden welke systemen zich op welke locatie bevinden. Dit betekent dat er duidelijk afgesproken moet worden onder welke voorwaarden systemen zullen worden aangeschaft, verhuisd en afgestoten, teneinde de juistheid van de registratie te waarborgen. Tevens is het wenselijk om elk systeem aan een bepaalde gebruiker te koppelen, zodat deze hiervoor verantwoordelijk kan worden gesteld.
Teneinde het beheer te vereenvoudigen en de kosten van de aanschaf en het beheer te reduceren, is het wenselijk om zo veel mogelijk te standaardiseren. Daarnaast zal de opdrachtgever een grens dienen te stellen aan het onderhoud, de upgrade en de vervanging van systemen. Ten slotte zullen ook grenzen gesteld moeten worden aan de onvermijdelijke groei van het totale pc-bestand.
Registratie van de configuratie-items is noodzakelijk omdat deze een aanzienlijke waarde vertegenwoordigen. Daarnaast zijn er vaak garantieverplichtingen verbonden aan systemen, waardoor de kosten voor onderhoud en reparatie op een derde kunnen worden verhaald.
Omdat het configuratiebeheer ook een belangrijke pijler is voor de nadere beheerfuncties, zal de juistheid en volledigheid van de registratie regelmatig moeten worden gecontroleerd.
Eisen in de SLA betreffen:

- de wijze van registratie van de configuratie items;
- een procedure voor het aanschaffen, verhuizen en afstoten van systemen;
- onderhoud, update- en vervangingsbeleid;
- de maximaal toegestane groei;
- de wijze van waardering en afschrijving;
- verhalen van service- en garantieverplichtingen;
- rapportage;
- de controle op juistheid en volledigheid van de registratie.

Softwarecontrole en -distributie Het beheer van de software is evenzeer van belang als het beheer van de hardware. Afhankelijk van de omvang van de te beheren software-items worden deze ook vaak als onderdeel van het configuratiemanagement gezien. Bij grotere organisaties is de registratie en distributie van software dermate omvangrijk dat hiervoor een aparte beheerfunctie wordt ingericht.
Op hoofdlijnen gelden dezelfde aspecten als bij het bovengenoemde configuratiebeheer. Bijzonder zijn nog het bijhouden en naleven van de licentieverplichtingen, en het testen en controleren van software op virussen en andere ongewenste programmatuur en functies.

Uiteraard zal de programmatuur voorzien zijn van de juiste documentatie en zal de gebruikers- en de beheerorganisatie op de nieuwe software voorbereid moeten zijn.
Eisen in de SLA betreffen:

- registratie;
- licentiebeheer;
- het testen op virussen;
- distributie van documentatie;
- opleidingen voor gebruikers;
- instructie van de helpdesk.

6 Uitbesteding van systeemontwikkelingsprocessen

Het ontwikkelen van een systeem is een vakgebied dat uitermate sterk in beweging is. Methoden en technieken volgen elkaar in snel tempo op. Er wordt in de universitaire wereld hard gewerkt aan het wiskundig onderbouwen van systeemontwikkelmethodieken en bewijsvoering voor correct werkende programmatuur. Dit laatste doel is nog niet bereikt.
In dit document wordt voor het begrip systeemontwikkeling de volgende definitie gehanteerd: het door een leverancier laten ontwikkelen van een specifiek voor die organisatie benodigd systeem. Systeemontwikkeling houdt zich bezig met het vertalen van functionele gebruikerseisen en -wensen naar software programma's.

Om tot een aanvaardbare kwaliteit van de op te leveren producten te komen, wordt veel aandacht geschonken aan het beheersen van het systeemontwikkelingsproces. Een veelgebruikte kwaliteitsstandaard is een volwassenheidsmodel voor systeemontwikkelorganisaties, het Capability Maturity Model (CMM), dat vijf volwassenheidsniveaus kent. In de Verenigde Staten is het bij overheden gebruikelijk dat bij aanbestedingen slechts bedrijven op de shortlist komen die minimaal op het derde niveau gecertificeerd zijn.
Hoewel het beheersen van het systeemontwikkelingsproces vele aspecten kent, worden hier twee aspecten behandeld die voor informatiebeveiliging direct van belang kunnen zijn. Deze aspecten zijn het genormeerd vastleggen van kwaliteitsspecificaties (omdat hiermee tevens de beveiligingsspecificaties vastgelegd kunnen worden) en de risico's die de diverse systeemontwikkelmethodieken kenmerken.
Voor het bepalen van de kwaliteit van systemen wordt vaak gebruikgemaakt van de ISO-norm 9126. In deze norm zijn ook beveiligingsaspecten beschreven. Om risico's adequaat te kunnen pareren is het noodzakelijk voldoende aandacht te besteden aan het correct definiëren van deze beveiligingseisen. De ISO-norm schenkt zowel aandacht aan de 'technische' eisen als aan de functionele en organisatorische eisen. Zo wordt per invalshoek de kwaliteitsbelevenis van de systeemontwikkelaar, de eindgebruiker en de beheerorganisatie beschreven. Hoewel er niet specifiek aandacht wordt geschonken aan

de beveiligingsfunctionaris, biedt dit model voldoende mogelijkheden om de beveiligingsaspecten goed te beschrijven [Van Zeist].
Het beheersen van systeemontwikkeling kan voor een deel worden ondersteund door het gebruik van methoden. De meeste methoden zijn gebaseerd op de life-cycle van een systeem. Ze beschrijven de specificatie-, implementatie-, test- en de exploitatie- en onderhoudsfase. Deze methoden helpen op diverse niveaus. Ten eerste dwingt een methode tot het vooraf nadenken over de te bereiken doelen, zodat een juiste inschatting van de te leveren inspanning kan worden gemaakt. Ten tweede voorzien de methoden vaak in checklists, zodat de ontwikkelaars en analisten geen essentiële items vergeten. Ten derde voorziet de methode in een universele vastlegging van definities en ontwerpen, zodat de diverse betrokken partijen elkaars werk kunnen begrijpen.
Voor vrijwel alle methoden bestaan geautomatiseerde hulpmiddelen, variërend van eenvoudige vertalers (compilers) tot luxe geïntegreerde computer-aided software-engineering(I-Case)tools die in staat zijn vanuit een functioneel ontwerp de programma's te genereren. Natuurlijk heeft iedere methode zijn voor- en nadelen. In paragraaf 6.3 worden de specifieke risico's met betrekking tot informatiebeveiligingsaspecten nader uitgewerkt.
Een extra bedreiging voor de beveiliging in systeemontwikkeltrajecten is de complexiteit van de te ontwikkelen systemen. Complexiteit ontstaat door het koppelen van verschillende softwarepakketten, het steeds complexer worden van besturingssystemen en de veelheid aan toepassingen. De veelheid aan toepassingen veroorzaakt complexiteit, omdat al deze toepassingen zodanig geconfigureerd moeten worden dat zij zonder elkaar te storen op een werkstation of server kunnen draaien.

Trends in systeemontwikkeling Dit hoofdstuk is geschreven vanuit de traditionele ontwikkelwijze van systemen. Hierbij wordt uitgegaan van systemen met een redelijke omvang, waarvan de specificaties niet fundamenteel veranderen en de minimale doorlooptijd zes maanden bedraagt.
In de huidige en toekomstige tijd zullen er meer en meer systeemontwikkeltrajecten van zes of minder weken komen. Internetdienstverlening zoals e-commercetoepassingen worden geregeerd door het credo 'wie het eerst iets op de markt zet, behaalt alle winst'. In deze hectische markt kan men zich geen langdurige systeemontwikkeltrajecten veroorloven. Systeemontwikkeltrajecten zullen zich in veel gevallen beperken tot het operationeel maken van een redelijk werkend en vooral smakelijk uitziend prototype. Er zullen veel meer dan

nu vormgevers aan het werk worden gezet om vooral de goed ogende buitenkant te ontwerpen, waardoor minder aandacht gegeven zal worden aan het zorgvuldig ontwerpen en testen van de op te leveren systemen. Immers, de acceptatietest is de markt en het product moet gisteren eigenlijk al operationeel zijn.
Om dit te bewerkstelligen zal men veel meer dan nu gebruikmaken van bouwstenen, het zogenaamde component-based development. De kwaliteit van de informatiebeveiliging wordt daarmee onder meer afhankelijk van de kwaliteit van deze componenten en niet te vergeten de samenstelling ervan. Het karakter van de informatiebeveiliging zal hierdoor niet wezenlijk worden gewijzigd. Wellicht zullen enkele hierboven aanbevolen maatregelen aan kracht inboeten. Immers, het in escrow geven van de broncode van een programma dat slechts in enkele weken gebouwd kan worden is weinig zinvol. De afhankelijkheid van geautomatiseerde systemen zal echter toenemen, evenals het goed beveiligde zakendoen.
'Zonder beveiliging geen business' is daarmee een blijvend correcte zienswijze. Ook snel ontwikkelde systemen verliezen hun waarde als blijkt dat er onwerkbaar veel fouten in zitten of dat er eenvoudig mee gefraudeerd kan worden.

6.1 ALGEMENE RISICO'S

Het gebruik van de methoden en technieken alsmede de begeleidende tools is kenmerkend voor systeemontwikkelwerkzaamheden. Het correct vertalen van eisen en wensen van een opdrachtgever naar goed functionerende programmatuur is daarbij essentieel. Een ander aspect is het onder controle houden van een systeemontwikkelproject. Uit onderzoek is gebleken dat in 1997 wereldwijd circa een kwart van alle systeemprojecten gestopt zijn vanwege het niet tijdig en ver buiten afgesproken budgetten opleveren daarvan.
Nieuwe systemen kunnen nieuwe risico's met zich meebrengen. Integratie van bedrijfsadministraties, zoals het geval is bij een ERP-implementatie, kent als voordeel dat daarmee waardevolle managementinformatie over de bedrijfsvoering kan worden verkregen. Daarmee ontstaat een nieuwe bedreiging, want deze informatie kan in verkeerde handen terechtkomen.
Voor elke stap in het systeemontwikkeltraject moeten met de leverancier afspraken gemaakt worden over de specifieke beveiligingsaspecten. Het systeem is meestal van essentieel belang om (een deel van) de bedrijfsprocessen naar behoren te laten verlopen. Het is dan ook belangrijk dat het systeem voldoet aan de verwachtingen en de

kwaliteitseisen van de organisatie. Dit vereist dat er voldoende aandacht besteed wordt aan de kwaliteit van specificaties zoals bijvoorbeeld is vastgelegd in ISO-norm 9126.
Het uitbesteden van systeemontwikkeling kan op een tweetal manieren worden vormgegeven. Bij geheel uitbesteden vormen mensen en middelen geen onderdeel van de klantorganisatie. Bij insourcing wordt het personeel als team onder projectverantwoordelijkheid van de leverancier ondergebracht op de locatie van de klant.

Bij het uitbesteden van systeemontwikkeling moeten tevens afspraken worden gemaakt op het gebied van beveiliging. Voorbeelden van beveiligingsaspecten die bij uitbesteding van systeemontwikkeling van specifieke betekenis zijn, zijn:
– Ongeoorloofd gebruik van (output van) gegevens; hierbij valt te denken aan het in opdracht laten programmeren van gepatenteerde ideeën.
– Opzettelijke inbreuk op systemen; hierbij valt te denken aan slordig programmeren, waardoor gegevens ten onrechte als juist worden geclassificeerd door de programmatuur of websites ongeautoriseerd toegang verlenen.
– Stoppen en uitvallen van operationele processen; niet goed uitgeteste programmatuur kan (geoorloofde) condities tegenkomen

TABEL 3

Aandachtspunten / aspecten	Beschikbaarheid	Exclusiviteit	Integriteit
Hardware	- Planning van ontwikkeling, test en overdracht	- Informatie over interne infrastructuur - Toegang tot interne infrastructuur - Communicatie met third party	- Compatibiliteit ontwikkelings-, test- en productieomgeving
Software	- Planning van ontwikkeling - Onderhoudsgarantie - Ondersteuning: welke, wanneer - Voortbestaan van leverancier	- Kennis van interne bedrijfsprocessen - Kennis van ontwikkelde programmatuur - Copyright	- Compatibiliteit met andere software - Kwaliteitsafspraken - Testtraject - Garantie-afspraken
Gegevens	- Testgegevens: welke, wanneer - Rapportage veiligheidsincidenten	- Communicatie met third party	- Kwaliteitscontrole op ontwikkeltraject - Controle op naleving afspraken

Aandachtspunten bij uitbesteding van systeemontwikkeling.

waar de code niet op berekend is, waardoor het programma in de meeste gevallen zal stoppen.
– Onvoldoende autorisatie; als de geprogrammeerde controles door niet-geautoriseerde personen kunnen worden uitgevoerd, ontstaan ongewenste situaties waardoor frauduleus handelen mogelijk wordt.

De algemene aandachtspunten bij het uitbesteden van systeemontwikkeltrajecten staan samengevat in tabel 3.

6.2 ONVOLDOENDE DESKUNDIGHEID

Het ontwikkelen van systemen stelt hoge eisen aan de deskundigheid van de systeembouwers. Deskundigheid op zowel het gebied van specifieke ontwikkelmethodieken of computertalen als op het vakgebied waarvoor een systeem ontwikkeld wordt, speelt een rol. Zonder gevoel voor de processen die zich bijvoorbeeld in de financiële wereld afspelen zal het ontwerpen van een systeem voor dat vakgebied, puur op basis van specificaties, geen bevredigend resultaat hebben.
Systeemontwikkeling houdt niet altijd compleet maatwerk in. De gewenste functionaliteit wordt vaak ingevuld met programmatuur van de plank, ook wel Commercially Of The Shelf (COTS) genoemd. Van deze programmatuur is niet altijd bekend aan welke betrouwbaarheidseisen deze voldoet. Dit vergt extra aandacht in het test- en acceptatietraject.
De systeemontwikkelaars hebben uit hoofde van hun functie in veel gevallen kennis van gevoelige bedrijfsinformatie. Zeker nu steeds meer systemen ontwikkeld worden die primaire taken van een bedrijf uitvoeren, is vertrouwelijke omgang met deze kennis van groot belang. Te denken valt aan ERP-systemen waarin bedrijfsinformatie als prijsstelling, winstmarge en salarisschalen zijn vastgelegd.

6.2.1 Normen en maatregelen

De basisnorm luidt:
– Het personeel dient goed opgeleid te zijn in de betreffende ontwikkelmethodieken en is tot een niveau gescreend waarbij gewaarborgd kan worden dat vertrouwelijke bedrijfsinformatie niet wordt verspreid.

Als belangrijke maatregelen tegen onvoldoende deskundigheid van het ICT-personeel kunnen worden genoemd:
– Er is nagegaan op welke wijze de serviceleverancier (insourced partij) zijn personeel selecteert.

– Er bestaan garanties dat het personeel vertrouwelijk omgaat met de informatie van de organisatie.

6.3 ONGESCHIKTE METHODE

Aan de diverse ontwikkelmethodieken kleven specifieke risico's. De huidige methodieken kunnen in de onderstaande drie groepen worden onderscheiden:

– Functionele aanpak. De te bouwen functionaliteit wordt net zo lang opgesplitst in deelfuncties tot elementaire bouwsteentjes ontstaan, die vervolgens geprogrammeerd kunnen worden. De risico's hiervan zijn uitlekken van vertrouwelijke informatie omdat het gehele traject lang duurt, en het verlagen van kwaliteitsaspecten zoals robuustheid, waardoor de beschikbaarheid van het systeem minder zou kunnen zijn dan verwacht.
– Objectgeoriënteerde aanpak. Deze aanpak gaat veel meer uit van een gegevensmodel en bouwt containers (objecten) waarin met gegevens gemanipuleerd wordt (gedrag van het object). Het ontwerpen van het gegevensmodel en de daarop aansluitende objecten is hier elementair. Het grootste risico hierbij is het niet voldoende aandacht schenken aan een correcte abstractie (gegevensmodel inclusief gedragsmodellering), waardoor een onjuiste objectklasse ontstaat. Behalve dat hierdoor waarschijnlijk de gewenste functionaliteit niet wordt geleverd, kunnen ook fouten ten aanzien van de toegangsbeveiliging en mogelijk ten aanzien van de robuustheid ontstaan.Met betrekking tot complexiteit is er een wezenlijk verschil tussen de functionele decompositiemethode en de objectgeoriënteerde aanpak. Fouten of niet optimale keuzes die gemaakt worden met functionele decompositie kunnen nog vrij eenvoudig worden hersteld, zelfs op het allerlaatste moment. Het samenstellen van objecten en klassen van objecten is een proces dat alleen op basis van kennis en ervaring met succes kan worden uitgevoerd. Een verkeerd gekozen objectklasse kan op het eind niet eenvoudig hersteld worden.
– Rapid Application Development (RAD) en hiervan afgeleide methodieken. Hier wordt gestart met het ontwerpen en coderen van de gebruikersinterface. Dit wordt ook wel prototyping of de bottom-upbenadering genoemd. Dit om de gebruikers vanaf het begin te laten participeren in het project en te laten meebepalen welke functionaliteit er geboden moet worden en hoe deze functionaliteit naar de gebruikers toe ontsloten moet worden. In deze methode wordt gebruikgemaakt van zogenaamde timeboxes. Software wordt op een vastgestelde datum opgeleverd. Hoewel

men afspraken maakt over de op te leveren functionaliteit is deze variabel en ondergeschikt aan de tijd in een timebox. Het grootste risico van deze methode is de gebruikersfocus. Omdat het gehele ontwerp in zeer sterke mate wordt bepaald in samenwerking met de gebruikers van het systeem kunnen de andere kwaliteitsaspecten, zoals omschreven in ISO 9126, hieronder lijden. Immers, als er minder functionaliteit geleverd kan worden dan is afgesproken, zal men geneigd zijn die functionaliteit die opgemerkt wordt door de gebruikers voorrang te geven boven aspecten die voor de gebruikers minder direct gezien worden. Met name de beveiligingsaspecten worden hier vaak de dupe van.

6.3.1 Normen en maatregelen

Voor de keuze van de geschiktste methode is geen algemeen geldende normering te geven.
Als belangrijke maatregelen tegen het maken van een verkeerde keuze van de ontwikkelmethodiek kunnen worden genoemd:

- Er is gekozen voor een ontwikkelmethodiek die past bij het te ontwikkelen systeem.
- Er is gekozen voor een ontwikkelmethodiek waarmee de serviceleverancier ervaring heeft.
- Er is gekozen voor een ontwikkelmethodiek die een optimale inbreng en controle van de eigen organisatie waarborgt.
- De broncode is in een standaard computertaal. Bij failliet gaan van bijvoorbeeld de leverancier van de I-Case-tool kan met behulp van deze broncode gebruikgemaakt worden van een andere ontwikkeltool.

6.4 ORGANISATORISCHE ONGESCHIKTHEID

Het laten ontwikkelen van een systeem is geen eenmalige zaak. Systemen zijn voortdurend aan wijzigingen onderhevig. Denk daarbij aan de voortdurende wetswijzigingen, de wijzigingen die door de infrastructuur worden veroorzaakt, enzovoort.
Nadat een systeem in gebruik wordt gesteld, dient dit onderhouden te worden door de eigen organisatie, de organisatie die het systeem ontwikkeld heeft, of een andere organisatie.
Om de continuïteit van het systeem te waarborgen dienen er afspraken te worden gemaakt met de ontwikkelende partij. Denk hierbij aan auteursrecht, persoonsrecht, enzovoort. Tevens wordt er voortdurend informatie uitgewisseld tussen de opdrachtgever en de serviceleverancier. Het op een juiste (veilige) wijze omgaan met deze informatie-uitwisseling wordt vaak veronachtzaamd.
Tijdens het ontwikkelen van het systeem, maar zeker in de onder-

houdsfase, kunnen zich beveiligingsincidenten voordoen bij de leverancier. Het is zaak goede afspraken te maken met de leverancier over de wijze van melden van deze incidenten.

6.4.1 Normen en maatregelen

Als basisnormen gelden:

- De systeemontwikkelorganisatie dient adequate beheersmaatregelen te treffen om bedrijfsinformatie vertrouwelijk te kunnen behandelen.
- De systeemontwikkelorganisatie dient minimaal gecertificeerd te zijn op CMM-niveau 2.

Als belangrijke basismaatregelen tegen organisatorische geschiktheid kunnen worden genoemd:

- Er zijn garanties over de beschikbaarheid van informatie, mocht de serviceleverancier overgenomen worden of failliet gaan.
- De applicaties, de bijbehorende documentatie en de wijzigingen daarop zijn door middel van escrow bij een derde partij veiliggesteld. Er zijn aanvullende afspraken gemaakt over eigendomsrecht van de broncode en basisontwerpen.
- De informatie-uitwisseling (bijvoorbeeld netwerkverbindingen) tussen systemen bij de serviceleverancier en de organisatie vindt beschermd plaats.
- Er bestaan afspraken over de wijze van melding van beveiligingsincidenten bij de serviceleverancier.
- Er zijn duidelijke bevoegdheden en verantwoordelijkheden van de opdrachtgever afgesproken, met aanvullende afspraken over rapportagelijnen.
- Er bestaan afspraken over een regelmatige controle door experts van de door de serviceleverancier getroffen informatiebeveiligingsmaatregelen en de gestelde beveiligingseisen.
- Er zijn afspraken gemaakt over de (wettelijke) aansprakelijkheid.

6.5 ONVOLDOENDE AUTORISATIEMOGELIJKHEDEN

Een systeem wordt in de meeste gevallen gebouwd voor een specifiek organisatieonderdeel. De vigerende procedures en autorisaties moeten dan, voorzover van toepassing, onderdeel zijn van het te bouwen systeem. Daar waar het systeem niet aan de eisen kan voldoen, moeten besloten worden of het risico kan worden geaccepteerd of dat de organisatie (deels) moet worden aangepast. Bij het introduceren van een ERP-systeem is dit laatste een gangbare activiteit.

In de praktijk blijkt dat hier wel sturing aan gegeven wordt, maar dat de specifieke beveiligingsaspecten niet duidelijk worden besproken, met als gevolg dat te veel personen meer bevoegdheden nodig hebben om het systeem te kunnen gebruiken dan noodzakelijk is. Daardoor worden de op papier vastgelegde bevoegdheden niet meer weerspiegeld in het gebouwde systeem.
Buiten deze gebruikersaspecten zijn er specifieke audit-aspecten die een rol spelen bij systeemontwikkeling. Het moet mogelijk zijn om door een derde te laten controleren of het systeem correct functioneert.

6.5.1 Normen en maatregelen

Als basisnorm geldt:

– Het gebruik van systemen dient een goede afspiegeling te zijn van het organisatieonderdeel. De eisen ten aanzien van de auditability moeten voldoen aan de voor de organisatie geldende normen.

Belangrijke basismaatregelen tegen onvoldoende autorisatiemogelijkheden zijn:

– Het systeem moet gebouwd worden met adequate integriteits- en security controls.
– Het netwerk van de serviceverlener dient adequaat beveiligd te zijn tegen ongeautoriseerde toegang van buitenaf.

6.6 ONVOLDOENDE SOFTWAREBEHEER EN -DISTRIBUTIE

Een systeem bestaat uit vele componenten. Het adequaat beheren van al deze componenten, de versies daarvan en de benodigde omgevingscomponenten (zoals de versie van het benodigde besturingssysteem, de versie van de database, de internetbrowser, de versie van het gebruikte ontwikkelgereedschap) is een complexe taak die goed moet worden uitgevoerd om garanties te kunnen geven voor het op te leveren systeem.
Bij het opleveren van een systeem spelen behalve het systeem zelf ook andere zaken een rol. De belangrijkste zijn:

– conversie, bijvoorbeeld het wijzigen van een aangepast gegevensmodel in de database, het wijzigen van een bestandsstructuur van de ene versie tekstverwerker naar de andere;
– het installeerbaar maken van het product op van tevoren bekend gestelde platforms (MS-Windows 95/98/NT, Linux, Apple OS);
– het virusvrij opleveren van de softwarecomponenten.

De locatie waar de uiteindelijk op te leveren systeemcomponenten worden bewaard, is de achilleshiel van deze activiteit. Deze locatie dient dan ook goed beveiligd te zijn tegen ongeautoriseerde toegang.

6.6.1 Normen en maatregelen

De basisnorm is:

– Het softwarebeheer- en -distributieproces dient adequaat geregeld te zijn.

Belangrijke basismaatregelen tegen onvoldoende softwarebeheer en -distributie zijn:

– Het hergebruik en afstoten van gebruikte informatiemedia is veilig.
– De serviceverlener geeft garanties met betrekking tot de virusproblematiek.
– De leverancier van het ontwikkelgereedschap geeft garanties voor de correcte werking van de gegenereerde programmatuur in relatie tot het gebruikte besturingssysteem en de versie daarvan.
– De locatie waar de systeemcomponenten zijn opgeslagen wordt goed beveiligd.

6.7 ONVOLDOENDE STURING DOOR DE OPDRACHTGEVER

Het ontwikkelen van een systeem bestaat uit meer dan het maken van adequate functionele en technische specificaties. Er zal tevens aandacht geschonken moeten worden aan de interne organisatie. Immers, de organisatie heeft bepaalde vastgelegde werkwijzen die men geautomatiseerd wil laten ondersteunen. Men moet zich realiseren dat de kwaliteit van deze werkwijzen rechtstreeks van invloed is op de kwaliteit van het te bouwen systeem. Als er onduidelijkheden zijn in de werkwijzen, dan komen deze in nog grotere mate terug in het geautomatiseerde systeem. Niet alle werkprocessen en -procedures zijn te automatiseren.
Het falen van automatiseringsprojecten is niet alleen te wijten aan onvoldoende kwaliteit van specificaties, maar veelal ook aan de onmogelijkheid de organisatorische leemtes adequaat te verbeteren. Systeemontwikkeling gaat vaak gepaard met herinrichting van bedrijfsprocessen. Al in een vroeg stadium van specificatie dient erop gelet te worden dat de kwaliteit van de autorisatiemethode met de nieuwe programmatuur gehandhaafd blijft. Bij specificaties moet duidelijk zijn hoe de nieuwe of aangepaste autorisatiemethode eruit ziet en hoe het nieuw te ontwikkelen systeem dat ondersteunt

(functiescheiding en autorisaties, fiattering van transacties, enzovoort). Tevens dient de vereiste interne controle vertaald te worden naar specificaties waaraan het nieuwe systeem dient te voldoen. Bekend moet zijn welke controles in de programmatuur ingebouwd moeten worden.

6.7.1 Normen en maatregelen

Als basisnorm geldt:

– De opdrachtgever dient adequate sturing te geven, ook de benodigde interne sturing aan de organisatie waar het geautomatiseerde systeem voor bedoeld is.

Als basismaatregelen tegen onvoldoende sturing van de opdrachtgever kunnen worden genoemd:

– Risico's moeten gedurende het gehele ontwikkelingstraject worden geanalyseerd (en niet achteraf).
– Bij het op te leveren systeem dient adequate, correcte documentatie te worden opgeleverd.
– Bij ontwikkeling van nieuwe systemen moet de bestaande wet- en regelgeving gehandhaafd blijven. Onderzocht moet worden welke regelgeving van toepassing is op de nieuwe programmatuur en welke specificaties daaruit voortvloeien. Te denken valt aan: het interne beveiligingsbeleid en interne beveiligingsrichtlijnen, de Auteurswet, de Wet op Bescherming Persoonsgegevens en de comptabiliteitswet.

6.8 ONVOLDOENDE DUIDELIJKE SPECIFICATIES

Het duidelijk en eenduidig specificeren van de eisen waaraan een systeem moet voldoen, is niet eenvoudig. Veel projecten gaan op dit punt mank. Het meenemen van beveiligingseisen in de specificaties wordt nog niet veel gedaan. Toch ligt hier een belangrijk winstpunt, want het bouwen van systemen waarin de beveiliging al in het basisontwerp is meegenomen, levert een beter product op dan systemen waar de beveiligingseisen later worden ingebouwd.
De huidige systeembouw is vaak een mix van maatwerk en het gebruik van standaard programmatuur (COTS). Het gebruik van deze maatwerkprogrammatuur vereist onderzoek of het product wel kan voldoen aan de beveiligingseisen. Dit is een extra aandachtspunt bij het opstellen van de specificaties.
De introductie van nieuwe programmatuur kan betekenen dat nieuwe technologieën in het bedrijf worden geïntroduceerd, waaraan nieuwe risico's zijn verbonden (gebruik van internet of e-mail voor bedrijfskritische applicaties bijvoorbeeld). In de afweging over

het ontwikkelen van een dergelijk product moet worden meegenomen of dit een aanvaardbaar risico is.

6.8.1 Normen en maatregelen

De basisnormen zijn:

- De specificaties waaraan het te ontwikkelen systeem moet voldoen dienen afgestemd te zijn met de systeembouwer en met de gebruikersorganisatie.
- De specificaties dienen voldoende scherp gedefinieerd te zijn om een systeem mee te kunnen bouwen.

Basismaatregelen tegen onvoldoende duidelijke specificaties zijn:

- Bij uitbesteding dient de leverancier op de hoogte te zijn van algemene richtlijnen ten aanzien van informatiebeveiliging die binnen de organisatie gelden.
- De gebruikte programmatuur, ook de commerciële producten, moet voldoen aan de gestelde beveiligingseisen.
- De voor de applicatie benodigde (nieuwe) technieken mogen geen extra risico's met zich meebrengen of deze risico's moeten aanvaardbaar zijn.

6.9 AANDACHTSPUNTEN IN DE SLA

De kwaliteit van de systeemontwikkeling wordt bepaald door zowel de wijze waarop het ontwikkelproces wordt beheerst, als de wijze waarop met de klant wordt gecommuniceerd. Met name een goede communicatie tussen klant en leverancier gedurende het gehele ontwikkelproces is van doorslaggevend belang voor de kwaliteit van het uiteindelijk op te leveren product. Aan het communicatieaspect zal dan ook relatief veel aandacht besteed moeten worden.
Het gebruik van SLA's is vooral aan de orde bij een meer permanente relatie tussen klant en leverancier, zoals bij dienstverlening vanuit het rekencentrum. Omdat een systeemontwikkeltraject vaak een eenmalig traject is, wordt aan de structurering daarvan vaak onvoldoende aandacht geschonken. Er wordt van uitgegaan dat de keuze voor (de juiste) set specifieke ontwikkelmethoden en -tools voldoende is, waarbij voorbijgegaan wordt aan de specifieke beperkingen daarvan.
Net als voor elk ICT-object zijn ook voor het systeemontwikkeltraject een goede projectstructuur en communicatie van essentieel belang. Voor de inrichting hiervan is het gebruik van SLA's zeer wenselijk, waarbij uiteraard zo veel mogelijk gebruikgemaakt kan worden van ontwikkelmethodieken en tools die de beste ondersteuning bieden in de betreffende situatie.

Onvoldoende deskundigheid Het ontwikkelen van nieuwe software is vaak een complex en kennisintensief traject waarbij de menselijke inbreng een grote rol speelt. De deskundigheid en betrokkenheid van de projectmedewerkers is dan ook van doorslaggevend belang voor de kwaliteit van het uiteindelijk op te leveren product. Dit geldt natuurlijk ook voor andere menselijke gedragingen, zoals gedisciplineerdheid en integriteit van de medewerkers, met name als de werkzaamheden op de locatie van de opdrachtgever worden uitgevoerd.
Eisen in de SLA betreffen:
- deskundigheid;
- algemene gedragsregels;
- geheimhouding;
- toezicht op functioneren;
- rapportage over functioneren.

Ongeschikte methode De ontwikkeling van software is een complex en risicovol proces. Om deze risico's te ondervangen is een groot aantal methoden en technieken ontwikkeld. In de praktijk is echter gebleken dat geen enkele hiervan ook alle mogelijke risico's volledig kan afdekken. Elke methode heeft dan ook sterke en zwakke punten, waardoor steeds slechts een deel van ontwikkelproblematiek kan worden gedekt. De keuze van de juiste methodiek en tools is dus in hoge mate bepalend voor de verdere structurering en het succes van het ontwikkeltraject.
Eisen in de SLA betreffen:
- gemotiveerde keuze van de methodiek en mogelijke risico's;
- aantoonbare deskundigheid op het gebied van de methodiek;
- duidelijke vastlegging van wederzijdse invulling van de methodiek;
- omschrijving van de op te leveren producten;
- gemotiveerde keuze van de tools;
- vastlegging van de keuze en gebruik van methoden en tools;
- mogelijkheden voor periodieke evaluatie of bijstelling.

Organisatorische ongeschiktheid Een systeemontwikkeltraject bestaat niet alleen uit het bouwen van een nieuw informatiesysteem door de systeemontwikkelaar, maar is tevens het begin van een reeks van vaak ingrijpende technische en organisatorische veranderingen binnen de organisatie van de opdrachtgever. Het ordelijke verloop van een ontwikkelproces vereist dan ook een deugdelijke structurering van de interne organisatie, niet alleen bij de ontwikkelaar, maar ook bij de opdrachtgever. Tevens is het van groot belang dat gedurende het gehele proces een optimale communicatie bestaat tussen beide partij-

en, die eveneens in de wederzijdse organisatiestructuren dient te zijn geworteld.
Steeds vaker wordt verwezen naar het Capability Maturity Model (CMM), dat afhankelijk van de 'evolutiefase' waarin een organisatie zich bevindt, een aantal criteria stelt. Gewoonlijk wordt uitgegaan van niveau 2, waarbij eisen worden gesteld inzake de structuur, de uitvoering, de meting en terugkoppeling van activiteiten. Deze activiteiten zijn in een aantal Key Process Area's (KPA's) samengevoegd. Vrij vertaald naar de door ITIL gehanteerde begrippen, zijn de volgende beheersprocessen van belang: change management, configuration management, service level management, helpdesk en incident management. Aanvullend wordt in CMM op niveau 2 nadrukkelijk aandacht besteed aan de aansturing van eventuele onderaannemers (door subcontract management) en de borging van de verschillende beheerprocessen (door service quality assurance).
Op de relatie tussen de systeemontwikkelaar en diens opdrachtgever zijn ook normen van een hoger niveau van toepassing, zoals juridische normen. Te denken valt aan eigendom van de ontwikkelde software, in depot geven van de broncode bij een derde (escrow), privacyaspecten en dergelijke.
Eisen in de SLA betreffen:
- duidelijk gedefinieerde beheerprocessen;
- voldoende functioneren van beheerprocessen;
- duidelijk vastgelegde communicatiepunten;
- voldoende invulling van juridische normen;
- rapportage per beheerproces;
- audit van de kwaliteit van beheerprocessen en de integriteit van de rapportages.

Onvoldoende autorisatiemogelijkheden Het autorisatiemechanisme heeft ten doel om de bestaande scheiding in functies en omgevingen te waarborgen. Binnen de organisatie van de systeemontwikkelaar is het autorisatiemechanisme van groot belang om niet alleen de ontwikkel-, test- en productieomgevingen van elkaar te scheiden, maar ook de verschillende ontwikkelomgevingen onderling. Zeker bij een grotere ontwikkelorganisatie zullen voor verschillende klanten meer ontwikkeltrajecten tegelijkertijd worden uitgevoerd, die onderling strikt gescheiden dienen te blijven. Uiteraard dient ook de informatie die door de klant ten behoeve van het ontwikkeltraject wordt verstrekt, vertrouwelijk te worden behandeld.
Vanuit het oogpunt van functiescheiding zal de ontwikkelaar in geen geval toegang mogen krijgen tot de productieomgeving van de opdrachtgever. Hiermee wordt voorkomen dat de ontwikkelaar ongestructureerde en ongedocumenteerde wijzigingen kan aanbren-

gen. Ook het bestaan van eventuele 'achterdeurtjes' zal voorkomen moeten worden.
Vanuit privacyoogpunt zullen persoongegevens slechts beperkt en met grote terughoudendheid mogen worden gebruikt. Het is in ieder geval onwenselijk dat persoongegevens in een andere dan binnen de reguliere productieomgeving worden gewerkt. Het gebruik van actuele persoonsgegevens in een ontwikkel- en testomgeving is dan ook niet wenselijk. Zelfs het gebruik van 'onherkenbaar gemaakte' persoonsgegevens in bijvoorbeeld een testsituatie zal slecht beperkt en onder strikte voorwaarden mogen geschieden.
Eisen in de SLA betreffen:
- een duidelijk autorisatiemechanisme bij de ontwikkelaar;
- geheimhouding van verstrekte informatie;
- afscherming van andere projecten;
- geen toegang tot de productieomgeving van de opdrachtgever voor de ontwikkelaar;
- geen gebruik van actuele persoonsgegevens;
- overdracht via change management;
- overdracht na formele test- en acceptatieprocedure;
- audit van bestaan en werking van het autorisatiemechanisme.

Onvoldoende softwarebeheer en -distributie De ontwikkeling van softwaresystemen is vaak een complex proces waarbij een groot aantal mensen gelijktijdig aan verschillende onderdelen daarvan werken. Ook zal een bepaalde softwaremodule niet in één keer worden ontwikkeld, maar eerst nog een aantal keren worden bewerkt voordat het gewenste eindresultaat is bereikt. Ook daarna zullen onder invloed van de verschillende test- en acceptatiefases opnieuw vele wijzigingen plaats vinden. Om ervoor te zorgen dat er steeds met de juiste en meest actuele versie van de software wordt gewerkt, is een stringent versiebeheer noodzakelijk. Tevens zal met behulp van het versiebeheer inzichtelijk gemaakt kunnen worden of een softwaremodule ook daadwerkelijk alle stappen en kwaliteitscontroles heeft doorlopen.
Behalve in de status van de te ontwikkelen software is het ook belangrijk dat inzicht bestaat in de versie van de softwaretools en de technische infrastructuur die bij de systeemontwikkeling is gebruikt. Deze kunnen van directe invloed zijn op de kwaliteit van de op te leveren software. Zeker als achteraf, bijvoorbeeld bij het testen, blijkt dat bepaalde versies van tools of de technische infrastructuur tot fouten hebben geleid, moet men kunnen controleren welke andere softwaremodules daar mogelijk ook problemen mee kunnen krijgen. De gebruikte tools en infrastructuur dienen op voorhand zo veel mogelijk vrij te zijn van fouten of tekortkomingen. Zo mogelijk

wordt van de leverancier een bepaalde minimale kwaliteitsgarantie verlangd.
Eisen in de SLA betreffen:
- eenduidig versiebeheer;
- inzicht in de gebruikte tools en versies daarvan;
- inzicht in de samenstelling en versies van de gebruikte technische infrastructuur;
- melding bij problemen met bepaalde versies of configuraties;
- kwaliteitsgarantie voor de gebruikte tools en infrastructuur;
- periodieke audit van het functioneren van softwarebeheer en -distributie.

Onvoldoende sturing door de opdrachtgever Essentieel voor de succesvolle voltooiing van het systeemontwikkeltraject is een goede communicatie tussen klant en opdrachtgever. Voorafgaand aan het ontwikkeltraject vindt eerst een nauwkeurige en gedetailleerde vastlegging plaats van de gewenste eigenschappen van de te ontwikkelen software. Dit kan echter niet meer zijn dan een eerste stap. Door de duur en de complexiteit van het ontwikkelingstraject zullen zich ook tijdens de uitvoering van het project vragen voordoen. Ook bestaat altijd de mogelijkheid dat gedurende het ontwikkelingstraject eerder vastgelegde uitgangspunten en/of randvoorwaarden alsnog moeten worden bijgesteld.
Het omgaan met deze voortdurende veranderingen zonder in een kunstmatige bevriezing van de werkelijkheid te vervallen, is een van de grote uitdagingen en daarmee ook een van de kritieke succesfactoren van elk groot ontwikkelingstraject. Hieraan het hoofd te bieden vergt niet alleen een goede communicatie maar ook een aanzienlijk commitment van zowel de opdrachtgever als de opdrachtnemer.
In geval van dreigende of daadwerkelijke conflicten is het verstandig om op voorhand afspraken te hebben gemaakt over mogelijk geschillenbeslechting. Met name een arbitrageprocedure is gezien de relatieve snelheid en deskundigheid te verkiezen boven een reguliere juridische procedure. Verdere zuiver juridische maatregelen ter beslechting van conflicten, zoals aansprakelijkheidsstelling, dwangsommen en toepasselijk recht, zullen merendeels in de overeenkomst zelf zijn opgenomen en niet in de SLA.
Eisen in de SLA betreffen:
- duidelijke ontwikkelspecificaties;
- procedures voor overleg en communicatie;
- waarborging van de prioriteit van functionele aspecten boven technische aspecten;
- afspraken over conflictbemiddeling en arbitrage;
- verdere juridische maatregelen.

Onvoldoende duidelijke specificaties Bij het formuleren van de functionele specificaties van een nieuw te ontwikkelen softwaresysteem dient tevens terdege rekening gehouden te worden met de gewenste beveiligingseisen. Deze dienen nauw aan te sluiten bij het binnen de organisatie gangbare niveau van beveiliging.
Indien de systeemontwikkeling zal leiden tot de introductie van geheel nieuwe technologieën binnen de organisatie, zal daar ook in het bestaande beveiligingsbeleid aandacht aan besteed moeten worden. Dit kan eventueel leiden tot aanvullende beveiligingsmaatregelen, waarop bij de specificatie van de ontwerpeisen geanticipeerd moet worden.
Om de daadwerkelijke doorvoering van specifieke beveiligingsmaatregelen af te dwingen en om de kwaliteit van de getroffen beveiligingsmaatregelen te kunnen vaststellen, moeten deze terdege getest worden. Zo mogelijk zal al in de bouwfase duidelijk moeten zijn welke aspecten op welke wijze getest zullen worden. Bij gebleken tekortkomingen zullen de getroffen beveiligingsmaatregelen alsnog op niveau gebracht moeten worden.
Eisen in de SLA betreffen:
- duidelijke beveiligingsspecificaties;
- vooraf duidelijkheid over de te hanteren testnormen;
- aanpassingen bij gebleken tekortkomingen.

7 Conclusies

Om verschillende redenen is het beheer van de ICT-middelen bij vele bedrijven een punt van blijvende zorg. De keuze voor uitbesteding kan een effectief instrument zijn om tot een aanzienlijke verbetering van de kwaliteit van de ICT-dienstverlening te komen tegen een inzichtelijker en waarschijnlijk ook lager kostenniveau. Zodra ervoor wordt gekozen om (een deel van) de ICT-dienstverlening uit te besteden, ontstaat tussen de klant en de leverancier een zogenoemde uitbestedingsrelatie. Daarbij behoudt de klant de eindverantwoordelijkheid voor de ICT-dienstverlening en stelt hij de normen op waaraan de dienstverlening zal moeten voldoen. Deze normen worden op hoofdlijnen vastgelegd in de uitbestedingsovereenkomst en vervolgens nader gespecificeerd in de onderliggende Service Level Agreements (SLA's). Om een goede uitvoering van hetgeen is afgesproken te bewaken en een goede communicatie tussen partijen te waarborgen, is het van belang dat er aanvullende organisatorische maatregelen getroffen worden om de uitbestedingsrelatie ook daadwerkelijk in te vullen. Hierbij wordt in toenemende mate gebruikgemaakt worden van de verworvenheden van nieuwe beheersinzichten, zoals de ITIL-methodiek.

Het daadwerkelijke proces van uitbesteding is vaak een diepgaand veranderingsproces met grote gevolgen voor de organisatie van de klant. Om de hierdoor ontstane onrust zo veel mogelijk te beperken wordt ernaar gestreefd een dergelijk proces zo snel mogelijk af te handelen. Daarnaast blijkt binnen het uit te besteden ICT-proces vaak een groot aantal zaken niet of onvoldoende te zijn geregeld. In een dergelijke hectiek kan het voorkomen dat belangrijke zaken, zoals beveiligingsaspecten, niet de aandacht krijgen die deze verdienen.
In deze studie is een inventarisatie gemaakt van de belangrijkste beveiligingsaspecten die bij uitbesteding aan de orde zouden moeten komen. Omdat het begrip beveiliging een groot aantal aspecten omvat, is er voor gekozen om sterk gestructureerd en modelmatig te werk te gaan. Daarbij is als eerste stap het gehele proces van ICT-dienstverlening verdeeld in zogenaamde ICT-objecten, die elk een min of meer zelfstandig onderdeel van uitbesteding kunnen vormen.

Om de beveiligingsrisico's binnen elk ICT-object zo volledig mogelijk te beschrijven is vervolgens een overzicht gemaakt van de belangrijkste bedreigingen en de daartegen te nemen maatregelen. Bij de totstandkoming van elke uitbestedingsrelatie zal een inventarisatie gemaakt moeten worden van de bestaande risico's en de noodzakelijke beveiligingsmaatregelen. De omvang en diepgang van deze maatregelen wordt gedicteerd door de beveiligingsnormen, die dan ook een belangrijk onderdeel vormen van de SLA en – al dan niet in een geabstraheerde vorm – het uitbestedingscontract.

Model en matrix Om ervoor te zorgen dat tijdens het hectische proces van uitbesteding alle belangrijke beveiligingsaspecten op een gemakkelijke en inzichtelijke kunnen worden geadresseerd, is gekozen voor het gebruik van de volgende ICT-objecten:
- uitbesteding van rekencentrumprocessen;
- uitbesteding van netwerkprocessen;
- uitbesteding van werkplekprocessen;
- uitbesteding van systeemontwikkelingsprocessen.

Afhankelijk van de concrete situatie van uitbesteding kan steeds een keuze worden gemaakt voor het gebruik van het meest toepasselijke ICT-object.

Ten aanzien van de bedreigingen die binnen een bepaald ICT-object zijn te onderkennen, is een onderverdeling gemaakt naar de aard van de verschillende bedreigingen, te weten;
- menselijk falen;
- systeemtechnisch falen;
- infrastructureel falen;
- organisatorisch falen.

Hierbij zij nog aangetekend dat met name het organisatorische falen een aanzienlijke hoeveelheid aan complexe en hardnekkige problemen kan veroorzaken.

Uitgaande van het geschetste model is een matrix opgesteld met daarin een overzicht van de belangrijkste bedreigingen per ICT-object, alsmede de bijbehorende compenserende beveiligingsmaatregelen die in een SLA opgenomen dienen te zijn (zie tabel 4). Voorzover van toepassing is per beveiligingsaspect tevens een verwijzing naar de Code voor Informatievoorziening opgenomen. In de laatste kolom is ten slotte een indicatie gegeven van het onderdeel van de beheersorganisatie waar de verantwoordelijkheid voor de

uitvoering van de betreffende beveiligingsmaatregelen kan worden belegd.
Zowel klant als leverancier van uitbestedingsdiensten kan aan de hand van de matrix op eenvoudige wijze vaststellen welke beveiligingsaspecten er in de SLA dienen te worden opgenomen.

TABEL 4

Nader uitgewerkt in de hoofdstukken:				Bedreiging:	
3 rc	4 nb	5 wp	6 so		
				Menselijk falen	
				Onoplettendheid	
			X	Ondeskundigheid	
				Onvoldoende ondersteuning	
		X		Ongeoorloofd gebruik van systemen en programma's	
X	X	X	X	Ongeoorloofd gebruik van gegevens en output	
	X			Ongeoorloofd gebruik van verbindingen	
			X	Opzettelijke inbreuk (intern)	
X	X	X		Misbruik/diefstal/inbraak (extern)	
				Systeemtechnisch falen	
X				Aantasting integriteit functioneren	
X	X		X	Aantasting integriteit systemen/componenten	
X				Ongeautoriseerde bewerkingen	
X		X	X	Verlies opgeslagen gegevens	
	X			Verlies getransporteerde gegevens	
	X			Teruglopen verwerkingssnelheid	
X		X		Niet beschikbaar zijn	

	Mogelijke maatregel(en):	Link naar code voor informatiebeveiliging	Aandachtspunt voor:
	Verduidelijken werkzaamheden Collegiale/interne controle		Manager
	Opleiden		Manager / PZ
	Duidelijke werkinstructies Helpdesk informatie		Manager Helpdesk
	Toegangsbeveiliging Controle op geoorloofdheid programma's Registratie en evaluatie gebruik	Hoofdstuk 9, 12.1.2, 12.1.5, 8.4.2, 9.7.1, 9.7.2	Autorisatiebeheer Werkplekbeheer Functioneel beheer
	Classificatie van gegevens Registratie en evaluatie gebruik Toegangsbeveiliging	Hoofdstuk 5, 8.4.2, 8.6.3, 9.7.1, 12.1.4, Hoofdstuk 9	Autorisatiebeheer Werkplekbeheer Functioneel beheer
	Afscherming van (deel van) netwerk Toegangsbeveiliging	8.5.1, Hoofdstuk 9	Autorisatiebeheer Netwerkbeheer
	Toegangsbeveiliging Controle op gebruik illegale software Virusdetectie Registratie en evaluatie gebruik Integriteitscontrole personeel	Hoofdstuk 9, 12.1.2, 8.3.1, 8.4.2, 9.7.1, 6.1.2	Autorisatiebeheer Werkplekbeheer Manager PZ
	Fysieke en logische (netwerk)toegangsbeveiliging Gegevensversleuteling Diefstalpreventie-instructies	Hoofdstuk 7, Hoofdstuk 9 (9.4.9), 10.3.2, 6.2.1	Autorisatiebeheer Werkplekbeheer Manager
	Productiesystemen vrij van ontwikkeltools Standaard systemen en versies Standaard configuratie-instellingen	8.1.5, 12.1.2	Werkplekbeheer Configuratiebeheer
	Ingebouwde integriteitschecks Genereren van statusmeldingen	10.2.2	Functioneel beheer (systeem of netwerk)
	Toegangsbeveiliging Registratie en evaluatie gebruik	Hoofdstuk 9, 8.4.2, 9.7.1	Autorisatiebeheer Applicatiebeheer
	Voorzieningen redundante opslag Direct signaleren gegevensverlies Back-up en recovery	8.4.1, 8.6.3, 8.4.1	Werkplekbeheer Functioneel (systeem)beheer
	Consistentiecontrole en ontvangstbevestiging Gebruik correctief communicatieprotocol	8.7.2, 8.7.4, 10.2.3	Netwerkbeheer
	Signaleren: automatische detectie en tuning Oplossen structurele problemen (kwaliteit/capaciteit)	8.2.1, 10.2.2	Capaciteitsbeheer Probleembeheer
	Signaleren en escaleren uitval Calamiteitenprocedure Recoveryprocedure dan wel uitwijk	8.4.3, 11.1.1	Calamiteitenbeheer Probleembeheer Helpdesk

TABEL 4

Nader uitgewerkt in de hoofdstukken:				Bedreiging:	
3 rc	4 nb	5 wp	6 so		
				Infrastructureel falen	
×				Conditioneringproblemen (warmte, vocht)	
				Brand- of waterschade	
×				Elektromagnetische straling	
×				Stroomuitval of spanningsverschillen	
×		×		Toegangsbeveiliging	
				Organisatorisch falen	
×			×	Onvoldoende structuur	
			×	Onvoldoende communicatie	
×			×	Onvoldoende productiebeheer (of systeemontwikkelcapaciteit)	
×		×	×	Onvoldoende autorisatiebeheer	
		×		Onvoldoende werkplekbeheer	
×	×	×	×	Onvoldoende configuratiebeheer	
			×	Onvoldoende softwarebeheer en distributie	

	Mogelijke maatregel(en):	Link naar code voor informatiebeveiliging	Aandachtspunt voor:
	Detectiesystemen Dubbele airco	7.1.1, 7.1.3, 7.2.1	Gebouwbeheer Productiebeheer
	Detectie (water, rook, hitte) Automatische blussing Bouwkundige voorzieningen (opvang lekwater, brandmuren, etc)	7.1.1, 7.1.3, 7.2.1	Gebouwbeheer Productiebeheer Calamiteitenbeheer
	Bouwkundige voorzieningen (kooi van Faraday)	7.1.1, 7.1.3, 7.2.1	Gebouwbeheer
	UPS-systemen Uitschakelen niet-noodzakelijke apparatuur	7.2.2	Productiebeheer Calamiteitenbeheer Functioneel beheer
	Compartimentering Gebruik van fysiek toegangssysteem Bezoekersregeling	7.1.2, 7.1.4	Bewaking Autorisatiebeheer
	Beschrijving van processen en producten Opstellen normen en procedures Organigram Vaststellen functies, taken en bevoegdheden Planning-&-controlcycli Eigendomsrechtgegevens	Hoofdstuk 3 en 4	Manager
	Afspraken met gebruikers Rapportage en derdenonderzoek Duidelijke facturering Beschikbaarheid gegevens/documentatie		Servicebeheer
	Inzicht in taken, middelen en capaciteit Productieplanning Prioriteitstelling Geschiktheid systeemontwikkelmethodieken		Productiebeheer Servicebeheer
	Inzicht in functies en functiescheidingen Toekennen en beheren van autorisaties Controle	4.1.4, Hoofdstuk 9, 12.2.1	Autorisatiebeheer
	Inzicht in beschikbare middelen en capaciteit Prioriteitstelling	8.2.1	Werkplekbeheer
	Overzicht van alle configuratie-items en specifieke eigenschappen Versiebeheer en licentievoorwaarden	5.1.1	Configuratiebeheer
	Specifiek ingericht voor softwarecomponenten en releases; Virusvrij opleveren van software Conversie van gegevens Installatie en de-installatie programmatuur voor beoogd platform Garanties geschiktheid ontwikkelgereedschap tav beoogd platform	5.1.1	Software Control en Distributie

TABEL 4

Nader uitgewerkt in de hoofdstukken:				Bedreiging:	
3 rc	4 nb	5 wp	6 so		
X	X			Onvoldoende capaciteitsbeheer (incl. DASD)	
		X		Onvoldoende service helpdesk	
X	X			Onvoldoende wijzigingsbeheer	
X				Onvoldoende probleembeheer	
X			X	Onvoldoende calamiteitenbeheer	

Bedreigingen en mogelijke maatregelen.

	Mogelijke maatregel(en):	Link naar code voor informatiebeveiliging	Aandachtspunt voor:
	Vastlegging van maximale capaciteit Signaleren capaciteitsproblemen	8.2.1	Productiebeheer Helpdesk Probleembeheer
	Identificeren, classificeren en bewaken incidenten Prioriteitstelling Volledige registratie	6.3.1, 8.1.3	Helpdesk Probleembeheer Servicebeheer
	Gescheiden omgevingen Exclusieve wijzigingsprocedures Registreren van wijzigingsverzoeken en wijzigingen	8.1.5, 10.5.1, 10.5.2, 10.5.3	Wijzigingsbeheer Probleembeheer Servicebeheer
	Classificeren en vastleggen van problemen Prioriteitstelling en voortgangsbewaking	5.2.2, 8.4.2	Probleembeheer Helpdesk Servicebeheer
	Calamiteitenplan Prioriteitstelling Back-up/uitwijk Broncode in escrow geven	8.1.3, 8.4.1, Hoofdstuk 11	Calamiteitenbeheer Probleembeheer Helpdesk

Literatuurlijst

ACIB	Handleiding A&K Analyse, bijlagen 5 Checklist bedreigingen, 8 Basistabellen maatregelen en 9 Voorbeeldmatrices Componentsoort/Incident/Dreiging/Maatregel, ACIB, 1996.
Bautz1	J. Bautz et al., Elektronische werkplekbeveiliging: de bedreigingen versus de te nemen maatregelen, Ten Hagen & Stam, 1998.
Bautz2	J. Bautz et al., Checklist informatiebeveiliging, Ten Hagen & Stam, 2000.
Cazemier	J.A. Cazemier, P.L. Overbeek, L.M.C. Peters, ITIL Security Management, 1999.
Code	Code voor Informatiebeveiliging, Nederlands Normalisatie-instituut, eerste versie (1994) en herziene versie (1999).
Damen	G.H.T. Damen et al., Cryptografie in de praktijk, Ten Hagen & Stam, 2000.
Nivra	Automatisering en Controle: Deel VII Kwaliteitsoordelen over informatievoorziening, NIVRA geschrift 53, Kluwer, 1989.
OTB	OTB-studie Inbelbeveiliging, 1997.
PI	PI studie Netwerkbeveiliging.
Van Dam	P.P.A. van Dam en anderen, Internet, intranet en beveiliging: het technische kader, Ten Hagen & Stam, 1998.
Van Zeist	B. van Zeist et al., Kwaliteit van softwareprodukten, praktijkervaringen met een kwaliteitsmodel, Kluwer bedrijfswetenschappen, 1996.
VIR	Voorschrift Informatiebeveiliging Rijksdienst, Ministerie van Binnenlandse Zaken, 1994.

- http://www.ibm.com/globalnetwork/outscsvc.htm
- http://www.ibm.com/services/profservices/sos-index.html
- http://www.getronics.nl/organisatie/dienstverleningouts.htm
- http://www.hp.nl/outsourcing/NFouts98/art03_services.htm
- http://www.origin.nl/solutions/index.htm#SO
- http://www.kpmg.nl/
- http://www.unisys.nl/
- http://www.digital.nl/nl/diensten/oms/index.html
- http://www.comsysinc.com/capabili/services.htm
- http://www.hollandconsultinggroup.nl/activiteiten/adviesgebieden/uitbesteding.ht
- http://www.outsourcing.com/OSM1How.htm
- http://www.cssa.co.uk/home/pubs/practice/itout.htm
- http://www.regiolicht.nl/homepages/erenger1/indexthss.htm