

magazine voor IT service en security management

www.itbehermagazine.nl

IT beheren 6

Levob:

**“Kleine investering,
doeltreffend change
management”**

Meten, sturen & voorspellen

Tips en valkuilen bij meten en sturen

Grip op netwerkbeschikbaarheid

Fontys: succes van een geoutsourcete helpdesk

Microsoft MOF op de ontleedtafel

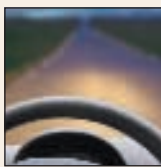
pagina 31

■ MOF versus ITIL ■ Is MOF maf? ■ Bereid u voor op IPv6 ■ Creëer veilige applicatie-omgeving ■

augustus 2003

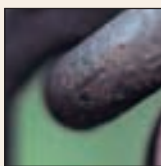
RSA
pagina 2

14 Meten is weten, sturen is de kunst



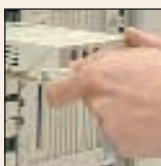
Definieer 'keuzeplateaus', zodat een groeimodel voor metrics ontstaat
Rapporteren en meten zijn aan de orde van dag, vooral als IT wordt afgerekend op haar toegevoegde waarde. De auteur beschrijft de valkuilen en knelpunten van meten, en formuleert een aantal heldere, eenvoudige uitgangspunten om de problemen weg te nemen. Met als ultieme doel het vergaren van de juiste stuurinformatie.

19 Rekenen aan netwerkbeschikbaarheid



Op zoek naar de zwakste schakel
Dit artikel beschrijft een model om te rapporteren over behaalde beschikbaarheid, de ernst van storingen meewegend. Deze gegevens kunnen dan afgezet worden tegen de afspraken in de SLA. Daarnaast is het model te gebruiken om de beschikbaarheid te voorspellen en dus het netwerkontwerp te verbeteren.

24 Levob: change proces in een kleine organisatie



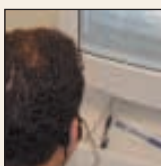
Met een kleine investering een doeltreffende procesinrichting
ITIL wordt de laatste jaren minder dwangmatig gehanteerd. Vaak wordt slechts een deel van de ITIL-processen ingevoerd. Maar kleinere bedrijven zijn om allerlei redenen huiverig om met ITIL aan de slag te gaan. Dat dat niet nodig is, bewijzen de mensen bij verzekeraar Levob: de kleinschalige, maar succesvolle invoering van change management.

31 Acceptatie Microsofts beheerframework in cruciale fase



Eerste ervaringen, literatuur en certificaten rondom MOF komen los
ITIL is al jaren dé norm voor de inrichting van IT-beheerprocessen. Toch wil Microsoft een eigen variant in de markt te zetten: het Microsoft Operations Framework. De auteurs leggen MOF op de ontleedtafel en maken de onvermijdelijke vergelijking met ITIL. Gaat het wat worden?

37 Procesverbetering op de Fontys Helpdesk



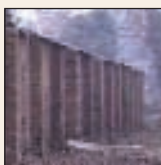
Goedlopende helpdesk houdt scholen betrokken
Tegenwoordig worden we overspoeld met theorieën over verbeteringen op helpdesks. Maar hoe gaan dit soort processen in de praktijk? Zijn helpdesks al in staat het primaire bedrijfsproces daadwerkelijk te ondersteunen? Dit artikel beschrijft de opkomst en ontwikkeling -- inclusief knelpunten en resultaten -- van de helpdesk van de Fontys Hogescholen, in een traject van outsourcing.

43 Migreren naar IPv6



Beschrijving van aanpak voor onvermijdelijke overgang
De migratie van IPv4 naar IPv6 vindt niet van de ene op de andere dag plaats. Maar eens zal deze een feit zijn. En als het zover is, hoe verloopt dan de daadwerkelijke migratie van uw lokale netwerk? Welke stappen moet u straks zetten? Denk er alvast over na. Dit artikel helpt u op weg.

47 Integren van nieuwe applicaties in veilige omgeving



Beheer op basis van rollen noodzakelijk
Wie in een goede technische beveiliging wil voorzien, dient de gehele technische infrastructuur te onderzoeken op zwakke plekken en risico's. Bovendien moeten nieuwe systemen en applicaties gecontroleerd in deze veilige omgeving geïnstalleerd kunnen worden. De auteurs beschrijven hun aanpak, die bij een grote bank wordt ingezet.



Symbiose

We kennen allemaal de situatie waarbij een klant en een leverancier tegenover elkaar staan. In de ICT komt dit net zo vaak voor als in andere sectoren. De klant staat op zijn strepen en de leverancier moet het maar uitvoeren. Het toont de wederzijdse afhankelijkheid die voornamelijk is gebaseerd op de dreiging van niet-betalen of strafkorting. Menige pathologische relatie suddert zo jaren door.

Onlangs was er een seminar waarbij drie outsourcers zich presenteerden. Schuberg Philis en GlidePath, als twee nieuwkomers, en EDS, als oudgediende. De voordrachten gaven een ondubbelzinnig beeld. Het lijkt erop dat de 'traditionele' outsourcing business modellen hun langste tijd hebben gehad. Je kunt er alleen een succes van maken als je je als partners opstelt. Ken Ferderer, ICT-baas van Priority Telecom, een klant van Schuberg Philis in een sector waar het momenteel erg slecht gaat, omschreef het als volgt. "Mijn strategische horizon is gekrompen tot een maand, mijn tactische tot een week. Help mij te overleven. Als ik omval, gaan jullie mee. Om door deze zware tijden te komen hebben we een symbiotische relatie nodig."

Het antwoord van Pim Berger, directeur van Schuberg Philis is helder. "We garanderen honderd procent uptime. Halen we dit niet, dan krijgt de klant een stevige maandomzet korting. Onze SLA's zijn bij voorkeur niet langer dan drie pagina's, om niet te verzanden in welles-nietes-gezeur. Riscicomagement en change management hebben topprioriteit." Uiteraard haalt men de theoretische uptime niet. Volgens Berger komt het echter zelden voor dat een klant de korting claimt waar hij recht op heeft. Dat is een mooi signaal en het bewijs dat je in een gelijkwaardige relatie zit waarbij de belangen gelijk zijn. Ideale outsourcing kent geen pathologische, maar een symbiotische relatie.

Een bedrijf dat outsourcing overweegt, heeft tegenwoordig zeer veel businessmodellen om uit te kiezen. Binnen de businessmodellen bestaat een groeiend aantal varianten. Van co-location, via ASP, offshore, helemaal tot business process outsourcing. Fysieke locaties van mensen en systemen tellen niet meer, glasvezel doet wonderen. Als een opdrachtgever eenmaal de stap naar outsourcing heeft gezet, volgen gebeurtenissen elkaar snel op. Mensen gaan over en krijgen een nieuw carrièreperspectief. Applicaties en infrastructures worden opgekrikt en ingeschaald naar volwassenheid. De bezem gaat door het ratjetoe aan netwerk, servers en OS'en. Risico's worden gemanaged, change processen heringericht, supportstructuren hergedefinieerd.

Oké, oké, dit is een ideaalplaatje. De tijden zijn hard, voor iedereen. Maar over het evenwichtig partnership als belangrijkste succesfactor om beide te overleven hoeven we het denk ik niet meer te hebben.

Herbert Boland
h.boland@wkths.nl

Colofon

IT Beheer Magazine voor IT service en security management is een uitgave van ten Hagen & Stam Uitgevers.

www.itbeheermagazine.nl

tenHagenStam
UITGEVERS

Hoofdredacteur

Herbert Boland
Postbus 34, 2501 AG Den Haag
h.boland@wkths.nl

Redactie

Nico van Beek
Johan Op de Coul
Jan Jaarsma
Hein Nieuwhof
Paul Peursum
Dick Kraaij (eindredactie)
Louise Wagenaar (bureauredactie)
E-mail: itbeheerredactie@wkths.nl
Tel.: (070) 3046918

Correspondenten

Bart de Best	Ronnie Lachniet
Gerard Blokdiik	Hans van de Looy
Martin Booman	Martijn van Oorschot
Guus Delen	Ernst J. Oud
Bob Driessen	Paul Overbeek
Dorjee van Halderen	Louk Peters
Aaldert Hofman	Leo Ruijs
Frans M. Kanters	Flip van de Waerd

Directeur

Sasja Albersen, s.albersen@wkths.nl

Uitgever Manager

Sieds de Boer, s.boer@wkths.nl

Uitgever

Gijs Vroom, g.vroom@wkths.nl

Hoofd verkoop advertentie-exploitatie

Rob de Kleijnen, r.kleijnen@wkths.nl

Marketing

Esther Devilee, e.devilee@wkths.nl

Advertenties:

Gerard Brouwers, accountmanager,
g.brouwers@wkths.nl, Tel.: 06-51587299
For sales representatives in Belgium/Luxemburg, France,
Germany, Italy, U.K., USA and Switzerland contact
Martin J. Weber, International Sales Manager,
intsales@wkths.nl, phone +31-70-3045769, fax +31-70-3045812

Vormgeving

Beeldvorm, Pijnacker

Fotografie

Henk Tukker, NFP Photography, Utrecht

Abonnementen

IT Beheer Magazine verschijnt 10 keer per jaar. Abonnementsprijs per jaar is in Nederland € 124,20 (excl. 6% BTW). AG-goldcardhouders € 111,30. Losse nummers € 15,50 per stuk. Een abonnement kan ieder gewenst moment ingaan. Beëindiging van het abonnement kan uitsluitend schriftelijk geschieden, uiterlijk twee maanden voor het einde van de abonnementsperiode. Nadien vindt automatisch verlenging plaats.

Voor abonnementen:

ten Hagen & Stam Uitgevers
Antwoordnummer 13017, 2501 VC Den Haag
Tel.: (070) 30 46 820, Fax: (070) 30 45 880
E-mail: info.ict@wkths.nl

Abonnementen België

Kluwer Uitgevers
Tel.: 0800 30143, Fax: 0800 17529
E-mail: info@kluwer.be

Samenstellers en uitgever zijn zich volledig bewust van hun taak een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kunnen zij geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden.

Ten Hagen & Stam b.v. legt uw gegevens vast voor de uitvoering van de (abonnements)overeenkomst. Uw gegevens kunnen door ten Hagen & Stam b.v., of zorgvuldig geselecteerde derden, worden gebruikt om u te informeren over relevante producten en diensten. Indien u hiertegen bezwaar hebt, kunt u dit melden aan ten Hagen & Stam b.v., t.a.v. Afdeling Relatiebeheer, Postbus 34, 2501 AG Den Haag.

Artikelen uit IT Beheer Magazine mogen alleen worden overgenomen, gekopieerd enz. na uitdrukkelijke schriftelijke toestemming van de uitgever.

© ten Hagen & Stam Uitgevers
ISSN 1567-5963

IT service 6

quote

- 6** ITB agenda
- 6** ITB sidelines
- 7** ITB clinic
- 8** ITB expeditie
- 11** ITB security matters
- 13** ITB beheerlijk
- 14** **Meten is weten, sturen is de kunst**
Definieer 'keuzeplateaus', zodat een groeimodel voor metrics ontstaat
Louk Peters, Nick Bakker en Martin van Vuure
- 19** **Rekenen aan netwerkbeschikbaarheid**
Op zoek naar de zwakste schakel
Peter Hasperhoven
- 24** **Change proces in een kleine organisatie**
Met een kleine investering een doeltreffende procesinrichting
Cees Doets en Ad Zoet
- 31** **Acceptatie Microsofts beheerframework in cruciale fase**
Eerste ervaringen, literatuur en certificaten rondom MOF komen los
Rudolf Liefers
- 37** **Procesverbetering op de Fontys Helpdesk**
Goedlopende helpdesk houdt scholen betrokken
Jurian Burgers
- 43** **Migreren naar IPv6**
Beschrijving van aanpak voor onvermijdelijke overgang
Marco van der Kraan
- 47** **Integreren van nieuwe applicaties in veilige omgeving**
Beheer op basis van rollen noodzakelijk
Hans Spaander en René Klootwijk
- 50** ITB service

9 september, thema-avond

Tooling service management

Plaats: Amersfoort, kantoor ITSMF

Info: www.itsmf.nl

9-10 september, congres

Security & Hacking

Plaats: Amsterdam, Novotel

Info: www.euroforum.nl

16 september, thema-avond

Alignment CMM en ITIL

Plaats: Amersfoort, kantoor ITSMF

Info: www.itsmf.nl

16-17 september, training

IP-VPN

Plaats: Baarn, Kasteel de Hooge Vuursche

Info: www.heliview.nl/training

25 september, minicongres

Joop Bautz Security Award 2003

Plaats: Putten, Kasteel De Vanenburg

Info: www.ngi.nl

2-3 oktober, masterclass

IT Security Management

Plaats: Amsterdam

Info: www.iir.nl

21 oktober, seminar

Windows 2003 Security

Plaats: Neder-over-Heembeek, België

www.itworks.be

28-29 oktober, congres

Doe je mee?

Plaats: Maastricht, MECC

Info: www.doejemee.com

4-6 november, forum

Service Desk Forum 2003

Plaats: Lisse, Golden Tulip

Info: www.servicedeskforum.nl

18 november, evenement

The Tooling Event

Plaats: Nieuwegein, NBC

www.thetoolingevent.nl

Aanschaf en gebruik ITSM-tools staan centraal op uniek eendaags evenement

The Tooling Event 2003

ICT-organisaties hebben al lange tijd grote behoefte aan praktische informatie omtrent de inzet en het gebruik van service en system management tools. De kosten die gemaakt worden om tot een goede selectie of implementatie te komen zijn vaak hoog en de ROI onduidelijk. Veel organisaties worstelen met de twijfel of er wel voldoende rendement uit de tools wordt gehaald. Deze en andere vraagstukken staan centraal bij het eerste *Tooling Event 2003*, dat IT Beheer Magazine in samenwerking met www.independenttool.nl organiseert op 18 november a.s.

Totaalbeeld

Alles op deze dag staat in het teken van de praktijk van selectie, implementatie en gebruik van service en system management tools. De bezoeker van The Tooling Event 2003 kan in één keer zien wat er allemaal wordt aangeboden op de Nederlandse markt en op welke manier andere organisaties deze tools inzetten. Onafhankelijke, laagdrempelige en praktisch toepasbare informatie rondom service en system management tools staat daarbij centraal.

Input gevraagd

Om de inhoud optimaal af te stemmen op de behoefte vragen de organisatoren aan de potentiële bezoekers om aan te geven met welke vragen zij zitten. Deze inventa-

risatie wordt voorafgaand aan het evenement uitgevoerd via een groot aantal media. Belangrijk is dat bezoekers van het evenement waardevolle, direct toepasbare informatie kunnen uitwisselen met collega's en leveranciers.

De komende tijd wordt u via IT Beheer Magazine, Automatisering Gids, Informatie, Independenttool en via www.thetoolingevent.nl op de hoogte gehouden van het programma.

Voor vragen en suggesties kunt u contact opnemen met Judith van Liempt van Independenttool BV via tel. 010 - 2142208.



Uitbesteden regelen op de golfbaan

Nico van Beek

Toen Van Oorschot, directeur ICT bij de firma Verre Vliegzeuren, die week voor de derde keer bij de CEO werd geroepen, begreep hij dat het nu echt fout zat. Aan de grote tafel zaten een paar vijandig kijkende MT-leden en twee, strak in het pak zittende maar verder erg opgewekt ogende heren, die hij niet kende. Uit zijn ooghoeken zag hij op de tafel ook al zijn memo's van de laatste maanden liggen; memo's waarin hij had uitgelegd dat het zo ongeveer een dag per week platliggen van de computer te wijten was aan personeels- en geldgebrek, tekortkomingen van leveranciers, rode stoplichten en open bruggen.

Tweemaal zo duur

Het was duidelijk: dit kon zo niet doorgaan. Uitbesteden was de boodschap en de conceptovereenkomst was inmiddels al met de aanwezige vertegenwoordigers van een outsourcingfirma doorgenomen. En zo werd de automatisering van Verre Vliegzeuren overgedragen aan de Universal Sourcing Association (USA). Hoogerhuis, de opvolger van Van Oorschot, had nog wel gevraagd hoe het in de SLA opgenomen beschikbaarheidspercentage van 95% tot stand was gekomen. Een stomme vraag! 99% zou tweemaal zo duur zijn geworden en het bedrijf was inmiddels zo gewend geraakt aan een uptime van minder dan 80%, dat die 95% allang mooi was.

Bonus fee

De USA pakte de zaken krachtig aan en leverde maandrapportages vol eigendunk

waarin de beschikbaarheid zelfs boven de 100% bleek uit te komen. De facturen volgden die rapportages op de voet, want een betere dan overeengekomen performance bleek volgens de kleine lettertjes in de SLA een bonus fee tot gevolg te hebben. De combinatie van behoorlijk tegenvallende kosten en arrogantie begon te irriteren. Zo ook de hoge beschikbaarheid, want het, bij ontstentenis van computercapaciteit, even een schakje kunnen zetten was er niet meer bij.

De onredelijke klantontevredenheid irriteerde de USA op zijn beurt behoorlijk, evenals het gezank over en het niet betalen van de facturen.

Back-ups overbodig

Toen iedereen er aan gewend was dat, als gevolg van de permanente beschikbaarheid, back-ups overbodig waren geworden, viel na een paar maanden de computer een aantal uren uit. Natuurlijk net toen het

hoofdverkoop de laatste hand aan haar jaarprognose legde. De escalatie richting USA haalde weinig uit. Nog ruimschoots binnen de overeengekomen 95% toch?! De relatie verslechterde verder toen de USA niet bleek te porren voor het door Verre Vliegzeuren gewenste overhevelen van een gering deel van de techniek naar een bevriende leverancier.

Relatie opbouwen

Enfin, de zegeningen van uitbesteding waren duidelijk niet aan Verre Vliegzeuren besteed. De consultant die Hoogerhuis inmiddels verving, werd verzocht de zaak in het reine te brengen. Zij had die honderden boekjes en artikelen over outsourcing natuurlijk wél gelezen. Hoewel uitbesteden de hype van de huidige jaren is, is enige zorgvuldigheid bepaald op zijn plaats. Het tussen neus en lippen door op de golfbaan regelen daarvan is onvoldoende en contra-productief. Met name is van belang – maar er is niets nieuws onder zon! – dat een goede relatie wordt opgebouwd tussen uitbesteder en aanbesteder. De gedachte dat een dichtgespijkerd contract alles tot genoeg regelt, zoals de literatuur wel eens wil doen geloven, is de grote fout die telkens opnieuw wordt gemaakt.

Met Verre Vliegzeuren is het overigens helemaal goed gekomen. Met de USA gaat het wat minder.

Nico van Beek is redacteur van dit blad en tevens consultant bij Cap Gemini Ernst&Young.

Best practice

In de rubriek ITB Clinic behandelen we best practices – alledaagse, veelvoorkomende en ogenschijnlijk kleine kwesties, maar die menigeen regelmatig hoofdbreken bezorgen. Clinic beschrijft, doceert en adviseert. Een groep van auteurs schrijft de column bij toerbeurt en kiest de onderwerpen uit de eigen omgeving.



Rudolf Liefers

Linda Goedhart is sinds ongeveer een jaar service level manager bij de gemeente Zaanstad. Die heeft enige tijd geleden een groot deel van het IT-beheer uitbesteed aan een externe partij. De gemeente heeft voor het beheren van de service levels van haar systemen een aantal service level managers ingezet: één die zich richt op het applicatie-beheer van de bedrijfssystemen, één voor de kantoorautomatisering en de generieke systemen en één voor de technische automatisering. Linda richt zich op de bedrijfssystemen, zoals DIS, Aris, Personeels-informatiesysteem en kantoorautomatisering. Momenteel werkt zij aan het opstellen van de webversie van de servicecatalogus en het verder inrichten van het service level management-proces. Ook het inventariseren van informatiebehoeften en uitleg over pakketten, wat binnen de gemeente onder de noemer "applicatieconsultancy" valt, behoren tot haar taakgebied.

Van programmeren naar ITIL

Vanuit haar opleidingsachtergrond (HEAO-BI) is Goedhart als programmeur begonnen, om daarna de overstap te maken naar technisch beheer. Vanuit beheer groeide zij door naar technisch consultant, om daarna als service level manager aan de slag te

Ontmoeting met Linda Goedhart, gemeente Zaanstad

Service management, een duik in onbekende wateren

IT Beheer Magazine is op bezoek bij Linda Goedhart, service manager bij de gemeente Zaanstad. Deze gemeente, waar een gedeelte van het technisch beheer is uitbesteed, is inmiddels vrij ver gekomen met de inrichting van service management. Goedhart geeft aan Rudolf Liefers tekst en uitleg en concludeert dat van haar functie een grote flexibiliteit wordt verwacht. En het lijkt wel wat op duiken, Linda's grote hobby. Dit is de zesde aflevering van portretten in ICT Service Manager Expeditie.

gaan. Hiertoe heeft ze onder andere ITIL Foundations en een aantal ITIL Practitioners gedaan. ITIL-kennis rekent zij dus tot haar basisuitrusting, en ook is ze goed thuis in het kwaliteitsdenken. Verdere opleidingen in service management en een opleiding rondom het INK-model zullen haar meer nuttige bagage geven.

Als Linda verdieping van haar kennis nodig heeft, gaat ze vaak eerst te rade bij haar

collega's. Media als vaktijdschriften (IT Beheer Magazine) en internet zijn vaak goede bronnen van informatie. Ze geeft aan dat de verenigingen zich te weinig profileren en dat activiteiten vaak net buiten haar bereik van een uur reistijd vallen.

Naast haar werk is duiken een van Goedharts grote passies. Op het moment van ons gesprek is ze nog maar amper terug van een duikvakantie in een warm en zonnig land.

Service managers op expeditie

In de nieuwe column 'itb Expeditie' presenteren we de komende maanden ontmoetingen met de mensen die het vak maken tot wat het is.

De ICT Service Manager Expeditie is een onderzoeksinitiatief van de Beroepsgroep ICT Service Management en IT Beheer Magazine. Dit is opgezet om inzicht te krijgen in de omgeving waarin service managers opereren en hoe zij zelf tegen het vakgebied aankijken. In de Expeditie gaan service managers zelf op onderzoek uit en interviewen zij vakgenoten. Iedere maand publiceert dit blad een van de gesprekken.

Wilt u meer weten of zelf meedoen aan de Expeditie? Neem contact op met Arjen Droog van de Beroepsgroep, arjen.droog@ngi.nl.

Kennis op één plek

Zoals binnen veel gemeenten gebruikelijk hebben de informatiemangers in Zaanstad een decentrale positie binnen de gemeentelijke diensten (Stadsbedrijven, Stad, Wijken en Publiek), terwijl automatisering centraal belegd is. Deze informatiemangers werken sterk vanuit het perspectief van hun diensten. Maar gezien de verdere inzet van applicaties over meerdere diensten heen, is betere afstemming tussen informatiemangers onderling steeds meer nodig. De service level manager vervult hierin een coördinerende rol, samen met de medewerkers van Personeel, Informatie & Organisatie.

Hoewel Zaanstad een deel van het beheer – het technisch beheer van het server- en werkstationpark – heeft uitbesteed aan een



Linda Goedhart: "Met de juiste afspraken, vertrouwen in je (duik)partner en goede voorbereiding kom je er wel"

derde partij, houdt de gemeente applicatiebeheer, functioneel beheer en service level management in eigen hand. Applicatiebeheer is samengevoegd in één afdeling, Informatie Beheer Concernapplicaties (IBC). Van die afdeling is Linda Goedhart de service level manager. Door de vorming van IBC is veel kennis van applicaties, zowel technisch als functioneel, verenigd op één plek, wat veel voordelen oplevert voor de organisatie.

Rol van service level manager

Met de uitbestede IT-organisatie is een heldere ketenrelatie opgezet, die is vastgelegd in SLA's. De uitbesteding heeft een aantal positieve zaken opgeleverd. Linda vindt het kleinere aantal loketten het meest in het oog springen. Eindgebruikers kunnen voor ondersteuning terecht bij de (tevens) uitbestede helpdesk en de klant (dienst) vindt zijn aanspreekpunt bij de service level managers.

De service level managers vervullen de rol van account manager vanuit de functionele gebieden binnen I&A; de informatie-managers zijn wat dat betreft hun tegenspelers. Hierdoor is een schijnbare dubbelrol ontstaan, wat soms zorgt voor onduidelijkheden en vertragingen. De

informatiemanager is immers het aanspreekpunt voor de medewerkers binnen de gemeentelijke diensten. Volgens Linda zal meer en betere communicatie tussen de informatimanagers en de service level managers deze aandachtspunten weg nemen, zodat zij minder vaak onbedoeld op elkaars stoel gaan zitten.

Communicatiemiddel servicecatalogus

Linda Goedhart onderhoudt contacten met de informatimanagers binnen de diensten en vult daarmee een van de rollen van de service level manager in. De servicecatalogus is een belangrijk communicatiemiddel dat Linda en haar collega's hiervoor inzetten. De catalogus is geen nieuw fenomeen binnen deze gemeente. Een jaar of drie, vier deden de Zaankanters er al de eerste ervaringen mee op.

Linda geeft aan dat zich de laatste jaren veel belangrijke wijzigingen hebben voorgedaan. "Wij betrekken de informatimanagers nu veel meer en eerder in de toetsingsronden rondom de servicecatalogus. We hebben het bijvoorbeeld toegankelijker gemaakt door praktijkvoorbeelden op te nemen".

Intussen is de servicecatalogus volgens Goedhart een professioneel medium gewor-

den, dat ook steeds meer in aangepaste vorm zijn weg vindt naar de eindgebruikers. Zij beschrijft: "Deze vorm is veel toegankelijker, zowel qua taalgebruik als technologie. In de toekomst zal hij vooral beschrijven welke diensten daadwerkelijk overeengekomen zijn. De servicecatalogus is dus steeds minder een *pick-list*, maar meer een document waarin de rechten en plichten, de relevante contactpunten en de te volgen procedures voor de eindgebruiker staan. Een webversie is in de maak. Die zal de toegankelijkheid en het onderhoud verder verbeteren".

Elastiek

Linda vindt het vak van service manager leuk: "Je bent de hele dag bezig met mensen uit verschillende delen van de gemeente. Daar heb je wel een helikopter-visie voor nodig. Je moet wel moeite doen om de toegevoegde waarde van service management onder de aandacht van de mensen te krijgen, zowel binnen de diensten als in het IT-domein. Dat blijkt ook als de service level managers meer vanuit de ketengedachte willen gaan sturen, terwijl de IT-deelleveranciers nog sterk met hun stukje bezig blijven en nog niet ver genoeg over hun eigen vakgrenzen heen kijken." "Het is een uitdagend vak", zegt Linda. "Je moet een beetje van elastiek zijn". Niet dat je dan met iedereen meebuigt, legt ze uit. Maar je moet 'meebewegen' binnen de kaders die de organisatie gesteld heeft en die voor iedereen bekend moeten zijn. Wat dat betreft lijkt het wel op duiken, haar favoriete sport. Dat betekent soms ook een duik in relatief onbekende wateren. Maar met de juiste afspraken, vertrouwen in je (verplichte duik)partner en een goede voorbereiding breng je het in de meeste gevallen tot een goed einde. "Als het dan toch misgaat, ben je te overhaast geweest, heb je je niet goed voorbereid of heeft het te maken een gebrek aan vertrouwen."

Linda Goedhart is bereikbaar via l.godhart@zaanstad.nl

Rudolf J. Liefers MIM is bestuurslid van NGI-Beheer en senior consultant bij Cap Gemini Ernst & Young. E-mail: rudolf.liefers@cgey.nl.

Informatiebeveiliging Jaarboek 2003-2004

Het *Informatiebeveiliging Jaarboek 2003-2004* biedt voor het vijfde achtereenvolgende jaar actuele bijdragen van tal van deskundigen op het gebied van informatiebeveiliging en risicomanagement. Het centrale thema van het jaarboek dit jaar is: 'Business bepaalt, informatiebeveiliging faciliteert'. In zes hoofdstukken presenteren specialisten hun laatste visies en inzichten. Deze hoofdstukken zijn: Visie op informatiebeveiliging, Organisatie en management van informatiebeveiliging, Tactisch management voor informatiebeveiliging, Best practises, Business Continuity Management en Communicatie en de mens. Het *Informatiebeveiliging Jaarboek 2003-2004* is samengesteld door Willem J. Huurman en Frans M. Kanters, vaste correspondent van IT Beheer Magazine. Het is verkrijgbaar bij ten Hagen & Stam.

Joop Bautz Security Award 2003

Op donderdagmiddag 25 september vindt de uitreiking plaats van de Joop Bautz Security Award, op kasteel De Vanenburg in Putten. De middag begint om 14.30 uur en kent naast de uitreiking enkele lezingen. Meer info via NGI, afdeling Beheer.

Alumni In ConTact

De TU Delft speelt een belangrijke rol in de opleiding van informatici. Dat blijkt bijvoorbeeld uit de voortrekkersrol en afgestudeerden van Looijen op het gebied van

beheer en van Herschberg op het gebied van beveiliging. Op initiatief van een aantal oud-studenten (onder wie redacteur van dit magazine, Johan Op de Coul) en de Alumnivereniging van Delftse informatici wordt een onderzoek uitgevoerd naar de loopbanen van afgestudeerde informatici. Het initiatief is gelanceerd onder de titel 'Alumni In ConTact 2004, Wat doe jij met jouw informaticastudie?' Over de resultaten verschijnt een boekje en wordt begin 2004 een symposium georganiseerd. Meer info via de website alumni.ch.tudelft.nl.

Publicsoft verhuisd

Publicsoft is verhuisd naar Molensteyn 60 in De Meern, postbus 241, 3454 ZL De Meern. Telefoon-, fax- en mobiele nummers zijn niet gewijzigd. Het Publicsoft Operations Center blijft gevestigd in het KPN CyberCenter in Schiphol-Rijk.

Axios en Devoteam

Axios Systems en Devoteam zijn een partnerovereenkomst aangegaan voor het aanbieden van IT service management-oplossingen. In eerste instantie is dit voor België, Nederland en Luxemburg, maar later zal dit worden uitgebreid tot geheel Europa. Devoteam adviseert assist voor helpdesk- en IT service management-oplossingen. Devoteam heeft assist geïnstalleerd in het opleidingscentrum en daarnaast kunnen geïnteresseerden de assist aan de tand voelen in de twee demonstration centres in België en Nederland. Meer info via www.axiossystems.com.

TeleCity en ISIT in on demand storage-diensten

TeleCity, aanbieder van Internet Data Center-diensten, en ISIT, leverancier van storage-oplossingen, bieden drie 'On Demand Storage'-diensten aan, namelijk: storage on demand, replication on demand en backup on demand. Bij de diensten wordt gebruikgemaakt van een nieuw storageplatform in het data center van TeleCity. Gebruikers betalen slechts voor de capaciteit die ze in gebruik hebben. TeleCity zorgt voor de hosting van de infrastructuur en voor de eerstelijns ondersteuning. ISIT neemt de tweedelijns ondersteuning en eventuele on-site installaties voor haar rekening.

Patrol Express

BMC Software brengt een nieuwe versie van Patrol Express uit. Met deze software kunnen bedrijven op afstand de werking van verschillende bedrijfssystemen bewaken. Daarmee slaat men een brug tussen een 'lichte' bewaking die sommige systemen vereisen, en de zware oplossingen waarmee kritieke bedrijfssystemen beheerd worden. Versie 3.0 bevat veel nieuwe functionaliteiten. Zo bewaakt het webtransacties vanuit het perspectief van de eindgebruiker, en biedt het gebruikers een optie om internetwachtijden via meer dan 30 punten te meten. Verder biedt het nieuwe mogelijkheden om webtransacties te controleren na on-lineconfiguratie, en ondersteunt het bovendien de belangrijkste dynamische HTML-technieken en populaire types om content te downloaden. Ook bevat Patrol Express 3.0 nieuwe functies op het gebied van berichtgeving en rapportering.

Marval en ASL

De ASL Foundation heeft de Marval Service Management suite als eerste oplossing aangewezen die volledig compliant is aan alle relevante ASL-processen. Alle processen in de Marval-oplossingen conformeren zich aan de standaard die de ASL Foundation heeft gezet voor applicatiebeheer. ASL is een raamwerk voor applicatiebeheer naast en complementair aan de ITIL-standaard voor infrastructuurbeheer. Het is het eerste internationaal erkende framework voor applicatiebeheer. Meer info via www.noty-etasl.com en www.marval.nl.

GE Access' tienstappenplan naar veiligheid

GE Access heeft een gratis stappenplan uitgegeven dat bedrijven moet helpen hun netwerk beter te beveiligen. Het tienstappenplan bespreekt de belangrijkste probleemgebieden bij de beveiliging van het netwerk en geeft praktisch advies om deze problemen aan te pakken. Ook gaat de gids in op de mogelijke gevolgen van het niet aanpakken van problemen. In het stappenplan wordt bijvoorbeeld ingegaan op het 'patching'-, wachtwoord- en firewallbeleid en op het updaten van de virus-definities in de firewall. Het stappenplan is te vinden op www.europe.access.com.

Het pasjesballet

Paul Overbeek

Een, twee, drie, húp. In spagaat vliegt daar Rudolf Nurejev. En hoog op de spitzen, daar gaat Giselle. De controller, Elvis, glijdt er in een volmaakte pas de deux achteraan. Om vlak bij de pasjeslezer nog een wulpse heupbeweging te maken.

In rap tempo trekken bedrijven, inclusief overheden, hun beveiliging op. Deels een effect van 9-11. Deels ook een antwoord op de algehele verloederding. Het besef dat de wereld van 2003 niet meer dezelfde is als die van 1960. Tóén kon je de achterdeur nog gewoon op laten staan. Ja, tóén was geluk heel gewoon.

Wat is ook alweer de bedoeling van die pasjes? Ten eerste: authenticatie. Je geeft het pasje uit aan Pietje. En als het pasje wordt gebruikt, dan is dat dus Pietje, en niemand anders. Helaas: mensen lenen hun pas uit aan iedereen met een goed verhaal. En met de beste bedoelingen. Verder worden pasjes doorgaans verloren in de directe omgeving van het gebouw. Je kunt je toegang dus nooit beheersen op basis van alleen een pasje. De trend is het pasje te combineren met een pincode: iets dat je hebt, en iets dat je weet. Ten tweede: autorisatie. Met pasjes kan je binnen je gebouwen een veel fijnmazigere toegang regelen. De computerruimte wordt extra afgeschermd, de postkamer, en natuurlijk wordt de directiegang ook afgeschermd van de modale medewerker. Ten derde: bewustwording. De blauwe pas is een bezoeker, met de naam van zijn gastheer erop. De groene pas is voor tijdelijke krachten: die mogen niet onbegeleid rondlopen. En voor vaste krachten: de foto-pas.

Dit zijn mijn tips voor het pasjesballet. Allereerst: zet foto, voornaam en achternaam zo groot mogelijk op het pasje. Zo leer je je collega's kennen. Zorg er vervolgens voor dat het pasje makkelijk op ooghoogte zichtbaar is. Ik vind het zelf nogal gênant om op kruishoogte iemands pas te controleren. Zorg dus voor draagmiddelen zoals een koord of elastiek om de nek. Maak het systeem bestand tegen al te hulpvaardige medewerkers. Maak dat pasjes moeilijk uit te lenen zijn door andere functies aan de pas te binden: de koffieautomaat, bezoek aan de kantine of toegang tot de parkeergarage. Maar boven alles: voorkom het hulpvaardig openhouden van deuren. Immers, een galante man anno 2003 houdt zijn pasje voor de lezer om een dame door te laten. Maar ook als ik, bepaald niet overdadig aantrekkelijk, ergens hulpeloos manoevrerend met laptop en koffer een pand probeer binnen te komen, is er altijd wel iemand die even een deur voor me open wil houden. Dat heet het 'meelooprisico'. Minimaal moet je toch met persoonssluisjes of tourniquetjes werken. De tijd dat je de achterdeur open kon laten voor de melkboer is voorbij.

Terug naar die pas-de-chat. Waarom zitten zelfs binnen één gebouw die pasjeslezers niet op één en dezelfde hoogte? Draag ik het pasje om mijn nek, dan moet ik soms limbo-dansend langs de lezer. Draag ik het pasje aan de broekband, dan moet ik het been heffen, gelijk een nooddriftige hond. Kortom, doe alle pasjeslezers op gelijke hoogte. Uw bedrijf is geen trainingskamp voor het Scapino-ballet.

Dr. ir. Paul Overbeek RE is directeur van KPMG Information Risk Management en doceert techniek aan de UvT (TIAS). Hij is bereikbaar via overbeek.paul@kpmg.nl.

Doe-het-zelfbeheer

Recentelijk heeft Axis Nederland, voorheen Applix BV, versie 3.0 van Applix ITSM geïntroduceerd. Deze versie kenmerkt zich onder andere door toevoegingen, zoals Self Service en het ITSM Dashboard, waardoor het toegankelijker is voor klanten van de IT-serviceorganisatie. Zij kunnen via intranet of internet zelf incidenten loggen, wijzigingsverzoeken indienen en de status ervan inzien. Deze functionaliteit ontlast de servicedesk aanzienlijk. Het ITSM Dashboard geeft de medewerker van de IT-serviceorganisatie in één oogopslag inzicht in incidenten, problemen, wijzigingen en acties die aan hem zijn toegewezen. Vervolgens kan hij direct doorklikken naar de taak die hij als eerste dient op te pakken. In Applix ITSM 3.0 zijn naast Self Service en het ITSM Dashboard diverse andere functionaliteiten toegevoegd die de effectiviteit en efficiëntie van de serviceorganisatie vergroten. Een voorbeeld: dankzij een vragenlijst met vooraf gedefinieerde vragen en antwoordmogelijkheden kan een medewerker van de serviceorganisatie met relatief weinig inhoudelijke kennis van applicaties bepalen welke dienst is verstoord. Vervolgens draagt het product automatisch de juiste oplossing aan. Meer info op www.axis.nl.

Monitoringssysteem voor serverruimtes

ATAL, leverancier van dataregistratie-oplossingen heeft recentelijk een monitoringssysteem geïntroduceerd voor de kritischecom-fortparameterstemperatuur en relatieve vochtigheid in serverruimten. De EthernetProbe wordt eenvoudig in een bestaand bedrijfsnetwerk opgenomen en is direct operationeel. Door aan de unit een eigen IP-adres toe te kennen is de EthernetProbe - gebruikmakend van de geïntegreerde webserver - vanaf elke pc met een standaard webbrowser toegankelijk. De EthernetProbe kent real-time weergave en historische trendgrafieken.

Detachering rekencentra

Comparex Nederland is gestart met een eigen detacheringstak die gericht is op datacenteromgevingen. Met het detacheren en outsourcen van ICT-professionals zegt de organisatie in te spelen op een grote marktbehoefte. Dit komt doordat steeds meer bedrijven te kampen hebben met hoge beheerskosten. Hierdoor besluiten zij hun storage en servers te consolideren en hun eigen rekencentra op te zetten. Voor deze datacenters is specifieke expertise en ervaring nodig, waar organisaties meestal niet over beschikken. De detacheringprofessionals zijn gespecialiseerd in storageconsolidatie, serverconsolidatie, back-up en restore, disaster recovery én Citrix-omgevingen. Dit op basis van mainframe, Unix, Windows en Linux.

Consul InSight Security Manager 4.5

Consul kondigde onlangs de introductie van Consul InSight Security Manager 4.5 aan, voorheen Consul/eAudit. Het product is gericht op het correleren van IT-beveiligingsgebeurtenissen en kan grote hoeveelheden data vergelijken, zoals voorkomt binnen grote organisaties met duizenden platformen en systemen. Het verschilt van bestaande beveiligingsoplossingen, omdat het zowel externe als interne gebeurtenissen op de voet volgt. Bij de meeste oplossingen worden alleen externe gebeurtenissen met elkaar vergeleken, zoals firewall-activiteiten. Interne gedragingen, zoals die van trusted users, worden doorgaans niet voldoende geanalyseerd. InSight Security Manager vergelijkt het gedrag van gebruikers op besturingssystemen, databases en applicaties. Dit levert een completer onderzoek en beoordeling van beveiligingssystemen op.

Cramm

3-ANGLE Software & Services heeft een nieuwe versie gelanceerd van het Risico Analyse en Risico Management pakket CRAMM. Sinds 1 april 2003 is CRAMM IV Nederlands Profiel beschikbaar. Deze versie wordt gezien als de opvolger van het risicoanalysepakket Esaka, dat vooral veel binnen de overheid werd gebruikt. Cramm is behalve een product ook een methode die in 1985 in opdracht van de Engelse overheid ontwikkeld is door de CCTA. Met CRAMM is het mogelijk om op een gestructureerde wijze onderzoeken te doen naar risico's binnen bedrijfsprocessen en informatiesystemen. Zie ook www.cramm.org.

Symantec ManHunt

Symantec introduceerde ManHunt 3.0, een geavanceerde netwerkgebaseerde IDS-oplossing. De oplossing combineert multi-gigabit netwerk intrusion detection, real-time analyse van bedreigingen, en functionaliteiten voor proactieve preventie en respons, om organisaties beter te beschermen tegen nieuwe bedreigingen en denial-of-service aanvallen. Het product controleert het netwerkverkeer op snelheden tot twee gigabit per seconde, op interfaces van 6 gigabit, afhankelijk van de systeemconfiguratie. Dankzij de multi-layer architectuur worden aanvallen op het netwerk nauwkeurig geïdentificeerd. Symantec ManHunt combineert vier detectie-technologieën: Protocol Anomaly Detection, signature-detectie, denial-of-service- en scan-detectie, en IDS evasion-detectie.

MOF of MAF?

ITIL is op. Dat wil zeggen dat de meeste IT-organisaties ITIL wel hebben ingevoerd en de positieve elementen eruit hebben toegepast. Ook zijn we in de loop der tijd tegen de tekortkomingen en mankementen van ITIL aangelopen. Iedereen wordt zich er nu langzaam bewust van dat er meer nodig is dan ITIL alleen om beheer op een hoger niveau te krijgen.

Nu komt Microsoft met MOF. Het Microsoft Operations Framework is een methodiek voor het beheren van (Microsoft-)IT-platformen. Wanneer je MOF bekijkt, valt meteen op dat MOF gebaseerd is op ITIL. De Service Management Functions van MOF lijken dan ook verdacht veel op de bekende ITIL Support & Delivery processen. Is MOF dan oude wijn in nieuwe zakken of biedt het ook nieuwe dingen?

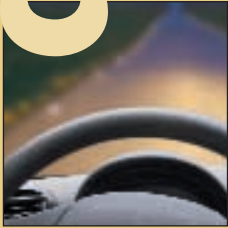
Het voordeel van MOF zit in de pragmatiek. Zo wordt in het aandachtsgebied van Operations concreet beschreven hoe job scheduling en system administration moeten worden uitgevoerd. Natuurlijk wel gebaseerd op Microsoft-omgevingen. Ook wordt aangegeven welke afdelingen welke activiteiten dienen uit te voeren. Dus waar ITIL alleen beschrijft wat er aan besturing gedaan moet worden, geeft MOF ook aan hoe operationele beheeractiviteiten uitgevoerd moeten worden. Dat laatste is voor de operationele beheerders veel interessanter.

Nu is de vraag waarom Microsoft MOF heeft ontwikkeld. Volgens de MOF pocket guide om het beheer van bedrijfskritische systemen op het Microsoft-platform verder te verbeteren. Dit klinkt heel mooi, maar iedereen weet dat Microsoft alleen in zaken investeert waar geld mee te verdienen valt. Microsoft wil een groter marktaandeel hebben op het gebied van bedrijfskritische systemen, oftewel: Microsoft in het Rekencentrum. En dat betekent marktaandeel wegnemen van HP, IBM en Sun. Je kan dus MOF als ook zien als MAF: Microsoft Acquisition Facility, oftewel een marketingmiddel.

Betekent dit nu dat MOF in zichzelf slecht is? Het antwoord zal uit de markt moeten komen. Hoe zal MOF door de beheerders worden opgepakt? Indien de toegevoegde waarde van MOF wordt ingezien, dan kan MOF net zo'n succes worden als ITIL. Op het moment dat de verschillende partijen MOF links laten liggen, dan zal MOF niet meer zijn dan wat salesmateriaal. Het oordeel van de beheerder is nodig.

De vraag is dan ook: "Wordt het MOF of wordt het MAF?" Het antwoord is aan u.

Michiel Borgers is Managing Consultant bij Cap Gemini Ernst & Young en voorzitter van de afdeling Beheer van het NGI. Hij is bereikbaar via michiel.borgers@cgey.nl.



Definieer 'keuzeplateaus', zodat een groeimodel voor metrics ontstaat

Meten is weten, sturen is de kunst

Rapporteren en meten zijn aan de orde van dag. Dat geldt des te meer als de omzet terugloopt en de bedrijfswinst daalt, en IT wordt afgerekend op haar toegevoegde waarde. Wat zijn valkuilen en knelpunten van meten? Hoe neem je die weg?

Door een aantal heldere, eenvoudige uitgangspunten te kiezen, uit te gaan van wat de business wil en niet alles in één keer te willen. De toegevoegde waarde van IT is niet alleen beter meetbaar te maken, maar ook beter stuurbaar.

Meten is het waarnemen en vastleggen van gebeurtenissen. Dit principe geldt voor metingen op allerlei gebied, variërend van proces tot techniek, van kwaliteit tot organisatie. De kunst van het meten is het laten hanteren van het juiste meetsysteem door een actief regelsysteem, zoals een thermometer in de handen van een dokter. De arts zal van te voren *drempelwaarden* en bijbehorende *acties* hebben vastgesteld en de *beslissingen* op de juiste plaats hebben gelegd: tot 39 graden is het aan 'moeders', bij 39 plus krijgt de patiënt medicijnen voorgeschreven en boven de 40 graden is zijn toestand acuut en wordt ziekenhuisopname een serieuze optie.

Metingen en waarnemingen vormen het fundament van de analyse. De analyse is de basis voor een advies en actie: sturen. Hoe goed zijn wij als dokter? En hebben we wel het juiste meetinstrumentarium om goed te kunnen sturen? Liggen de beslissingen en acties op de juiste plaats?

To metrics or not to....

In deze tijd van economische teruggang proberen organisaties vooral te overleven. Voor de IT-organisatie liggen de accenten op prijs/prestatie, kostenbesparing en resultaatverplichting. Centraal staat dat de toegevoegde waarde van IT aangetoond moet worden. Met als doel dat IT-dienstverlening wordt geleverd tegen minder kosten en met meer kwaliteit.

Louk Peters, Nick Bakker en Martin van Vuure

Nu is en blijft kwaliteit een lastig begrip. Kwaliteit in de ogen van wie? Die van de eindgebruikers, de budgethouders of de IT-medewerkers? En hoe maak je dat operationeel? Om meer houvast te krijgen, grijpen veel organisaties terug op 'dashboard'-modellen, zoals INK, EFQM, TCO en de balanced scorecard. Hiermee geven zij sturing en inhoud aan de beoogde kwaliteitsverbetering – dat is de bedoeling tenminste. Bijna alle modellen geven aan dat het zaak is te sturen op meeteenheden, kengedaten, metrics, en niet op zoiets vaags als een buikgevoel. Toch nemen nog veel organisaties een strategische beslissing op basis van vage aannamen. Zo blijkt uit een recent onderzoek¹ dat ongeveer de helft van de topmanagers zich zelfs *gedwongen* voelt op die basis beslissingen te nemen. Of sturen vanuit de buik altijd slechter is dan sturen op 'harde' cijfers is nog maar de vraag. Metrics roepen een beeld op van een stuurman die aan het roer van zijn 'IT-schip' staat en louter op basis van zijn kompas en snelheidsmeter kan sturen of bijsturen waar het nodig is. Veel managers houden van grafieken; net als kleine jongens zijn ze dol op een dashboard met veel klokken en lampjes. Zou dat geen schijnzekerheid kunnen zijn? De Titanic had immers ook een kompas en een snelheidsmeter aan boord... Kortom, naast meetgegevens blijken communicatie, escalatie en het nemen van de juiste beslissingen noodzakelijk om de juiste koers te blijven volgen.

Valkuilen en knelpunten

IT-organisaties verschillen in volwassenheid. Aan de ene kant bestaan er IT-organisaties die nog moeten beginnen met meten. Anderzijds zijn er IT-organisaties die kilo's aan rapporten produceren die niemand leest. Wat is wijsheid? Om die vraag goed te kunnen beantwoorden, presenteren we allereerst zes valkuilen. Al deze situaties komen geregeld voor in de praktijk, bij bedrijven die door middel van rapportages echt willen gaan sturen.

Valkuil 1: alles willen meten

Vanuit de techniek is veel, heel veel te meten. Zo zijn van het gebruik van een server duizenden zaken te registreren. Wat gemeten wordt, hangt af van het gebruik van de server. Zo kan dezelfde server in gebruik zijn als webserver, databaseserver of fungeren als een firewall. De eerste is veelal memory-intensief en de tweede disk I/O-intensief, terwijl voor de laatste vooral de throughput en veiligheid van belang

zijn. Bij server 1 wordt vooral geheugenbe-zetting gemeten, bij server 2 I/O-perfor-mance en bij server 3 het aantal onge-wenste intruders. Wat zeggen die metingen nu? Niets, als niet van tevoren is bepaald dat die rapportage wordt gebruikt als stuurinformatie met een bepaald doel. Ook hier klinkt de 'waarom'-vraag en geldt veel minder wát te meten is.

Herkent u dit?

De IT-organisatie kan met meten en sturen wel degelijk de mist ingaan. Enkele praktijkvoorbeelden.

- Een IT-organisatie beschikt over heel veel rapportage. Iedereen lijkt te sturen. Op alle niveaus wordt er aan radertjes gedraaid, zonder dat medewerkers het idee hebben dat de organisatie er als geheel ook beter van wordt. Geen inzicht in de samenhang van processen leidt tot sub-optimalisatie.
- Een consultant stuurt een waslijst aan mogelijke KPI's (key performance indicatoren) van een ITIL-proces op naar de IT-manager met de vraag daaruit een keuze te maken. In een eerste reactie heeft de IT-manager enkele KPI's aangekruist. Als de consultant later doorvraagt bij de operationele service manager, blijkt dat nog niets uit dit proces wordt gemeten en sturing op die KPI's nu dus nog niet kan. Het 'waarom' van verbetering van dit proces komt daarbij opnieuw naar voren. Niet zozeer het ontbreken van sturing als zodanig is hier het bezwaar. Hier moet vooral duidelijkheid komen over wie wanneer wat doet in dit proces.
- Op een internetsite is door technici goed aan te geven wanneer er gehackt wordt. In de praktijk blijkt dat menig bedrijf niet genoeg vooruitdenkt. Zo is de vraag wat er moet gebeuren wanneer meer dan *x portscans* door middel van een niet geoorloofd protocol plaatsvinden, niet beantwoord.
- De grote spraakverwarring: de business meldt dat de helpdesk slecht bereikbaar is. De IT-manager verweert zich daartegen door te rapporteren dat de helpdesk steeds meer incidenten oplost en dat ook sneller doet.

Valkuil 2: niet beslissen

'Meten is weten' wordt vaak ervaren als basis voor de IT-dienstverlening. De kracht van meten is de herhaling. Uit de herhaling volgt de voorspelbaarheid. Zullen we beter of slechter zijn dan vorige week, vorige maand, vorig jaar in de dingen die we doen? Het doel van die metrics is het mogelijk maken van sturing en dus ingrijpen. Die laatste activiteit is meestal nu net niet vormgegeven, terwijl het juist kritisch is. Wie schrijft, die blijft; en wie rapporteert, is ingedekt voor zijn 'baas'. Prachtige grafieken en tonnen aan rapporten worden opgeleverd, maar doen we daar ook wat mee? Leest iemand überhaupt de rapportage van bijvoorbeeld systeembeheer en is deze ook bedoeld om (bij) te sturen? Rapportage lijkt dan op een diagnose zonder medicijn. Metingen leiden niet tot beslissingen.

Of sturen vanuit de buik altijd

slechter is dan sturen op 'harde'

cijfers is nog maar de vraag. De

Titanic had ook een kompas...

Valkuil 3: geen betekenis

Een andere valkuil zijn *betekenisloze metrics*. In vele ITIL-boeken zijn hele lijsten van key performance indicatoren (KPI's) per ITIL-proces opgenomen. De neiging is aanwezig om dan maar lukraak enkele van die KPI's te kiezen en daarop te gaan sturen. Verwar common practice echter niet met common sense. Zijn die KPI's wel nodig voor uw organisatie? Meten ze de juiste dingen? Kortom, zijn ze wel key voor uw organisatie? Een key betekent een beperking; het is zaak de juiste indicatoren te kiezen. In de beperking openbaart zich de meester. Is duidelijk waarop we willen sturen? Geven de indicatoren inzicht in de zaken waaraan de IT-afdeling haar uren besteedt en dus geld uitgeeft? Draagt inzicht in deze indicatoren wel bij aan het verbeteren van de toegevoegde waarde van IT voor de business?



Valkuil 4 : meten leidt tot ongewenst gedrag

Metingen kunnen ook een onbedoeld en ongewenst effect hebben. Zo kan strak sturen op het verkorten van de gemiddelde doorlooptijd van incidenten ten koste gaan van de kwaliteit van de oplossing en het ongewenste effect hebben dat gebruikers 'afgesnauwd' worden die te lang van stof zijn. Immers, de gesprekstijd heeft directe gevolgen voor de doorlooptijd van een inci-

dent. Hier geldt het adagium: zeg mij wat u meet en ik zal mij ernaar gedragen.

Valkuil 5: niet het goede meten

Nog een valkuil is dat het meetinstrument bepaalt wat gemeten wordt. De rapportage die het service management-tool oplevert, bepaalt waarop gestuurd gaat worden. Niet wijzelf, 'dokter', of de business als 'patiënt', maar uitsluitend de thermometer bepaalt dan of we ziek of gezond zijn.

Valkuil 6: geen drempels

Ten slotte komt het voor dat meeteenheden niet gecombineerd zijn met drempelwaarden of dat men daarbij heeft nagelaten te bepalen welke maatregel past bij overschrijding van een drempelwaarde.

Metrics for the sake of metrics

Veel gebruikte metingen hebben een te sterke interne IT-focus. Een van de grootste valkuilen is het loslaten van de bedrijfsstrategie. Het is opvallend hoe weinig IT-organisaties de resultaten van een klanttevredenheidsonderzoek gebruiken als uitgangspunt voor verbetering van de kwaliteit van de IT-dienstverlening². Vanuit de business heeft men behoefte aan herkenbare indicatoren die aansluiten bij business drivers als groei (kan er nog meer bij?), bedrijfszekerheid (doet-ie het of doet-ie het niet?), integriteit (is mijn geloofwaardigheid zekergesteld?), flexibiliteit (heb ik voldoende ruimte om in te spelen op verandering?) en ROI (staan de kosten in verhouding tot de baten?). IT vindt het dan lastig haar technische indicatoren te vertalen in die termen die de business begrijpt. Dat is de omgekeerde wereld. Ga uit van wat de business wil. IT gaat nog te veel uit van de techniek met haar technische indicatoren.

Is er een vertaler in de zaal? Wat zeggen al die KPI's en metrics van de IT-afdeling nu over de bedrijfsstrategie van bijvoorbeeld kostenbesparing? Wat zeggen al die mooie cijfers over onze relatie met de business? Cijfers alleen zijn niet voldoende om de relatie met de business gezond te houden.

Supposed level agreement?

De samenwerking tussen business en de IT-organisatie is te symboliseren met het beeld van een tandem. De business stuurt en de IT-organisatie zorgt voor de IT-dienstverlening om de bedrijfsstrategie te realiseren. Die samenwerking tussen business en IT vindt haar beslag in de veel gebruikte service level agreements. Deze SLA's zijn meestal door de IT-afdeling geïnitieerd en

opgesteld. Gehanteerde meeteenheden zeggen niets over het uitvoeren van de bedrijfsstrategie. Het lijkt erop alsof de IT-afdeling niet echt meetrap en zelf een andere route in haar hoofd heeft. Zo werd onlangs een SLA opgesteld waarin de beschikbaarheid van een bepaalde bedrijfskritische applicatie gegarandeerd werd met een beschikbaarheidspercentage van 99 en nog drie decimalen achter de komma. In deze organisatie worden verstoringen die gebruikers melden keurig geregistreerd, maar tellen ze niet mee in het berekenen van het maandelijkse beschikbaarheidspercentage van die applicatie, louter op technische indicatoren.

Wie houdt wie hier voor de gek? Een SLA zou een afspraak moeten zijn voor een te leveren prestatie op basis van ervaringen uit het verleden. Een afspraak om komend seizoen een niet getraind atleet over 2,30 meter te laten springen zal niet worden gehaald, een dergelijke afspraak met een atleet die eerder 2, 20 meter sprong getuigt van ambitie.

Oplossingsrichtingen

Uit de genoemde valkuilen stappen kan op verschillende manieren. De volgende uitgangspunten zijn van belang:

- stel doelen, stel vragen en meet;
- KISS: keep IT, short and simple – neem een aantal iteratieve stappen om te komen tot een meetsysteem;
- kies het juiste ambitieniveau.

Doelen, vragen, meten

Te vaak is het doel van een IT-service management-verbetertraject te vaag, niet meetbaar en heeft het geen relatie met de business. De doelen moeten duidelijk zijn en gebaseerd zijn op het SMART-principe. Waarom willen we dat en dat meten, moet de centrale vraag zijn. Wie die doelen eenmaal gesteld heeft, kan zich gaan afvragen hoe die doelen te bereiken en met welke meetwaarden. Dit staat bekend als het paradigma van Goals, Questions & Metrics³. Door dit GQM-paradigma toe te passen bij de verschillende belanghebbenden krijg je ieders verwachtingen helder. We geven een voorbeeld van het GQM-paradigma.

- Doel: reduceren van de impact van IT-verstoringen op de business.
- Vragen: welke verstoringen in welke IT-diensten hebben de grootste impact op de business? Wat zijn de oorzaken van deze IT-verstoringen? Hoe kunnen we deze IT-verstoringen oplossen of – nog beter – voorkomen? Welke quick wins

zijn er te halen?

- Meetwaarden: wat is het huidige gemiddeld aantal incidenten en de gemiddelde stortingstijd per dienst? Welke problemen liggen aan de meeste incidenten grondslag? Hoeveel wijzigingen worden doorgevoerd om deze problemen op te lossen? Wat is de stortingstijd die optreedt na implementatie van die wijzigingen?

KISS: keep IT, short and simple

Metrieken kunnen betrekking hebben op verschillende aspecten, uiteenlopend van harde meetbare zaken – zoals schijf- en geheugengebruik – tot meer zachte indicatoren: sfeer, cultuur, stijl van leidinggeven en dergelijke. Ondanks het verschil in de aspecten zijn de stappen op hoofdlijnen vergelijkbaar. Om te komen tot een meetsysteem zijn de volgende iteratieve stappen nodig.

- Maak doel en nut van het meten (bijvoorbeeld de rapportage) duidelijk vanuit een aantal perspectieven: gebruik hiervoor bijvoorbeeld de balanced scorecard.
- Wat zijn in mijn organisatie de kritieke succesfactoren?
- Zoek naar kritische prestatie-indicatoren (KPI's) die voor de business begrijpelijk, controleerbaar en beïnvloedbaar zijn en het liefst SMART (specifiek, meetbaar, aanwijsbaar, realiseerbaar en tijdsafhankelijk) zijn. Gebruik geen indicatoren die niets verduidelijken, zoals cpu-cycli, maar pas indicatoren toe die een relatie hebben met de gedefinieerde kritische succesfactoren.
- Bepaal de reikwijdte van het meetobject. Bijvoorbeeld bij processen: welke activiteiten zijn kritisch? Breng de activiteiten die tot het proces behoren goed in kaart. Een voorbeeld bij techniek: welke servicecomponenten zijn kritisch voor het ondersteunende bedrijfsproces? Wat is dan de zwakste schakel in de keten? Dit vereist inzicht in de opbouw van de IT-infrastructuur.
- Richt een meetsysteem in: als je weet welke gebeurtenissen je vastgelegd wilt hebben, leg ze dan vast en aggregeer de gegevens.
- Stel de drempelwaarden vast: welke maatregelen moeten wanneer worden genomen en rapporteer die. Rapporteer zeker bij overschrijding van die drempelwaarden ('report by exception'). Tip bij beveiliging: definieer bij overschrijding

Geen inzicht in de samenhang van processen leidt tot suboptimalisatie

Plateau - <i>Adagium</i>	Te ondernemen stappen	Producten
Plateau 0 <i>Wat is er?</i>	- WAT meet ik nu? - Analyse van de processen, systemen - Inventarisatie IT-infrastructuur	- Raamwerk - Overzicht bestaande situatie
Plateau 1 <i>Metten = weten</i>	- WAAROM wil ik wat meten? - HOE meten? - Inrichten monitoring/rapportage	- Meetplan of meetmatrices - Selectie KPI's - Structureel overleg met de business
Plateau 2 <i>Van weten naar reageren</i>	- WIE onderneemt WELKE actie? - Bepalen drempelwaarden en deze koppelen aan escalatie of verbeteracties - Acties voor korte termijn ('quick wins) definiëren	- Actieplan korte horizon - Voorgedefinieerde tegenmaatregelen - Projecten
Plateau 3 <i>Van reageren naar vooruitzien</i>	- WANNEER... - Trendanalyses uitvoeren - Uitzonderlijke momenten (bijvoorbeeld piekbelasting) analyseren - Focus op bottlenecks en SPOF's - Langetermijnacties definiëren	- Informatieplan - Actieplan lange horizon - Programma's
Plateau 4 <i>Van vooruitzien naar pro-activiteit</i>	- ALS... DAN - Vertalen van trends naar toekomstige dienstverlening - Actief beïnvloeden van de vraag naar IT-diensten	- Integratie van IT-en business-strategie - IT onderdeel van business plan

tabel 1 Groeimodel van meten

van kritische drempelwaarden geautomatiseerde acties of een actief alerting systeem. In het weekeinde is de frequentie van hackpogingen namelijk het hoogst en de bemensing van beheer het laagst.

- Stel vast dat rapportages ook daadwerkelijk door de betrokken medewerkers worden ontvangen, gelezen en begrepen. Is dat niet zo, pas de rapportages dan direct aan.
- Borg dat er iets gedaan wordt met de rapportage. Neem de verbeteracties op in de rapportage en analyseer en controleer in hoeverre de ondernomen acties daadwerkelijk hebben bijgedragen aan het bereiken van het gestelde doel.
- Evalueer of de rapportage ook bijdraagt tot een inzicht in de (verhoogde) toegevoegde waarde van IT voor de business. Waren de kritische momenten van de afgelopen periode zichtbaar in de rapportage? Zijn er aanpassingen nodig in de doelstellingen, de kritieke succesfactoren of de KPI's, de drempelwaarden of het meetinstrument?

Kiezen van het juiste ambitieniveau

Een grote valkuil bij het inrichten van een meet- of monitoringsysteem is om in één keer "alles" te willen meten – in de zin van alles wat er te meten valt. Hoe kan de IT-organisatie ervoor zorgen dat zij niet een te grote broek aantrekt? Het definiëren van plateaus kan helpen keuzen te maken,

zodat een groeimodel ontstaat. Daarin verschuiven stapsgewijs de adagiums naar een hoger doel naarmate de tijd verstrijkt (zie tabel 1). Zo'n model is bedoeld om een perspectief voor de toekomst te schetsen en de acties op korte termijn te focussen en het meetsysteem KISS te houden.

Veel instrumenten, terughoudend met meten

Het meten van de echte toegevoegde waarde van verbeteracties vereist voor veel IT-organisaties dat zij betere statistieken gebruiken. Stuurinformatie is wel het laatste waarop een IT-organisatie moet bezuinigen. Want dan gooit zij haar middelen weg die kunnen aantonen of zij wel effectief en efficiënt bezig is. De kernvraag moet zijn: hebben wij de juiste stuurinformatie? Sturen met inzicht vereist zowel een duidelijke visie en een strategie, om te bepalen waar je naartoe wilt, als een investering in de juiste meetinstrumenten, om te bepalen of je op de goede weg bent. Sturen is een kunst. Sturen vereist namelijk een goede communicatie om een vertaalslag te maken van de metingen naar de verbeteracties. De metingen moeten goed operationeel gemaakt zijn in de organisatie. Met de Apollo 13 is het indertijd toch nog goed afgelopen, doordat men de juiste zaken heeft gemeten, tijdig escaleerde ("Houston, we have a problem...") en gezamenlijk de goede corrigerende maatregelen wist te treffen.

Literatuur

ITIL in de praktijk, Nick Bakker en Louk Peters, ten Hagen & Stam Uitgevers, 2002, ISBN 90-440-0298-8

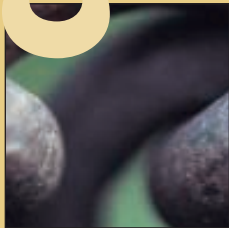
Implementatie IT service management, Louk Peters, ten Hagen & Stam Uitgevers, 2003, ISBN 90-440-0684-3

Referenties

1. Business Intelligence Monitor 2003 van SAS
2. Zie *ITIL in de praktijk*
3. Het GQM-paradigma is ontwikkeld in de jaren tachtig door Victor Basili van de Universiteit van Maryland, USA.

Louk Peters, Nick Bakker en Martin van Vuure zijn consultant bij PinkRocade.

Zij zijn bereikbaar via L.Peters@pinkroccade.com.



Op zoek naar de zwakste schakel

Rekenen aan netwerkbeschikbaarheid

Rapporteer over de behaalde beschikbaarheid van een netwerk en weeg de ernst van storingen mee. Peter Hasperhoven presenteert een definitie en een model waarmee je die opdracht kunt uitvoeren. De behaalde beschikbaarheid kan dan afgezet worden tegen wat in de SLA is afgesproken. Daarnaast is het model te gebruiken om de beschikbaarheid te voorspellen en dus om het netwerkontwerp te verbeteren.

Hoge beschikbaarheid van infrastructuur is een steeds vaker gehoorde eis. Eigenlijk moet een netwerk natuurlijk altijd en volledig beschikbaar zijn, maar iedereen snapt dat dat nu eenmaal niet haalbaar is. Daarom wordt doorgaans een wisselend aantal negens geclaimd. Hierbij wordt met enig ontzag gekeken naar de *five nines* (99,999% uptime) waarmee vooral grote providers graag schermen. Maar in de praktijk is het voor een gegeven netwerk moeilijk in te schatten wat de beschikbaarheidsverwachtingen zijn, en omgekeerd, voor een geëiste beschikbaarheid het netwerk zodanig te ontwerpen, dat het voldoende betrouwbaar is zonder de redundantie zwaar te overdimensioneren.

Onduidelijk

Het overwaaien van beschikbaarheidsgaranties uit de providerwereld heeft één groot nadeel: vaak is niet duidelijk wat ermee bedoeld wordt. Traditioneel wordt de beschikbaarheid meestal van een point-to-point verbinding gegeven, of zelfs van een telefooncentrale (single point), maar wat is de beschikbaarheid van een netwerk dan?

Als 'alles het doet', is deze vraag niet zo moeilijk te beantwoorden. Dan is het netwerk beschikbaar. En als de spanning in het hele gebouw, inclusief de computerruimte,

is uitgevallen, is het ook duidelijk: beschikbaarheid nul. Maar hoe ga je om met het uitvallen van een verdieping, terwijl alle andere gebruikers gewoon doorwerken, of met het uitvallen van één verbinding voor een werkstation? Kun je dat tellen als downtime en er dus de netwerkbeheerder op afrekenen als het te lang duurt?

Vaak is niet duidelijk wat met

'beschikbaarheidsgaranties' wordt bedoeld

Definitie van beschikbaarheid

Om een definitie van beschikbaarheid te krijgen die de ernst van de storing meeweegt in de impact op de prestaties, gaan we uit van het aantal productieve uren dat met een netwerk gerealiseerd kan worden. Het maximale aantal uren is dan het aantal aansluitingen vermenigvuldigd met het aantal uren in een jaar. De beschikbaarheid over een jaar wordt dan gedefinieerd als het aantal geleverde productie-uren gedeeld door het maximale aantal productie-uren. Hiervoor wordt onderstaande formule gebruikt:

$$\text{Beschikbaarheid} = \frac{\text{Uren}^{\text{max}} - \text{Uren}^{\text{storing}}}{\text{Uren}^{\text{max}}}$$

Bijvoorbeeld: uitgaande van 7×24 -productie gaan er in een jaar $365 \times 24 = 8.760$ uren. Een netwerk van duizend aansluitingen kan dus maximaal 8.760.000 productie-uren leveren. Wanneer nu in een jaar één keer het hele netwerk een uur down is geweest, levert dat verlies van duizend productie-uren op. Een storing van een etmaal, waarbij vijftien aansluitingen betrokken zijn geweest, levert een verlies van $15 \times 24 = 360$ uren op. En telt dus minder zwaar. De beschikbaarheid is dan:

$$\text{Beschikbaarheid} = \frac{8.760.000 - (1.000 + 360)}{8.760.000} = 99,984 \%$$

Dat valt mee!

Dit is een uitstekend mechanisme om in een SLA-rapportage te gebruiken. In tabel 1 is bijvoorbeeld een maandrapportage met cumulatieve beschikbaarheid weergegeven.

Van meten naar voorspellen

De volgende vraag is nu hoe we deze storingsuren kunnen voorspellen, zodat we het ontwerp erop kunnen aanpassen. Het grootste deel van het antwoord op die vraag zit in de Mean Time Between Failure (MTBF). Dit is een schatting die fabrikanten van apparatuur maken. De MTBF geeft het gemiddelde aantal uren aan dat een type apparaat zonder storingen draait. Als een apparaat bijvoorbeeld een MTBF van 40.000 uur heeft, gaat het gemiddeld eens in de $40.000/8760 = 4,6$ jaar stuk (ofwel $8760/40.000 = 0,2$ storingen per jaar). Als een netwerk zes van deze apparaten bevat, kan gemiddeld op $6 \times 0,2 = 1,2$ storingen per jaar gerekend worden.

En als we dan ook nog weten hoeveel gebruikers gemiddeld door zo'n storing getroffen worden en hoelang die gemiddeld duurt (uitgedrukt in de Mean Time To Repair of MTTR), kunnen we berekenen hoeveel verloren productie-uren dat veroorzaakt.

Als illustratie nemen we het netwerk volgens figuur 1. Dit netwerk bestaat uit een modulaire Ethernet-switch als collapsed backbone in de Main Equipment Room (MER), met Gigabit Ethernet-verbindingen gekoppeld aan stackable 100Mbps-switches

tabel 1 Een maandrapportage met cumulatieve beschikbaarheid.

Hierin is:

- **duur:** hoe lang de betreffende storing heeft geduurd in minuten;
- **gebruikers:** het aantal gebruikers/aansluitingen dat door de storing getroffen is;
- **storingsuren:** het aantal door de storing uitgevallen productie-uren (duur \times gebruikers / 60). Bij het cumulatieve overzicht is dit het aantal storingsuren van de betreffende maand;
- **max. uren:** maximaal aantal productie-uren in de betreffende maand ($24 \times$ het aantal dagen in die maand \times het aantal gebruikers);
- **beschikbaarheid:** volgens de gegeven formule (max. uren – storingsuren) / max. uren.

Beschikbaarheidsrapportage maand april 200X

Omschrijving storingen

Datum	Omschrijving	Duur (min)	Gebruikers	Storingsuren
10-apr	SER-switch <...> defect vervangen door leverancier	227	31	117.3
14-apr	Stroomstoring MER-switch	5	1200	100.0
Totaal storingsuren				217.3
Max. uren				864000
Beschikbaarheid				99.975%

Cumulatief

Maand	Dagen	Storingsuren	Max. uren	Beschikbaarheid
Januari	31	125.2	892800	99.986%
Februari	28	198.6	806400	99.975%
Maart	31	24.0	892800	99.997%
April	30	217.3	864000	99.975%
TOTAAL	120	565.1	3456000	99.984%

in de Satellite Equipment Rooms (SER's). Er zijn 8 SER's. De aansluitingen van de SER's zijn verdeeld over twee glasvezelborden van de MER-switch. Alle servers zijn op een derde glasvezelbord in de MER-switch gekoppeld. Via de SER's zijn vijfhonderd werkplekken aangesloten. In elke SER is een stack van drie gekoppelde, 24-poorts, Ethernet-switches geïnstalleerd. De eerste in die keten van SER-switches heeft een verbinding met de MER-switch. Het netwerk wordt dag en nacht gebruikt, en idealiter is het dus 7 x 24 uur beschikbaar.

Dit netwerk kent geen enkele vorm van redundantie. De MER-switch is een duidelijk *single point of failure*.

Tabel 2 geeft de onderdelen met hun MTBF, MTTR en de daaruit voortvloeiende impact op storingsuren.

Uit tabel 2 blijkt in de eerste plaats dat een netwerk zonder enige vorm van redundantie toch al een redelijke beschikbaarheid haalt. Maar verder is in de tabel vooral af te lezen welke componenten de grootste impact hebben op de beschikbaarheid en waar dus de meeste winst te halen valt bij het verbeteren van de betrouwbaarheid van het netwerk.

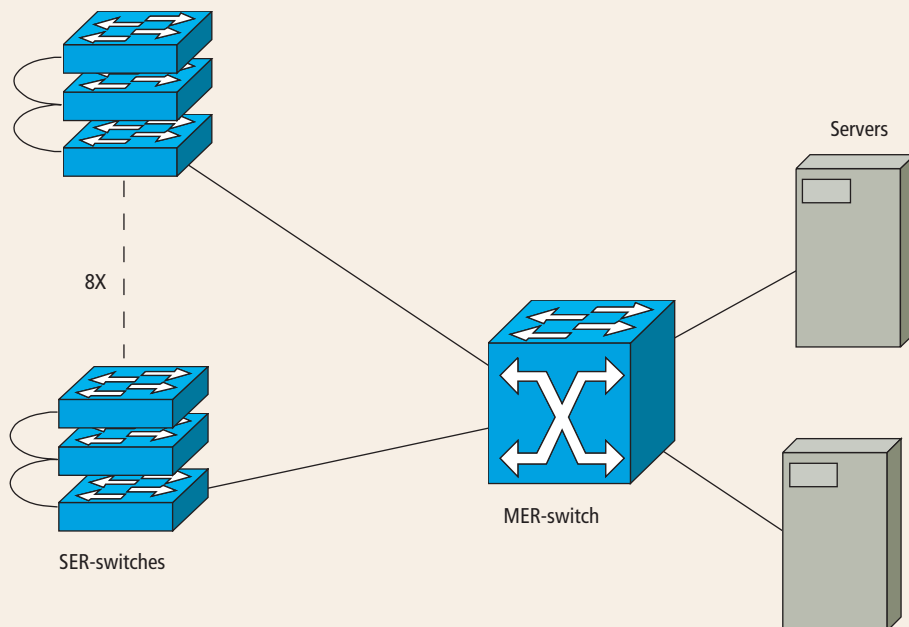
Storingsimpact verlagen

In dit voorbeeld wordt de grootste bijdrage in storingsuren geleverd door de SER-switches en de voeding van de MER-switch. Er zijn in principe twee manieren om deze impact omlaag te krijgen:

- verlaging van de MTTR;
- verlaging van het aantal gebruikers dat geraakt wordt.

Een manier om de MTTR naar beneden te krijgen is een betere afspraak met de leverancier, of het zelf op voorraad houden van een of meer reserve-onderdelen. Door een SER-switch op de plank te hebben, is de MTTR eenvoudig naar één uur te krijgen, vooropgesteld dat een storing tijdig gesignaleerd wordt.

Daarnaast kan in het geval van de SER-switches het aantal gebruikers dat per storing wordt beïnvloed omlaag. Door de switches in een stack niet in een keten, maar in een ring te verbinden (met andere woorden door ook een verbinding van de eerste naar de derde te maken) daalt het aantal gebruikers dat last heeft van een storing van 42 naar 21.



figuur 1 Netwerk voor het rekenvoorbeeld

Component	Aantal	Aantal gebruikers	MTBF	Storingen per jaar	MTTR	Storingsuren
MER-chassis	1	500	1000000	0.0088	24	105
MER-voeding	1	500	40000	0.2190	24	2628
MER-controller	1	500	100000	0.0876	24	1051
MER-Gbps-bord -> SER's	2	250	250000	0.0701	24	420
MER-Gbps-bord -> Servers	1	500	250000	0.0350	24	420
SER-switch	24	42	75000	2.8032	24	2826
SER-Gbps-module	8	63	250000	0.2803	24	424
Uren per jaar	8760					7875
Max. uren	4380000					
Storingsuren						7875
Beschikbaarheid						99.820%

tabel 2 De onderdelen van figuur 1 met hun MTBF, MTTR en de daaruit voortvloeiende impact op storingsuren.

Hierin is:

- **component:** de onderdelen van het netwerk, zoals beschreven;
- **aantal:** het aantal componenten van elk type in het hele netwerk;
- **aantal gebruikers:** aantal aansluitingen dat (gemiddeld) last heeft van een storing in de betreffende component. Merk op dat dit voor een SER-switch op 42 is gesteld: per switch zijn gemiddeld 21 gebruikers aangesloten, maar wanneer de eerste switch van een stack kapotgaat (die met de backbone-aansluiting dus), is de hele stack uitgeschakeld; wanneer de middelste switch stuk gaat, zijn twee switches onbereikbaar, en als de laatste stuk gaat, heeft alleen die laatste er last van. Gemiddeld dus twee switches oftewel 42 gebruikers;
- **MTBF:** gemiddelde tijd tussen twee storingen in uren. De gegeven getallen zijn voorbeelden, maar wel gemodelleerd naar werkelijke getallen van grote fabrikanten;
- **storingen per jaar:** aantal storingen in de betreffende component die per jaar verwacht mogen worden (aantal uren per jaar/MTBF x aantal componenten);
- **MTTR:** gemiddelde hersteltijd, in dit geval op 24 uur gesteld. Dit kan bijvoorbeeld betekenen dat er een contract is met een leverancier die binnen 24 uur een vervangende component moet leveren;
- **storingsuren:** aantal uren per jaar dat gebruikers niet kunnen werken als gevolg van storingen in deze component (kans op storingen x MTTR x aantal gebruikers).

De voorspellende waarde van het model is beperkt, omdat het met statistische aannamen werkt

Verlaging van de MTTR kan ook door een component dubbel uit te voeren, waarbij de reservecomponent de taak van de primaire component overneemt. In het geval van de voeding van de MER-switch is dit goed mogelijk. De bijdrage van de MTTR gaat dan zelfs naar nul of in elk geval bijna naar nul.

Ook de controller (zeg maar het moederbord) van de MER-switch kan wellicht dubbel uitgevoerd worden. Daarbij zal de MTTR niet naar nul gaan, omdat zo'n controller doorgaans een paar minuten nodig heeft om op te starten en de configuratie over te nemen. Maar 0,1 uur (zes minuten) is een redelijke schatting. Al die maatregelen samen geven het effect dat wordt weergegeven in tabel 3.

Component	Aantal	Aantal gebruikers	MTBF	Storingen per jaar	MTTR	Storingsuren
MER-chassis	1	500	1000000	0.0088	24	105
MER-voeding	1	500	40000	0.2190	0	0
MER-controller	1	500	100000	0.0876	0.1	4
MER-Gbps-bord -> SER's	2	250	250000	0.0701	24	420
MER-Gbps-bord -> Servers	1	500	250000	0.0350	24	420
SER-switch	24	21	75000	2.8032	1	59
SER-Gbps-module	8	63	250000	0.2803	24	424
Uren per jaar	8760					1433
Produktieuren	4380000					
Storingsuren	1433					
Beschikbaarheid	99.967%					

tabel 3 Effect van de maatregelen

Er is een verlaging van de niet-beschikbaarheid van 0,18 % naar 0,03 % bereikt, oftewel een verbetering met een factor 6. Een volgende verbetering zou bijvoorbeeld bereikt kunnen worden door ook voor de onderdelen die nu de meeste impact hebben (MER-glasvezelborden en SER-backbone-modules) een reserve op voorraad te nemen.

Ontwerpoverwegingen

Natuurlijk is het model zoals dat hier gepresenteerd is, nogal schetsmatig. Het kan bijvoorbeeld nodig zijn om niet met een 24-uurs beschikbaarheid te rekenen,

De tijden achter de percentages

Argeloze gebruikers roepen vaak, als zij voor het eerst met dit soort rekenwerk geconfronteerd worden, dat het netwerk natuurlijk wel 99% beschikbaar zijn. Dat is min of meer spreekwoordelijk voor vrijwel altijd. Ze schrikken dan vaak wel als wordt uitgelegd dat 99% betekent dat het gehele netwerk 3,65 dag per jaar down mag zijn zonder dat dat erg gevonden wordt. Dan gaan de eisen snel omhoog.

Bij gesprekken over dit soort percentages is het goed om na te denken hoeveel downtime er eigenlijk achter die percentages zit. In tabel 4 is onmiddellijk te zien dat 99% beschikbaarheid voor de meeste toepassingen te weinig is (bovendien kan elk beetje serieus netwerk dat niveau op z'n sloffen halen), maar dat het andere uiterste – 99,999% – meestal wel erg ambitieus en daarmee duur uitvalt.

Beschikbaarheid	Downtime per jaar
99 %	87 uur
99,9 %	8,7 uur
99,99 %	53 minuten
99,999 %	5,3 minuten

tabel 4 Aandeel beschikbaarheid uitgedrukt in absolute duur

maar alleen te kijken naar kantooruren. Voor de SLA-rapportage is dat een min of meer triviale aanpassing: het maximaal aantal uren dat het netwerk beschikbaar is, wordt lager, en voor de storingsuren moeten alleen de uren binnen kantooruren worden meegerekend. Voor de ontwerpoverwegingen komt er iets meer bij kijken. De impact is daar een beetje afhankelijk van hoe er buiten kantooruren met storingen wordt omgegaan. Als het onderhoudspersoneel bijvoorbeeld in geval van een storing ook 's avonds doorwerkt, hebben storingen die kort voor het einde van de werkdag worden opgemerkt minder impact dan storingen die midden op de dag ontstaan. En storingen die 's nachts optreden en direct opgemerkt en verholpen worden, hebben misschien wel helemaal geen impact. Daarmee moeten de opstellers van de SLA-rapportage dan rekening houden.

Het model is verder makkelijk uit te breiden met andere componenten, zoals servers, werkstations of zelfs applicaties. Het is alleen vaak wel lastiger om van een applicatie de MTBF te achterhalen.

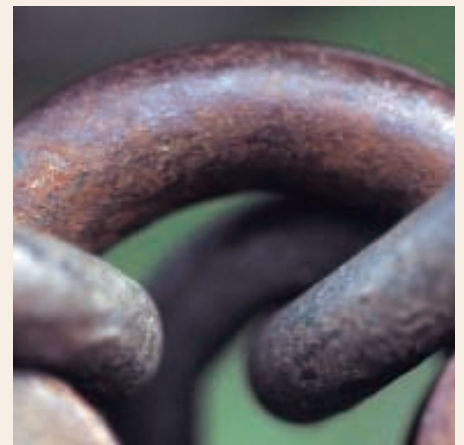
Ten slotte: de voorspellende waarde van het model is vanzelfsprekend indicatief, want statistisch. Een op grond van MTBF's voorspelde beschikbaarheid is daarom bruikbaar om de kwetsbare punten in het netwerk te identificeren en te verbeteren,

bij het vaststellen van SLA's op basis van zo'n voorspelling is voorzichtigheid geboden. Een storing die gemiddeld eens in de tien jaar voorkomt, heeft die ene keer wel tien keer de impact die in de voorspelling voor een jaar gerekend wordt. Dat betekent dat het model beter werkt voor grotere netwerken, omdat daar meer gelijksoortige componenten voorkomen.

Objectieve maatstaf

Het in dit artikel voorgestelde model is uitermate geschikt voor twee doeleinden. Ten eerste is het gebruik van verloren productie-uren een objectieve, goed te gebruiken maatstaf om de beheerder van uw netwerk te laten rapporteren wat de werkelijke behaalde beschikbaarheid is. Ten tweede kan het bij het ontwerpen of verbeteren van het netwerk gebruikt worden om de zwakste schakel te identificeren en maatregelen tegen uitval hiervan te treffen. Dit model kan ook prima in een offerte-aanvraag verwerkt worden, waarbij de leverancier gevraagd wordt een ontwerp te maken of aan te passen, zodat de vereiste beschikbaarheid gehaald kan worden.

Peter Hasperhoven is werkzaam bij Verdonck, Klooster & Associates in Zoetermeer en is bereikbaar via peter.hasperhoven@vka.nl.



Er wordt met enig ontzag naar de 'five nines' gekeken



Met een kleine investering een doeltreffende procesinrichting

Change proces in een kleine organisatie

ITIL wordt de laatste jaren minder dwangmatig of strikt gehanteerd bij ontwerp en implementatie van de processen. Pragmatiek wint aan populariteit – of het nu gaat om de diepte of de breedte van IT service management. Zo worden niet alle processen geïmplementeerd. Ook blijken organisaties met een verschillende detaillering in de geïmplementeerde processen goed overweg te kunnen. Maar minder grote bedrijven zijn om allerlei redenen huiverig om met ITIL aan de slag te gaan. Dat is niet nodig. Eenvoudig kan ook zeer doeltreffend zijn, zo bleek bij invoering van change management door Levob Bank & Verzekeringen.

De inrichting van Change Management bij Levob, volgens de algemene beschrijving van het proces in ITIL-terminen, staat in dit artikel centraal. Het begon allemaal heel herkenbaar. Vanuit de afdeling Systeem Ontwikkeling (SO) kwamen te veel en te hardnekkige signalen dat wijzigingen onvoldoende of niet gecommuniceerd werden. Veranderingen werden toevallig ontdekt en het oplossen van problemen kostte buitensporig veel tijd. In de ICT-organisatie hebben wijzigingen in de infrastructuur geregeld tot onaangename verrassingen geleid, zowel in de business als in de ICT-organisatie zelf.

Eenvoudig, snel en goedkoop

De situatie bij Levob mondde uit in een voorstel om change management in te richten. Maar niet zonder een duidelijke randvoorwaarde. Invoering moest eenvoudig, kort en met beperkte inzet van hulpmiddelen gebeuren.

Tijdens de voorbereiding stelde men enkele condities vast voor een succesvolle implementatie:

- Er bestaat een knelpunt dat breed ervaren wordt, of er is sprake van een breed in de organisatie gedragen verbeterdoelstelling.

- Er is een beslisser in de organisatie die eigenaar wordt van het veranderingstraject.
- De organisatie is bereid tot verandering en steunt de bovengenoemde eigenaar. Bij de inrichting en uitvoering van het traject zijn deze condities zorgvuldig bewaakt.

De uitvoering

De eerste vaststelling vergde in de voorbereiding veel tijd. De manager Technische Infrastructuur (TI) heeft zelf het initiatief genomen en het contact met de betrokken medewerkers in de afdeling SO gelegd. In eerste instantie kon hij alleen maar luisteren naar de 'brede ervaringen', omdat de irritatie over het knelpunt eerst geuit moest worden. Het gesprek is pas later gekomen.

Met de informatie uit deze contacten is de eigen afdeling geconfronteerd. Mensen hebben bewust tijd genomen om hun kritiek en de gemelde problemen met elkaar te bespreken, zonder meteen de oplossing te willen weten en te implementeren. Deze fase heeft gezorgd voor bewustwording. Ook werd begrip gekweekt voor de moeiten van de medewerkers. Daarmee werd een basis gelegd voor bereidheid om de werkwijze te veranderen.

Een tweede punt in deze fase van voorbereiding is de juiste omschrijving van het probleem geweest. Zowel voor de 'bena-deelden' als voor de uitvoerenden is het cruciaal dat de probleemstelling helder is en dat zij daarover overeenstemming hebben.

De probleemstelling werd uiteindelijk als volgt ingekaderd: TI bepaalt zelf *of* er geïnformeerd wordt over een wijziging, *wanneer* dat gebeurt en aan *wie*. Maar de praktijk toonde ruimschoots anders aan.

- Ten onrechte leefde binnen de organisatie de veronderstelling dat een wijziging geen gevolgen heeft voor gebruikers (ook SO wordt als gebruiker beschouwd).
- Informatie over de wijziging werd of te ruim vooraf of juist te kort voor de uitvoering gegeven. Soms kwam de informatie achteraf.
- Vaak werden te weinig betrokkenen geïnformeerd; de bedenker, de verantwoordelijke en de uitvoerder van de wijziging is meestal dezelfde persoon, wat leidt tot een verlies aan impactanalyse.



Cees Doets overhandigt systeembeheerder Rudy Brassier een module als symbolische verandering

Actief en passief informeren

Een oplossing werd relatief eenvoudig gevonden. Tijdens de gesprekken met de afdeling SO kwamen al diverse suggesties los. Het belangrijkste element uit de oplossingsrichting is: maak een groep gebruikers die *actief* geïnformeerd willen worden, door middel van e-mail, en maak een groep die *passief* geïnformeerd wil worden, door middel van een openbare map op Exchange.

Bij het doorspreken van de oplossing met de afdeling TI werd de noodzaak van deze werkwijze van actief en passief informeren ter discussie gesteld. Zou dit niet te bureaucratisch worden? Moet SO nu ook wijzigingen aankondigen?

Levob Bank & Verzekeringen

Levob Bank & Verzekeringen is de enige volledig zelfstandige bank/verzekeraar in Nederland die haar producten uitsluitend via onafhankelijke intermediairs aanbiedt. Het bedrijf is gevestigd in Leusden en telt ongeveer 450 medewerkers. De ICT-organisatie bestaat uit drie afdelingen: Systeem Ontwikkeling (SO), Technische Infrastructuur (TI) en Systeem Ontwikkeling/Technische Infrastructuur mainframe. De afdeling TI beheert Windows-, Unix- en Linux-servers, Oracle-databases, werkplekken en communicatie-apparatuur. Bij Levob ICT werken in totaal veertig medewerkers.

Microsoft
pagina 26

Microsoft
pagina 27

Alle inspanningen op een rij

Wat komt er kijken bij de invoering van Change Management? Onderstaand overzicht geeft een indruk van de omvang van het proces.

Procesontwerp

- Review van ITIL Change Management en downsizing van het proces naar de concrete behoefte: basis procesmodel voor Change Management, welke stappen en welke rollen
- Toewijzen van rollen aan functionarissen
- Vaststellen welke beschikbare hulpmiddelen voldoende ondersteuning bieden: MS Outlook
- Opstellen van templates ter ondersteuning van het proces

Afstemming

- Feedbackronde langs business en ICT-organisatie
- Fine tuning van procesontwerp en hulpmiddelen
- Finale goedkeuring

Realisatie

- Definitief maken van templates
- Inrichting van MS Outlook
- Overdracht proces aan betrokkenen in ICT-organisatie

Benodigde tijd

- Voorbereiding: twee sessies, totaal één dag
- Procesontwerp: één dag (in samenwerking met externe consultant)
- Afstemming: twee sessies en verwerking, één dagen
- Realisatie: opleveren documenten en hulpmiddelen, twee sessies, twee dagen

Nu was de tijd rijp om feedback te vragen van een specialist. Hoe zou die denken over het inrichten van de oplossing? Levobs belangrijke eisen en wensen waren:

- zorg ervoor dat het niet te bureaucratisch wordt;
- maak gebruik van bestaande tools en middelen;
- vermijd lange consultancy-trajecten;
- bereik een korte implementatietijd;
- realiseer dit zonder uitbreiding van FTE's.

De consultant moest de organisatie helpen een keuze te maken uit alle ITIL-elementen van het change management-proces. De kunst is zoveel mogelijk weg te laten en toch het probleem op te lossen. Uit het proces zijn die onderdelen weggelaten die voor een kleine organisatie geen toegevoegde waarde hebben, bijvoorbeeld de change-kalender en de change advisory.

Maatwerk

Change management bij Levob past compleet op drie A4-tjes en is maatwerk voor de eigen situatie. Het opgestelde proces bestaat uit vier onderdelen:

- aanvragen;
- voorbereiden en plannen;
- realiseren;
- evalueren.

Voor ieder onderdeel zijn alleen input, activiteiten en output vastgelegd, met nadrukkelijk de bijbehorende communicatielijnen. Een ander nieuw element in het proces is dat de uitvoerder van een wijziging verplicht wordt een collega te raadplegen, voordat de wijziging uitgevoerd mag worden.

In Exchange is een map Changes aangeemaakt. Hierin bevindt zich de procedure en tevens een template voor het aanmaken van een wijziging.

Passief informeren is gerealiseerd door een groep personen leesrechten te geven op deze map. Het bericht dat in de map Changes staat, moet de passief geïnformeerde medewerker zelf opzoeken. Voor het actief informeren is een verzendlijst in Exchange gemaakt. Het bericht in Changes wordt verstuurd aan iedereen die op de verzendlijst staat. Simpel!

Onder de map Changes hangen vier sub-mappen, die de status van de wijziging aangeven: Aangevraagd, In behandeling, Afgerond en Afgewezen. Over deze oplossing zijn SO en TI het samen eens geworden. Zie figuur 1.

Implementatie

Alle geplande wijzigingen zijn meteen ingebracht. Stap voor stap wordt de procedure door steeds meer betrokkenen gebruikt. Het lijnmanagement stimuleert en bewaakt de uitvoering van het proces. Het wekelijkse operationele overleg biedt voldoende gelegenheid om bij te sturen. De afdeling TI toonde zich aanvankelijk terughoudend in haar verwachting of iedere medewerker wel gediend zou zijn van de vele nieuwe e-mails. Maar de afdeling SO wist TI ervan te overtuigen dat zij ze graag willen zien.

Een grote groep gebruikers is van het begin af op de actieve verzendlijst geplaatst. Naarmate de tijd vordert en met het communicatie-aspect in change management ervaring wordt opgedaan, evolueert de actieve verzendlijst tot de uiteindelijk in de praktijk gewenste lijst.

Goed voorbeeld

De klachten zijn voorbij en van irritaties is geen sprake meer. De afdeling TI beschikt over een beter overzicht van de uitstaande



Onderwerp: 2003-xx (omschrijving):

Systeem/infrastructuur-component: NT-server

Status: Aangevraagd / In behandeling (Impact, Bouw, Planning, Realisatie) / Afgerond / Afgewezen

Datum aanvraag:
 Geplande datum change:
 Definitieve datum change:

Aanvrager:
 Uitvoerder:
 Eigenaar: Cees Doets
 Consultant(s):
 Acceptant:

Algemene opmerkingen:

Korte omschrijving impactanalyse:

Bijzonderheden implementatie:

figuur 1
 Template wijziging aanmaken

wijzigingen, het nieuwe proces borgt meer kwaliteit in zichzelf en door de 'communicatieplicht' wordt het risico van onvoorziene impact van een wijziging verkleind. De hoofdrolspelers in de ICT gebruiken het nieuwe proces. Er gaat een positieve werking van uit naar de gehele ICT. Een goed voorbeeld doet goed volgen, is de overtuiging die nu heerst. In relatief korte tijd is met een beperkte inspanning een wezenlijke verbetering gerealiseerd.

Ir. Cees Doets is manager van de afdeling Technische Infrastructuur van Levob en verantwoordelijk voor het change management; hij kan bereikt worden via ceesdoets@levob.nl.

Drs. Ad J. Zoet is managing consultant bij Formatie IT Control en is als extern adviseur betrokken bij de beschreven case; hij is bereikbaar via a.zoet@formatie.nl.

Glidepath
pagina 30



Eerste ervaringen, literatuur en certificaten rondom MOF komen los

Acceptatie Microsofts beheerframework in cruciale fase

Binnen het werkveld IT-beheer is de IT Infrastructure Library (ITIL) zo goed als de absolute referentie voor de inrichting van beheerprocessen. Het introduceren van een nieuw of zelfs maar aanvullend gedachtegoed is in het verleden meer dan eens stukgelopen. Zelfs aanvullingen en wijzigingen op de bestaande ITIL-stof worden maar moeizaam geaccepteerd. Microsoft haalt daarom een behoorlijke tour de force uit met de introductie van haar Microsoft Operations Framework (MOF). Dit artikel gaat in op het MOF, op de overeenkomsten en verschillen tussen MOF en ITIL en laat alvast een licht schijnen op de eerste ervaringen in het werkveld met deze materie.

MOF is het antwoord van Microsoft op de vraag hoe de IT-organisatie ervoor kan zorgen dat de kwaliteit van haar services, gebouwd op Microsoft-technologie, op het gewenste peil blijft. Het framework is specifiek voor beheer en exploitatie van Windows-technologie ontwikkeld en levert concrete bouwstenen (zoals kant-en-klare procesdocumentatie), waarmee organisaties bedrijfskritische omgevingen kunnen beheren. MOF bestaat deels uit ITIL en is verrijkt met een aantal specifieke componenten van Microsoft voor de inrichting van de beheerprocessen. Microsoft bouwt bewust voort op ITIL en stelt dat zij ITIL zowel adopteert als adapteert. Hierin verschilt de strategie dus al van de gesneuvelde voorgangers. En dit zou een belangrijke succesfactor kunnen worden. Het bedrijf uit Redmond wil dan ook niet concurreren met ITIL en zorgt er behoedzaam voor dat het ITIL Foundations-certificaat een basisvoorwaarde is voor het mogen volgen van MOF-opleidingen.

Het Operations Framework bestaat uit drie modellen: het procesmodel, het teammodel en het risicomodel. Alledrie hebben ze enerzijds veel raakvlakken met ITIL en anderzijds deels hun wortels in andere con-

Geen proefballon meer

Microsoft mikt met haar beheerstrategie duidelijk op een plek in de *enterprise arena* en wil daar een belangrijke speler worden. Daarnaast stellen de huidige economische spelregels eisen aan beheerbaarheid en beheerkosten van de strategische infrastructuren. De producten en diensten die Microsoft op dit gebied uitbrengt, onder de paraplu van de Microsoft Solutions for Management, zijn een duidelijk teken dat Big Greens bedoelingen serieus zijn. Er is duidelijk geen sprake meer van een proefballonnetje, zoals enkele jaren geleden, toen een eerste release van het MOF bijna even snel verdween als het verscheen.

cepten van Microsoft, zoals het Microsoft Solutions Framework. Dit geldt vooral voor het teammodel en het risicomodel. Binnen het procesmodel bevindt zich echter een aantal nieuwe zaken, die verder in dit artikel worden toegelicht.

Waarom MOF

Organisaties die hun bedrijfskritische processen automatiseren, stellen hoge eisen aan betrouwbaarheid en beschikbaarheid. De Microsoft-producten, zoals Windows 2000, worden steeds vaker ingezet als platform voor deze processen en de systemen daarvoor. Dit stelt hoge eisen aan deze producten, die nog altijd worden omgeven door al dan niet terechte stekelige opmerkingen over blauwe schermen des doods. Om de gewenste vijf negens (99,999% beschikbaarheid) te halen moet Microsoft haar platforms tot de 'best in class' laten behoren. Microsoft ziet professioneel beheer van de IT-omgeving als een van de voorwaarden om dit te kunnen realiseren. Door de beheerorganisatie in te richten aan de hand van de principes van Microsoft Operations Framework moeten

end-to-end diensten worden geboden en gemanaged, op basis van processen en procedures, in plaats van het beheren van slechts de servers en andere technologie. Ook zegt Microsoft te beseffen dat organisaties IT wendbaar (*agile*) willen inzetten. Zo kunnen ze snel maar betrouwbaar op veranderende situaties kunnen inspelen. Deze *agility* is door alle strategieën van Microsoft geweven, van architectuur tot beheer.

Overeenkomsten en verschillen

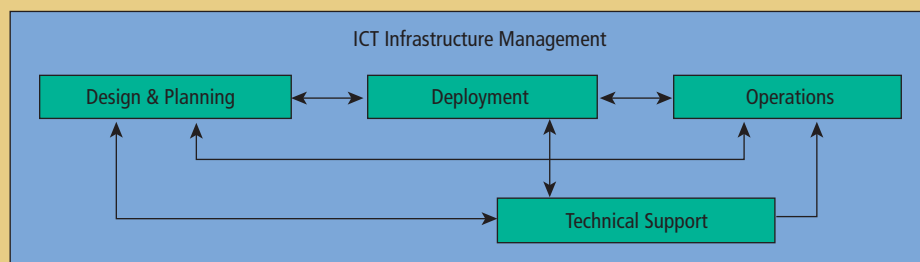
Microsofts keuze voor ITIL als basis van het Operations Framework is ingegeven door de wens om de al bestaande best practices te verstevigen en uit te bouwen. Naar mening van Microsoft is ITIL het afgelopen decennium een succesvolle best practice gebleken en zou het onverstandig zijn om niet hierop verder te bouwen.

De belangrijkste bouwsteen van MOF is het procesmodel. Dit model toont twintig beheerprocessen in een sequentiële volgorde, die zijn gebundeld in kwadranten: Changing, Operating, Supporting en

Zoek de verschillen: ICT Infrastructure Management naast MOF

Leo van Selm

MOF vult een gat in ITIL, precies daar waar het gaat om het continue operationele beheer. Begin dit jaar kwam het nieuwe ITIL-boek *ICT Infrastructure Management* uit. Zou dit boek het 'gat' vullen en hoe verhoudt zich dat dan met MOF? Deze vraag intrigeerde de Beroepsgroep voor ICT Service Management en zij organiseerde een thema-avond. Leo van Selm verwoordt de conclusies.



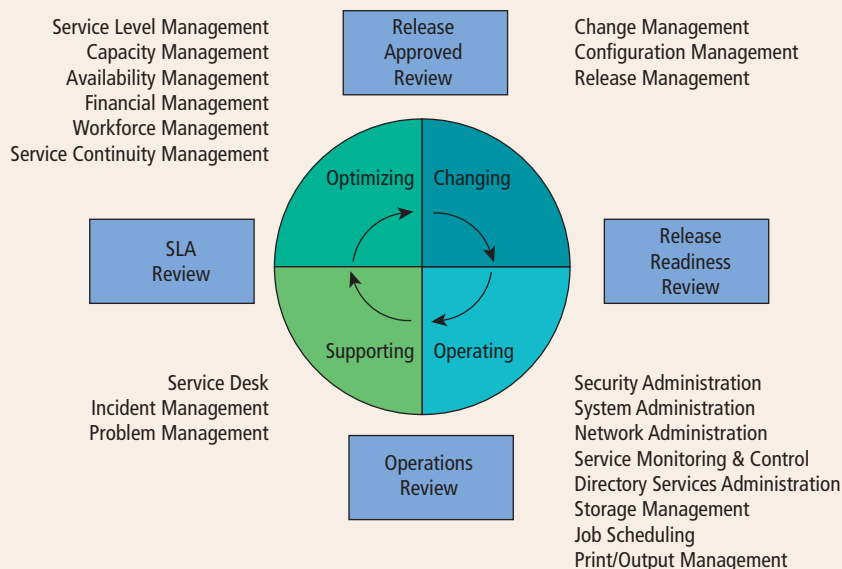
figuur 1 Processen van ICTIM

ITIL's ICT Infrastructure Management (ICTIM) beschrijft de processen van ontwerp tot en met het dagelijks beheer en onderhoud van de ICT-infrastructuur. Het wordt gepositioneerd als het fundament voor de (reeds lang bekende) processen voor support en delivery. Binnen ICTIM is een aantal processen gedefinieerd (zie figuur 1). Daarmee is de scope breder dan bij MOF. Maar ook MOF is een onderdeel van een bredere visie van het Microsoft IT Lifecycle-model (figuur 2).

Met name het ICTIM Operations-proces en de ondersteuning door het Technical Support-proces zijn te vergelijken met MOF. De processen binnen Operations zijn niet één op één hetzelfde als de operationele Service Management Functions (SMF's) binnen MOF. Een aantal is dat wel; zie de Engelstalige tabel 1.

Optimizing (zie figuur 1). De processen zijn grotendeels gelijk aan de bekende ITIL-processen uit de Support- en Delivery-boeken. In het Optimizing-kwadrant bevindt zich echter een nieuw proces: Workforce Management. Dit is een nuttig proces, aangezien dit zich specifiek richt op de opleidings- en kennismangementaspecten van beheerders.

Maar de grootste aanvulling zit wel in het Operating-kwadrant, waarin processen als Security Administration, Storage Management en Security Administration zijn ondergebracht. Deze geven een concrete invulling aan de voor veel mensen abstract gebleven ITIL-processen als Availability Management en Capacity Management. Ook zijn de Operating-processen relevant voor het dagelijkse werk, dat uit veel meer bestaat dan 'calletjes lopen en RFC's afhandelen'. Hoewel de processen sterk geënt zijn op Microsoft-technologie, diskwalificeert dat het Operating Framework absoluut niet; best practice-procesvoorbeelden moeten immers altijd worden aangepast aan de organisatie die ze implementeert.



figuur 1 MOF-procesmodel

Beginnen met MOF

Er zijn al enkele bedrijven bezig met het implementeren en inzetten van de operationele processen uit MOF. Met name bij *green field operations* lijkt dit goed te gaan.

Dit najaar komt er waarschijnlijk een erkend certificaat

MOF Foundations

Verskil tussen wat en hoe

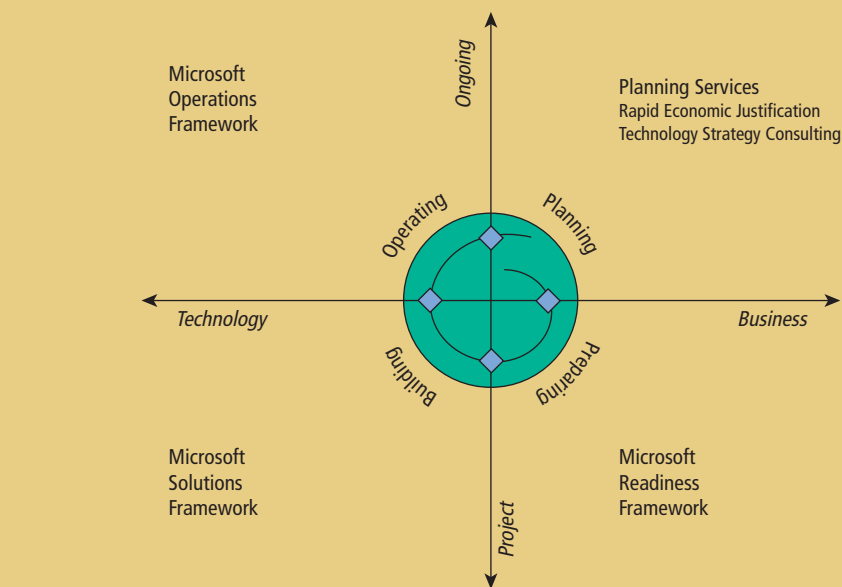
Binnen de beschrijving van de ICTIM Operations-processen wordt vooral benadrukt *wat* er moet gebeuren. MOF beschrijft *hoe* dingen uitgevoerd moeten worden. Daarbij richt MOF zich op de Microsoft-producten en geeft daar gedetailleerde instructies voor. Zie bijvoorbeeld de Windows 2000 Operations Guides op Microsoft Technet. Deze documenten zijn één op één toepasbaar als werkinstructies in een beheerhandboek.

ICTIM beschrijft in algemene zin *wat* er gedaan moet worden en is universeel toepasbaar.

Binnen ICTIM worden ook de rollen en verantwoordelijkheden beschreven, wat vergelijkbaar is met het teammodel van MOF. Ook hier bestaat weer een duidelijk verschil. MOF heeft een meer voorschrijvend karakter dan het beschrijvende karakter van ICTIM. Het risicomodel van MOF komt niet terug binnen het boek ICTIM.

Naslagwerk versus praktisch handvat

Samengevat is ITIL's ICT Infrastructure Management een naslagwerk en referentie voor het ontwerp, de ontwikkeling, de



figuur 2 Lifecycle-model van Microsoft

inrichting en de dagelijkse uitvoering van infrastructuurbeheer. Het is zeer goed toepasbaar bij het inrichten en optimaliseren van een IT-organisatie.

MOF is een pragmatisch en handzaam *framework*, dat directe invulling geeft aan de manier waarop je zaken moet aanpakken

en uitvoeren in een Microsoft-omgeving. Het valt dan ook te verwachten dat invoering van MOF binnen de kaders van ITIL concreet en snel resultaat geeft bij een 'rechttoe rechtaan' implementatie.

Organisaties die al wat langer bestaan, hebben er meer moeite mee – vooral doordat daar de bestaande functionele organisatie ‘in de weg’ zit. Het teammodel vormt binnen MOF een antwoord op de vraag hoe een beheerorganisatie kan worden vormgegeven. Hierbij wordt de oplossing gezocht in een rollenmodel, waarin zes rollen worden onderscheiden: Release, Infrastructure,

Support, Operations, Partner en Security (zie figuur 2). Deze indeling zorgt voor meer helderheid in een beheerorganisatie, onder de voorwaarde dat mensen ook daadwerkelijk binnen de kaders van hun rol hun taken uitvoeren. Een Release-medewerker is bijvoorbeeld meer projectgedreven en houdt zich niet bezig met Operations-taken. De Security-medewerker zorgt voor de vormgeving van en controle op de beveiligingsmaatregelen, die Infrastructure-medewerkers op hun beurt kunnen uitvoeren. Met name het opzetten van deze taakscheiding blijkt lastig in de praktijk, want het lijkt alsof de functie van een beheermedewerker daarmee wordt uitgediept. Niets is minder waar. Geregelde en gerichte job rotation van medewerkers over de rollen heen, onder aansturing van het Workforce Management-proces, kan het toch nog gevoelde leed aanmerkelijk verzachten. Het teammodel vormt dus een belangrijke meerwaarde ten opzichte van ITIL. De laatste zegt op de processen na niets over de organisatiemodellering. Een duidelijke omissie, waarover de laatste jaren veel discussie is geweest.

MOF a pocket guide

De documenten die het fijne van MOF beschrijven, bestaan uit een verzameling PDF-bestanden die niet altijd even handzaam zijn. Daarom is er recentelijk in Nederland een Engelstalige MOF Pocket Guide verschenen dat daarbij hulp biedt. Dit boekje vormt het begin van een reeks van publicaties rondom dit onderwerp. Dit jaar verwachten we in ieder geval nog een volwaardig beschrijvend boek over MOF, dat te vergelijken zal zijn met het bekende introductieboek service management van ITSMF.

ISBN: 9077212108.



ICTIM	MOF
Operational control and management of the services, components and their configurations Management of all ICT infrastructure events	<i>Service monitoring and control.</i> Observes the health of an IT service and acts when necessary to maintain compliance <i>Network administration.</i> Responsible for the design and maintenance of the physical components that make up the organization's network, such as servers, routers, switches, and firewalls
Workload and output management and scheduling	<i>Job scheduling.</i> Assigns batch processing tasks at different times to maximize the use of system resources while not compromising business and system functions <i>Print and output management.</i> Manages the costs and resources associated with business output and ensures security of sensitive output
Storage management, back-up and recovery	<i>Storage management.</i> Deals with on-site and off-site data storage for the purposes of data restoration and historical archiving and ensures the physical security of back-ups and archives
Management and control of all aspects of ICT operational security	<i>Security administration.</i> Responsible for maintaining a safe computing environment by developing, implementing, and managing security controls
Management of the supporting operational process	<i>Directory services administration.</i> Responsible for day-to-day operations, maintenance, and support of the enterprise directory <i>System administration.</i> Responsible for day-to-day tasks of keeping enterprise systems running and for assessing the impact of planned releases
Proactive operational management processes	–

tabel 1 Vergelijkbare processen in ICTIM en MOF

Is een bredere benadering van het traject van ontwerp tot en met operatie nodig in een grotere, heterogene omgeving, dan

is een aanpak van ‘out of the box’ vaak niet mogelijk. Hier is ICTIM een goede oplossing.

Leo van Selm is voorzitter van de beroepsgroep voor ICT Service Management en managing consultant bij PC-Ware Information Technologies. Hij is bereikbaar via leo@vanselm.nl.

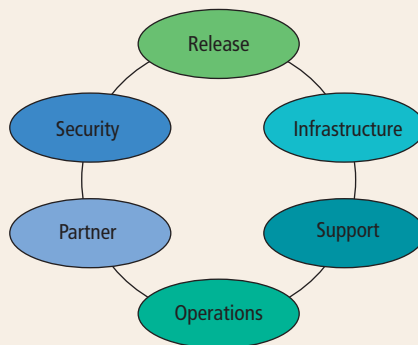
Implementaties

Microsoft stelt dat een implementatie van MOF idealiter gezien plaatsvindt bij een organisatie die overgaat naar Windows 2000 en zijn opvolgers. Ook organisaties die hun ontwikkelstraten gaan baseren op bijvoorbeeld .NET-technologie zijn gebaat bij MOF. In de Nederlandse markt zijn nog weinig gevallen bekend van implementaties van MOF. Wel is een aantal organisaties, waaronder een financiële instelling en een van de wereldwijd opererende accountancy- en IT-adviesorganisaties, ermee bezig. Maar hun initiatieven zijn nog te pril om er zinnige bevindingen over te kunnen optekenen. Wel hebben deze bedrijven een bewuste keuze voor MOF gemaakt, vaak in samenhang met andere producten van Microsoft. Hoewel het MOF is ontwikkeld voor Microsoft-producten, is het zeker niet onmogelijk de concepten toe te passen op andere typen systemen. Sterker nog, dat kan heel goed. Het team- en het risicomodel zijn zonder meer inzetbaar. Het procesmodel behoeft wat meer aanpassing, maar in de MOF-theorie is – als op een natuurlijk punt – een scheidslijn aangebracht tussen processen en (technische) procedures. Dit vergemakkelijkt de aanpassing.

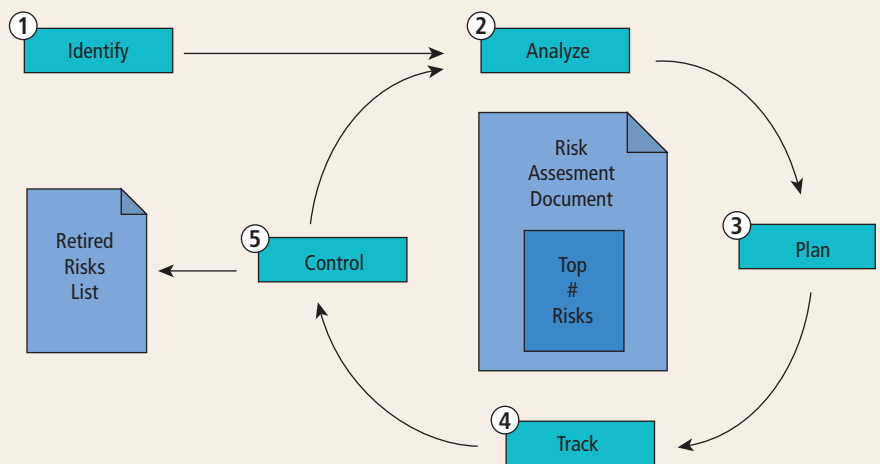
De markt en het framework

Het ligt niet in de strategie van Microsoft besloten zelf grootschalig diensten rondom MOF te gaan verkopen. Er bestaat wel een aantal diensten, zoals het Operations Assessment en de diverse MOF-trainingen. Deze zijn nog maar spaarzaam ingezet in de markt en slechts weinig partners van Microsoft zijn al in staat deze complexe en krachtige producten te hanteren. PinkRocade heeft in het verleden wel een groot aantal eigen medewerkers de MOF Essentials-training laten doorlopen, maar de echte marktdoorbraak moet nog komen. Wellicht gaat dit najaar een erkend onafhankelijk examineringsinstituut de MOF-examens afnemen en certificaten uitreiken, waardoor de waarde van deze opleiding wordt erkend en beloond. In het najaar is ook Cap Gemini Ernst & Young gereed voor het verzorgen van de MOF Essentials-training door eigen medewerkers. Zo ontstaat keuze in de markt en wellicht ook gezonde concurrentie. De grote vraag naar de opleiding zal goed op gang komen, zodra Microsoft besluit het MOF-certificaat te erkennen als onderdeel van het MCSA- en MCSE-traject. Verder blijft het wachten op de grote adoptie van Windows 2000 en Windows 2003.

Die is tot nu toe uitgebleven. Marktanalisten verwachten nu dat de massale 'uitrol' eind 2003 zal beginnen. De tijd zal het leren.



figuur 2 MOF-teammodel



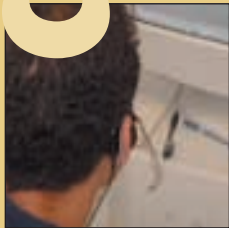
figuur 3 MOF-risicomodel

Tot slot

Bij zijn introductie in de markt is de weg van Microsofts beheerframework niet over rozen gegaan. Nu echter het product volwassen is en meer marktpartijen zich warmlopen, lijkt het erop dat het MOF zich een plek in de markt van *best practices* verworven heeft. De komende zes tot achttien maanden zullen uitwijzen wie er gelijk gaat krijgen: de strikte ITIL-volgers of de pragmatici, die kiezen voor beheerconcepten die passen bij de producten die beheerd moeten worden.

Rudolf J. Liefers MIM is bestuurslid van NGI-Beheer en senior consultant bij Cap Gemini Ernst & Young. Hij is bereikbaar via rudolf.liefers@cgey.nl

Tooling Event
pagina 36



Goedlopende helpdesk houdt scholen betrokken

Procesverbetering op de Fontys Helpdesk

Tegenwoordig worden we overspoeld met theorieën over verbeteringen op helpdesks, ja zelfs certificering komt hier om de hoek kijken. Maar hoe verlopen verbeteringen nu in de praktijk? Bijdragen aan een kosteneffectief beheer is al heel wat, maar daadwerkelijke ondersteuning van het primaire bedrijfsproces gaat nog weer een flinke stap verder. In deze praktijksituatie zien we de opkomst en ontwikkeling van een helpdesk in een situatie van outsourcing. De activiteiten worden op een rij gezet, inclusief de bereikte verbeteringen én de knelpunten die moesten worden opgelost.

De Fontys Hogescholen hadden begin 2001 drie duidelijke uitgangspunten om de aparte centrale helpdesk voor medewerkers (zie kader) te outsourcen: kennisborging, kwaliteitsverbetering en controle over de kosten. Een hele uitdaging dus. Nadat besloten was om dit samen met Simac te gaan invullen, is een traject opgezet met korte-, middellange- en langetermijndoelstellingen.

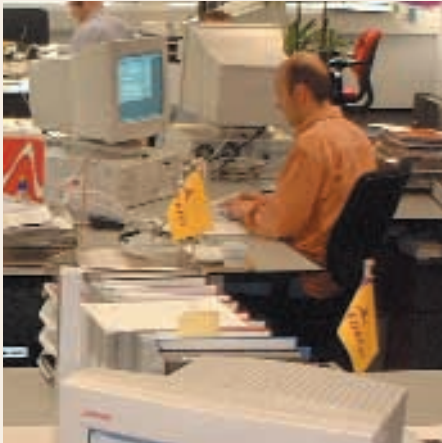
Nieuwe pc, nieuwe helpdesk

Op korte termijn heeft Fontys hard gewerkt aan het standaardiseren van haar ICT-infrastructuur. De organisatie heeft een volledige migratie, onder de noemer 'ICT-2000', achter de rug. Verder zijn applicaties nu centraal beschikbaar via het netwerk op basis van Novell Application Lounge. Ook kregen de interne beheerprocessen bij Fontys ICT Services vaste vorm, op basis van ITIL, met als doel om onder meer de opvolging van tweedelijns calls te waarborgen. Simac liet de start van de outsourcing samenvallen met het moment dat de medewerkers een upgrade kregen opgeleverd van hun werkplek in het kader van Fontys' ICT-2000-programma. Een nieuwe pc en een nieuw helpdesktelefoonnummer vormen

immers een logisch geheel en daardoor een gemakkelijk te accepteren verandering. Om kennis op te doen van de Fontys-organisatie als geheel en Fontys ICT Services in het bijzonder, besloot Simac gedurende de eerste drie maanden te gaan werken vanuit een van de lokale hogescholen. Daarna is de helpdesk vrijwel geruisloos verhuisd naar Simacs thuisbasis. Daar werd deze geïntegreerd als speciality desk op de algemene servicedesk van Simac. Nog steeds gebruiken de eindgebruikers een intern Fontys-telefoonnummer, en hoewel altijd wordt opgenomen met "Goedendag, Fontys-helpdesk..." weten de meeste bellers inmiddels wel dat ze bij Simac zijn uitgekomen.

'Eerste fase' verbeteringen

Omdat de afrekening van de dienstverlening op een prijs per call is gebaseerd, was het voor de helpdesk financieel aantrekkelijk steeds meer calls naar zich toe te trekken. Simac deed dit door helpdeskpersoneel bij te schakelen in piektijden en rekening te houden met Fontys' change- en businesskalender. De gemiddelde telefonische wachttijd werd teruggebracht van drie minuten naar een halve minuut. Hierdoor



**Aan hard werken om een server
weer in de lucht te krijgen gaat nu
communicatie over de verwachte
duur vooraf**

Fontys Hogescholen en de centrale helpdesk

De Fontys Hogescholen hebben circa 35.000 studenten en 3500 medewerkers, verspreid over 37 hogescholen in Nederland. Voor de studenten is er een centraal callcenter (zie ook kader *Desk-typologieën*) en zijn er lokale studentenbalies die allerlei ICT-gerelateerde services aanbieden. De 3500 medewerkers hebben twee eigen 'ingangen' tot de ICT-dienstverlening. Een centrale servicedesk fungeert als een soort business desk voor allerhande vragen op het niveau van applicatie-beheer en business-toepassingen. Voor het technisch beheer is er een aparte centrale helpdesk.

werd de drempel om de desk te bellen aanzienlijk verlaagd en kwamen er meer calls binnen. Het geldelijk gewin is echter gebaseerd op kortetermijndenken en slechts voordelig voor een van de partijen in de samenwerking. Daarom is er vanuit de principes van service management gestuurd op zaken die tot beider voordeel zouden leiden.

Kennisdiffusie

Beide partijen mogen garen spinnen bij het partnerschap. Op middellange termijn viel dit te realiseren door het oplossend vermogen van de helpdesk op te voeren (zie figuur 1). Dit is uiteraard gunstiger voor de eindgebruikers (snellere oplostijden), maar ook voor de klant. Om Simac te stimuleren pro-actief mee te werken aan deze doelstelling is een prikkel ingebouwd in de vorm van een verrekeningsmodel, dat is opgenomen in de SLA. Basis van dit model is dat zelf opgeloste calls meer geld in het laatje brengen dan calls die *dispatched* zijn naar de tweede lijn. Maar een financiële prikkel alleen is niet voldoende. Om de zaak ook inhoudelijk op orde te krijgen, werd het principe van de lerende organisatie van kracht, waarbij kennisdiffusie centraal staat. Veel communicatie dus, zowel tussen helpdeskmedewerkers onderling als tussen de helpdesk en Fontys ICT Services. Ook nu nog wordt elke maand de categorie waarin de meeste calls zijn geïdentificeerd, uitgeroepen tot "categorie van de maand". Hiermee stelt de helpdesk zich transparant op naar alle betrokken partijen, wat bevorderend werkt voor een voortdurende samenwerking. En het is uiteraard goed voor de ontwikkeling van kennis over de betreffende materie. Er werden *known incidents* gecreëerd en de oplossingen werden transparant opgeslagen, zodat collega's van deze ervaringen gebruik konden maken. Een tweede methode om het oplossend vermogen te vergroten is gebruik te maken van een remote overnametool. Hoewel dit pas na drie maanden volledig operationeel is geworden, gaf het werken hiermee eindgebruikers direct het gevoel dat actief aan een oplossing werd gewerkt. Voor Simac was het overigens 'slechts' bedoeld als middel voor een juiste eerste analyse en classificatie.

Afrekeningen

De eerste fase verbeteringen volgt ook direct uit de afrekening op basis van prijs per call. Fontys kreeg namelijk de gevolgen van niet goed voorbereide changes op een

presenteerblaadje aangereikt in de vorm van de maandfactuur. Hiermee werden incidenten ten gevolge van changes niet alleen op operationeel niveau, maar ook op tactisch niveau teruggekoppeld. Daardoor ontstond bij Fontys meer draagvlak om te werken aan de kwaliteit van haar change-proces.

Het mooiste resultaat na deze fase zijn de tevreden eindgebruikers. Zij genieten de voordelen van een optimaal bereikbare helpdesk met korte wachttijden en goede, snelle oplossingen. Toch bracht dit voor de Fontys-organisatie juist ook een nadeel met zich mee: steeds meer eindgebruikers wisten de weg naar de helpdesk te vinden. Daardoor werden er steeds meer calls aangemaakt en stegen de kosten dus ook sterk. Hoewel dat gunstig uitpakte voor Simac, is dit juist de trigger geweest om te beginnen met de ontwikkeling en implementatie van zaken die de langetermijn-doelstellingen moesten ondersteunen. Deze doelen zijn fundamentele kwaliteitsverbetering en het onder controle krijgen van de kosten.

Langetermijnverbeteringen

In dit verhaal zijn we inmiddels aangeland in 2002: de samenwerking is goed op gang gekomen en de helpdesk is uitgegroeid tot de voordeur, de ogen en oren van de gehele service-organisatie. Een ideale situatie om een begin te maken met het invullen van de langetermijn-doelstellingen. Om deze te bereiken zijn twee speerpuntprogramma's opgezet:

- extern gericht: inzoomen op de feitelijke ondersteuning van het businessproces van de klant;
- intern gericht: verhogen van de arbeidsvreugde van de helpdeskmedewerkers.

Ondersteuning businessproces

Om waarde toe te voegen aan het primaire businessproces moet inzichtelijk worden waar de knelpunten liggen én moeten deze worden aangepakt. Dit is gerealiseerd door het sluiten van de kwaliteitscirkel (Deming) die ten grondslag ligt aan het ITIL-model; meten, analyseren, terugkoppelen en oplossingen ter verbetering implementeren. Er waren inmiddels voldoende meetgegevens voorhanden, en dagelijks worden afwijkende situaties in een openbaar logboek bijgehouden. Op basis van deze bronnen is gestart met intensieve callanalyse. In feite is hier sprake van pro-actief problem management. Uiteraard kostte dat extra tijd van helpdeskmedewerkers en service

manager, maar het gaf wel resultaat. Dankzij voldoende wederzijds vertrouwen was deze moeite niet voor niets. De service manager maakte van de repeterende calls telkens een business case en toonde tijdens regulier overleg aan dat door het oplossen van de kernproblemen deze repeterende incidenten zouden verdwijnen. Fontys kon de zo ontstane 'ruimte' goed gebruiken, mede door de grote changes die de organisatie voor de boeg had. Onder meer stond de uitrol van Exchange-2000 op stapel, die tot extra calls zou gaan leiden (zie figuur 2).

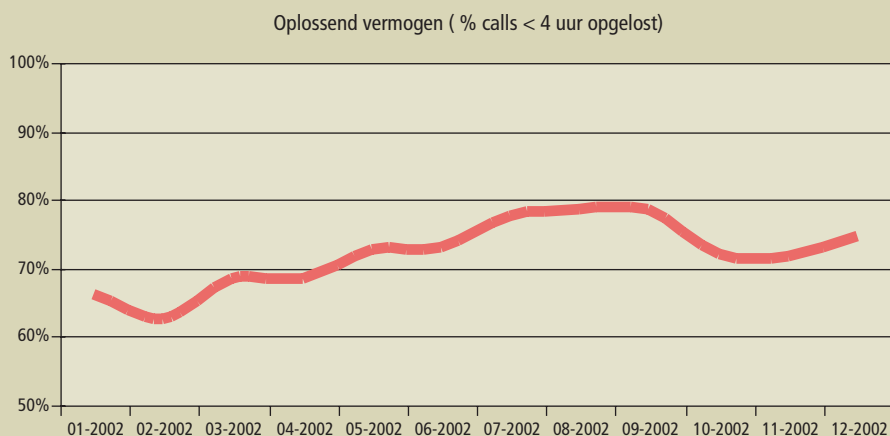
Eerlijkheidshalve zij wel vermeld dat het in de praktijk echt niet altijd eenvoudig was. Mensen van beide organisaties moesten immers van hun dagelijkse werkzaamheden worden losgemaakt om tijd te besteden aan structurele kwaliteitsverbetering. Dit instrument is dan ook zeker nog niet op alle mogelijke plaatsen effectief aangevend. Maar ook dat heeft zijn goede kanten. Er is nog lang zicht op verbeteringen.

Arbeidsvreugde omhoog

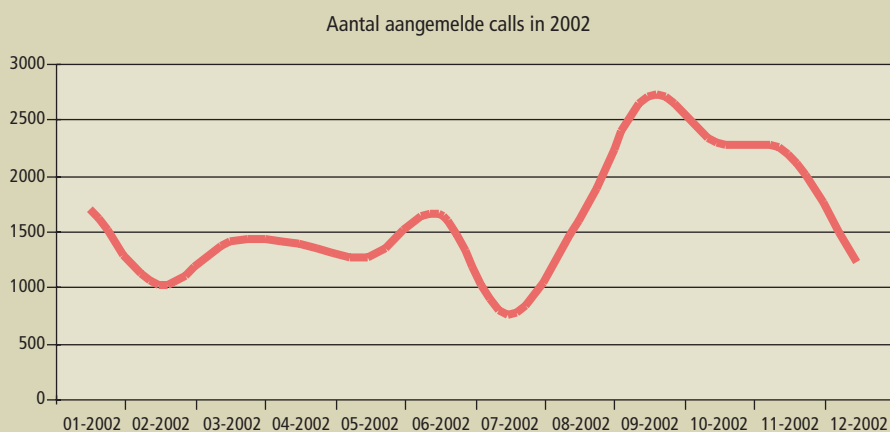
Het tweede speerpuntprogramma, het verhogen van de arbeidsvreugde van de helpdeskmedewerkers, is intern gericht. Het vergt inzicht in de individuele ontwikkelingsbehoefte van de medewerkers. Kun je daaraan voldoen, dan creëer je beter functionerende medewerkers, wat de dienstverlening in zijn geheel ten goede komt.

Om dit te realiseren is gewerkt aan competentie-ontwikkeling van de helpdeskmedewerkers, gericht op hard en soft skills. Zij die in de loop van de jaren de meeste Fontys-kennis hebben opgebouwd, vormen een kerngroep. De kerngroep staat vooraan in de *queue* en de overige medewerkers staan stand-by om bijgeschakeld te worden tijdens pieken. De kerngroep heeft hierdoor de meeste klantcontacten en krijgt eer van haar werk, omdat zij beter en sneller mensen kan helpen dan de backupmedewerkers. Dit werkt beter voor de bellers. Maar natuurlijk ook voor de kerngroepmedewerkers; juist zij ontvangen de complimenten voor de geboden oplossingen. Meer technisch gerichte medewerkers kregen meer tijd voor intensieve callanalyse én voor het uitwerken van oplossingsvoorstellen. Voor deze groep mensen was dit aspect van het werk juist plezierig. Niet steeds maar weer met klanten aan de lijn, maar ook eens structureel bezig zijn. Dan is er nog de supervisor van de groep. Hij zag zijn arbeidsvreugde verhoogd door meer inzicht in het bedrijfsmatige aspect

Callverloop en oplossend vermogen van de helpdesk

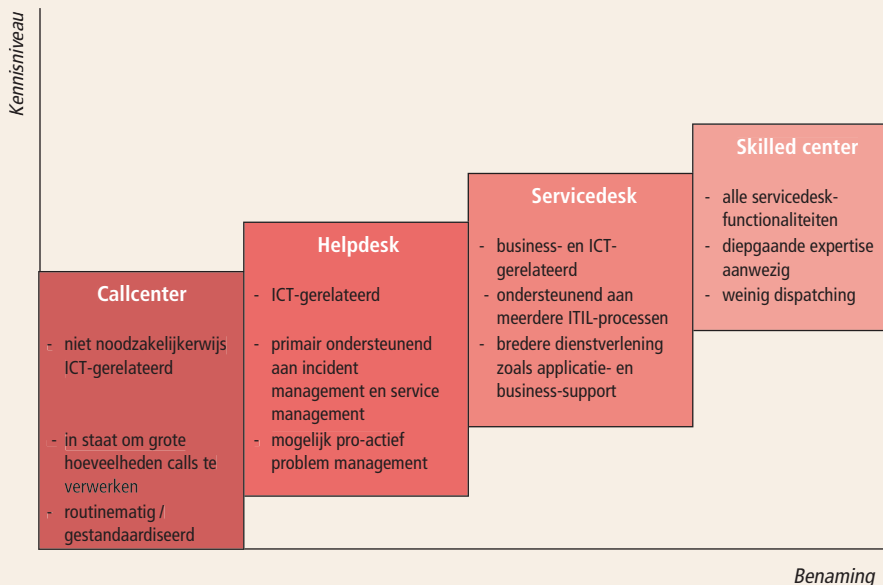


figuur 1 Het stabiel toenemend oplossend vermogen van de helpdesk gedurende de eerste negen maanden is duidelijk zichtbaar, ondanks het grillige verloop van het aantal aangemelde calls



figuur 2 Op een zomerdip (juni/juli) volgt een piek in het aantal aangemelde calls bij de start van het studiejaar. De stijging in augustus/september komt door de uitrol van Exchange-2000

van de dienstverlening. Hij kreeg steeds meer service management-taken toebedeeld. Daarmee kreeg hij inzicht in het berekeningsmodel, mocht hij relevante gegevens aandragen voor facturatie en werd hij intensiever betrokken bij de totstandkoming van de periodieke rapportages en rapportagebesprekingen. Deze upgradering van zijn verantwoordelijkheid was precies de uitdaging die hij zocht. Per groep medewerkers is ten slotte gekeken naar de benodigde en veranderbare competenties die het meest aansloten bij hun persoon op gedragsmatig en cognitief niveau (zie kader *Competentie-ontwikkelingsgebieden*). Elke medewerker kreeg het aanbod deze competenties te verwezenlijken door middel van een persoonlijk ontwikkelingsplan.



figuur 3 Desktypologieën. Deze figuur suggereert een logische ontwikkeling in typologie, maar die is er niet. Het is geen wetmatigheid om door te stromen naar een volgende typologie. Echte kwaliteitsverbetering is alleen te bereiken als men zich verdiept in de rol die de desk heeft in de organisatie als geheel.

Langetermijngevolgen

Elke helpdeskmanager weet hoe moeilijk het is om aan goed personeel te komen én deze mensen vast te houden. Mede door actief competence management is bereikt dat Simac-medewerkers graag en met ple-

zier op de speciality desk van Fontys werken. “Daar zijn immers persoonlijke én bedrijfsmatige uitdagingen in te vullen”, verklaart de supervisor van de groep. Verder signaleert hij een vreemd gevolg van al de kwaliteitsverbeteringen (zie ook de samenvatting in tabel 1). Men had gerekend op een snelle ontwikkeling en dito resultaten. Maar een vertragend element was niet voorzien: de moeilijkheidsgraad van de aangeboden calls steeg, omdat de eindgebruikers het vertrouwen hadden dat hun problemen daadwerkelijk zouden worden opgelost. Laat dit nu juist weer de interesse zijn van de groep ‘structureel-verbeters’, die hiermee z’n behoefte aan afwisselend werk zag toenemen.

Zorgenkind af

Ook de ICT-coördinator van Fontys noemt in een recent interview twee noemenswaardige effecten van de outsourcing. Ten eerste spreekt hij over de metamorfose die de helpdesk heeft ondergaan: van zorgenkind naar katalysator in professionalisering van de rest van Fontys’ ICT-service-organisatie.

Met name de maandelijkse rapportage bleek hierbij leidend. De effecten van het totale IT-beleid zijn namelijk terug te vin-

Instrumentarium	Primaire reactie	Bereikte doelen na twee jaar
Verrekening per call	IT provider streeft naar meer calls (stijgende omzet) Klant krijgt incidenten a.g.v. gebrekkig changeproces ook financieel teruggekoppeld	Klant én IT-provider streven naar minder calls (tevreden lange-termijnklantrelatie) Extra draagvlak voor continu problem management
SPOC	Er wordt meer gebeld vanwege snelle en goede hulp (tevreden eindgebruikers en stijgende omzet)	Minder calls (tevreden eindgebruikers én tevreden klant)
Goede serviceprocessen	Zware eenmalige projecten	Basis voor steeds efficiëntere beheerorganisatie
Bemensing	Capaciteit	Competentiegericht verbeteren
Remote access-tools	Big brother is watching you Directe hulp bij incidenten	Wederzijds vertrouwen Kwaliteitsverhogend
Pro-actieve procesdoelen	Vergt extra tijd en aandacht Uitdaging voor helpdeskmedewerkers	Stabieler infrastructuur en controle over de kosten Moeilijkere calls worden aangemeld
Outsourcing	Bestaande kwaliteit met gelijke kosten Professionalisering van de helpdesk	Hogere kwaliteit met controle over de kosten Professionalisering van de gehele ICT-organisatie én brug voor business-IT-alignment

tabel 1 Samenvatting van ervaringen

den in de workload op de helpdesk en dat vormt, tezamen met goede inhoudelijke analyses, waardevolle feedback op het eigen functioneren. Vóór de periode van outsourcing had men dit nog onvoldoende. Medewerkers zijn de kracht van deze gegevens gaan inzien en gebruiken ze om fluctuaties te verantwoorden. Ook wordt deze informatie steeds vaker gebruikt om investeringsvoorstellen voor structurele verbeteringen te onderbouwen. Let wel: de inzet van de ICT-medewerkers is primair niet veranderd. Voor de focus geldt dat des te meer. Deze is verschoven van techniek naar dienstverlening. Aan hard werken om een server weer zo snel mogelijk in de lucht te krijgen, gaat nu communicatie met de eindgebruikers vooraf. Zij krijgen te horen wat de vermoedelijke duur is van de storing en welke alternatieven er eventueel zijn om te kunnen doorwerken. Het effect hiervan is veel meer waard dan de feitelijke snelheid waarmee een server terug in de lucht is.

Mondige helpdesk

De ICT-coördinator van Fontys spreekt over de brug die inmiddels is geslagen tussen business en IT. Vroeger kwam in discussies met de 37 hogescholen altijd de slechte performance van de helpdesk ter sprake. Nu die sterk is verbeterd, is er ruimte voor discussie over IT-ondersteuning van hun primaire business. Voor het eerst sinds jaren vragen de schoolleidingen tegenwoordig naar cijfers uit de categorie ondersteuningsvragen. Zij zien nu in dat ze hiermee

Competenties	Stabiel	Veranderbaar
Cognitief	Analytisch vermogen	Vakkennis informatica
	Oordeelsvorming	Kennis van andere disciplines
	Abstractievermogen	Commercieel inzicht
	Creativiteit	Strategische visie
Gedragmatig	Sensitiviteit	Organisatie-, omgevings- en branchekennis
	Flexibiliteit	Leiderschap
	Integriteit	Communicatieve vaardigheden
	Stressbestendigheid	Samenwerken in teamverband
	Zelfstandigheid	Luisteren
	Doorzettingsvermogen	Conflicthantering
		Klantgerichtheid
		Initiatief
		Accuratesse
		Methodisch werken
	Plannen en organiseren	

tabel 2 Competentie-ontwikkelingsgebieden (bron: J.C. op de Coul, *Taken, Functies, Rollen en Competenties in de Informatica*)

zelf een instrument in handen hebben om aan callreductie te werken, en dus om de doelmatigheid van hun medewerkers te vergroten.

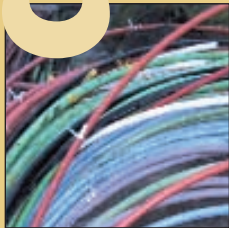
Bij de helpdesk zitten de ogen en oren van de gehele ICT-service-organisatie. De helpdesk heeft nu ook een mond gekregen, en die spreekt klare taal, die het waard is om naar te luisteren.

Jurian Burgers is werkzaam als consultant en servicemanager bij Simac ICT en bereikbaar via jurian.burgers@simac.nl.

Literatuur

- Help Desk Institute *white paper*, november 2002
 OGC, *ITIL Best practice for Service Support*
 J.C. op de Coul, *Taken, Functies, Rollen en Competenties in de Informatica*, ten Hagen & Stam Uitgevers, 2001, isbn 90-440-0343-7

ITB
pagina 42



Beschrijving van aanpak voor onvermijdelijke overgang

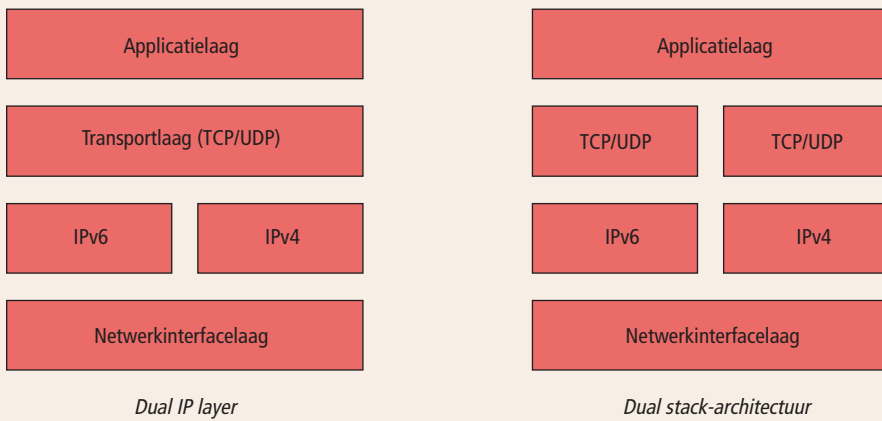
Migreren naar IPv6

Het zal niet vandaag of morgen gebeuren, maar IPv6 komt eraan. En als het zover is, hoe verloopt dan de daadwerkelijke migratie van uw lokale netwerk? Waar kunt u – nu al – over nadenken en welke stappen moet u straks zetten? Kortom, als vervolg op het artikel “Bent u al klaar voor IPv6?” in nummer 4 – over de voornaamste veranderingen en de voordelen van TCP/IPv6 boven v4 – nu aandacht voor de vraag: hoe gaan we dat aanpakken?

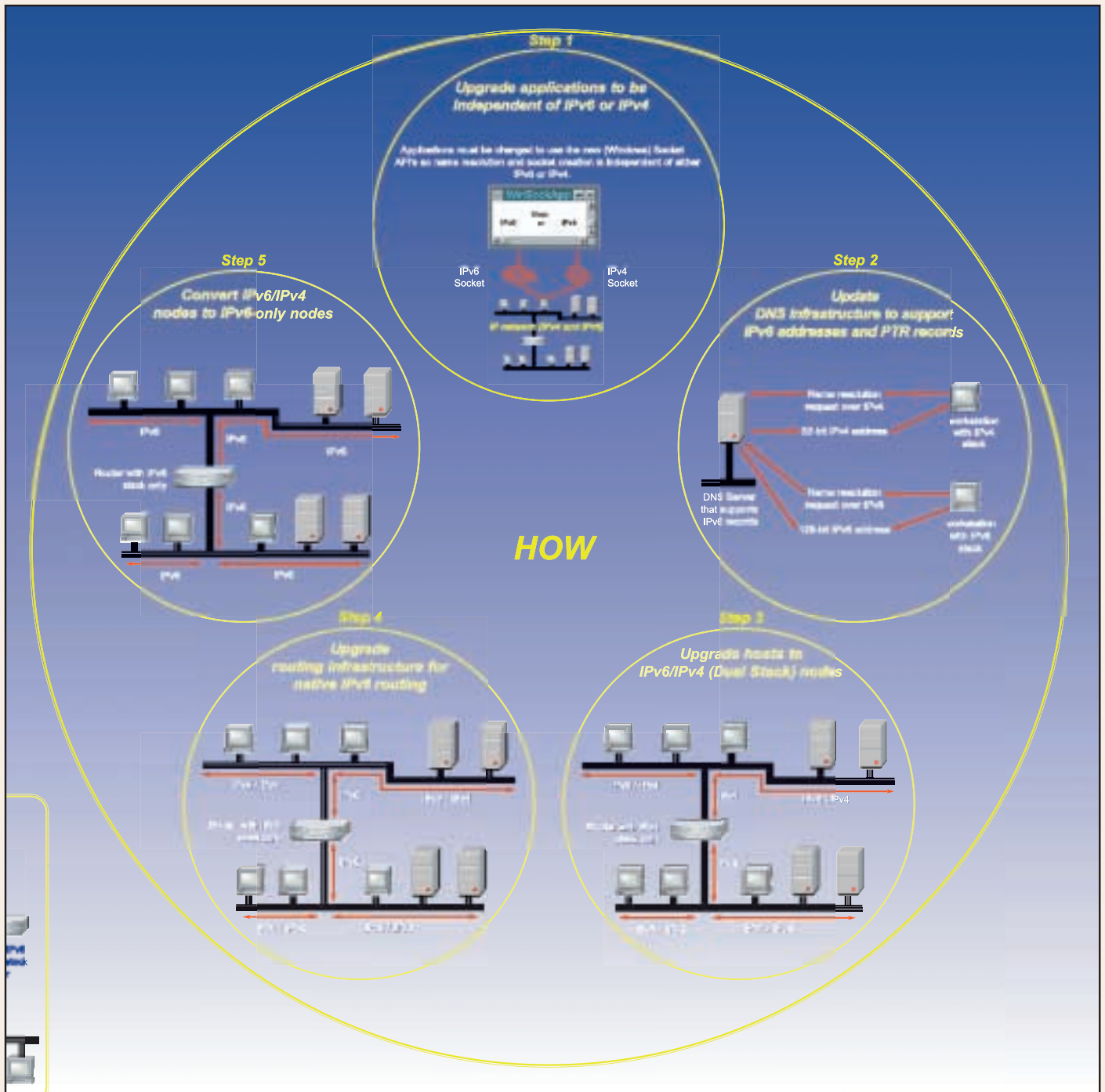
Vooropgesteld: dag X zal niet aanbreken. Bij de ontwikkeling van het nieuwe protocol is rekening gehouden met een geleidelijke overgang. De migratie van het huidige internet volgens IPv4 naar een op IPv6-leest geschoeid internet vindt niet van de ene op de andere dag plaats. Het is natuurlijk onmogelijk om internet op dag X met alleen IPv6-hosts en -routers (nodes) te laten werken. Een aantal ‘ingebakken’ mechanismen¹ zal ervoor zorgen dat IPv6-nodes probleemloos kunnen communiceren met de bestaande IPv4-nodes. Niet alleen zal de migratie gefaseerd verlopen, internet zal zelfs nog lange tijd bestaan uit zowel IPv6- als IPv4-nodes, misschien wel voor altijd.

LAN-migratie

In de vaste wetenschap dat er voldoende ondersteuning is en blijft voor oude IPv4-nodes, kunnen we nu gaan kijken hoe we een lokaal IPv4-netwerk gaan upgraden naar IPv6. Internet gaat in fasen over op IPv6, zo ook uw LAN. Deze gefaseerde aanpak is bovendien nodig om de beschikbaarheid van uw netwerk te waarborgen.



figuur 1 Twee mogelijke oplossingen van dual stacks



figuur 2 Fragment van een door Vanveen uitgebrachte poster, waarop overzichtelijk alle (technische) consequenties van de migratie in beeld zijn gebracht. De poster, in het formaat A1, is voor abonnees van IT Beheer Magazine gratis op te vragen bij de auteur door het verstrekken van uw postadresgegevens of via de website van Vanveen informatica (www.vanveen.nl).

Migratie van een IPv4-netwerk naar IPv6 verloopt in een aantal stappen:

- aanpassing van applicaties die de *sockets-API's* gebruiken;
- updating van DNS-infrastructuur;
- upgradung van hosts naar dual stack-nodes;
- upgradung van interne IPv4-routers naar IPv6-nodes;
- conversie van dual stack-hosts naar IPv6-hosts.

Applicaties die via TCP/IP communiceren, gebruiken vaak de *sockets application program interface* (API). De nieuwste versies van deze sockets-API kunnen nu ook IPv6 'praten'. Eerder geschreven applicaties, die dus zijn gebaseerd op de oude sockets-API, zullen echter gecontroleerd moeten worden op gebruik van IPv4-achtige zaken. Zo zijn IPv4-adressen hard in de code opgenomen (bijvoorbeeld een *loopback*-adres) of is een vaste veldgrootte gereserveerd voor een IPv4-adres waar een IPv6-adres met geen mogelijkheid in past. De veranderingen aan de sockets-API staan beschreven in RFC3493 – *Basic Socket Interface Extensions for IPv6*.³

DNS onder handen nemen

Vervolgens moet de DNS-infrastructuur (*domain name system*) onder handen genomen worden. Het huidige DNS 'snapt' alleen IPv4-adressen en moet natuurlijk ook IPv6-adressen aankunnen. Er zijn op dit moment twee RFC's voorhanden, RFC1886 en RFC2874, die op een verschillende manier IPv6-adresondersteuning bieden voor DNS. In het eerste voorstel wordt het AAAA-record-systeem beschreven, dat qua werking overeenkomt met het reeds bekende A-record-systeem⁴. Toen later bleek dat toch meer functionaliteit in DNS gewenst is, is het A6-record-systeem ontwikkeld.

Tot nog toe heeft de *Internet Engineering Task Force* (IETF) nog niet besloten welke aanpak het beste is. Beide RFC's zijn inmiddels wel geïmplementeerd; daarbij is RFC1886 meer verspreid, omdat die RFC eerder tot stand is gekomen en makkelijker te implementeren is. De voor- en nadelen van beide methoden staan beschreven in RFC3364.

Zodra het DNS IPv6-compatibel is, kan begonnen worden met het upgraden van alle hosts binnen een netwerk tot dual stack-nodes. Dit zijn hosts die zowel IPv6 als IPv4 kunnen communiceren. De dual stacks

Transitiemechanismen

Laten we de transitiemechanismen nog eens opsommen, met een korte beschrijving.

- *Dual stack* (ook bekend als *Dual IP Layer*). Hiermee kunnen hosts en routers zowel IPv4 als IPv6 communiceren.
- *IPv4-compatibele IPv6-adressen*. Een IPv4-adres in een IPv6-notatie.
- *IPv6-over-IPv4 tunneling*. Techniek waarbij IPv6-pakketjes in IPv4-pakketjes worden verpakt, opdat deze via een IPv4-netwerk kunnen worden verstuurd.

Het tunneling-principe valt uiteen in drie categorieën:

- *configured tunneling*. Dit is vergelijkbaar met het opgeven van een *default router*, zoals bij IPv4. Dit wordt gebruikt bij dual stack-hosts die aangesloten zijn op een IPv4-netwerk zonder IPv6-nodes in de buurt. Via de geconfigureerde tunnel kunnen deze hosts toch communiceren met IPv6-netwerken;
 - *automatic tunneling of IPv6 over IPv4*. Hierbij hoeft geen tunneleindpunt geconfigureerd te worden. Het tunneleindpuntadres wordt bepaald door het IPv4-compatibele IPv6-adres van het eindpunt. Het IPv4-adres mag echter geen adres zijn uit de *private range*;
 - *IPv4 multicast tunneling*. Hierbij wordt gebruikt gemaakt van *Neighbor Discovery*², waardoor het niet nodig is een eindadres te configureren; ook hoeft het geen IPv4-compatibel adres te zijn. Wel moet het IPv4-netwerk geconfigureerd zijn om multicast-verkeer aan te kunnen.
- *NAT (network address translation)*. In IPv4-netwerken wordt dit mechanisme gebruikt om de vertaling te verzorgen van lokale in globale IP-adressen en omgekeerd. In IPv6 verzorgt NAT echter de vertaling tussen IPv4- en IPv6-adressen. Dit vertaalmechanisme heeft wel wat nadelen. Zo worden niet alle mogelijkheden van IPv6 door dit mechanisme ondersteund. Maar als toegang tot IPv4-netwerken en -applicaties nodig is, kan dit een (tijdelijke) oplossing bieden.

Er is een aantal NAT-technieken ontwikkeld onder IPv6:

- *NAT-PT (network address translation – protocol translation)* – verzorgt vertaling van IP-adressen en protocollen;
- *NAPT-PT (network address port translation – protocol translation)* – verzorgt vertaling van zowel IP-adressen en protocollen als poortnummers. Hierdoor ontstaat de mogelijkheid meerdere IPv6-hosts te bedienen met één enkel IPv4-adres.

kunnen op twee manieren tot stand komen; zie figuur 1 voor een schematische weergave.

De dual stack-architectuur wordt door Microsoft in Windows XP en Windows 2003 toegepast.

Zodra alle interne routers alleen nog IPv6 communiceren en de dual stack-hosts zijn geconverteerd naar IPv6-hosts, werkt uw lokale netwerk volledig op IPv6. De routers die de communicatie naar buiten verzorgen, dienen nog wel voorzien te zijn van een dubbele stack. Deze kunnen met eerder beschreven tunneling-technieken IPv6-verkeer van het lokale netwerk transporteren naar andere IPv6-netwerken via bestaande IPv4-netwerken (internet).

Internetaanbieders en IPv6

Om gebruik te kunnen maken van IPv6 via internet zullen ook de internetaanbieders

Zolang uw IPv4-netwerk goed functioneert, is er geen reden om te gaan migreren

Ondersteuning van leveranciers

Alle beschreven technieken helpen natuurlijk niet als uw hardware en applicaties IPv6 niet ondersteunen. Het aantal leveranciers dat hun producten geschikt maakt voor het nieuwe protocol, groeit intussen met de dag. Om alvast uit te zoeken of uw producten kunnen werken met IPv6 zijn de volgende twee websites nuttig. Hier staan handige doorlinkadressen, alsmede e-mailadressen van personen die u wellicht meer kunnen vertellen over hun producten in combinatie met IPv6:

- <http://www.ipv6.org/impl/index.html>
- <http://playground.sun.com/pub/ipng/html/ipng-implementations.html>

Vanzelfsprekend kunnen uw eigen leveranciers meer vertellen over de ondersteuning van IPv6 in hun producten.

hun netwerken geschikt moeten maken voor IPv6-verkeer. Inmiddels biedt een aantal grote internetaanbieders in Nederland, onder wie Surfnets en XS4all, toegang tot andere IPv6-netwerken. Hierbij wordt gebruikgemaakt van het eerder beschreven principe van *IPv6-over-IPv4 tunneling*.

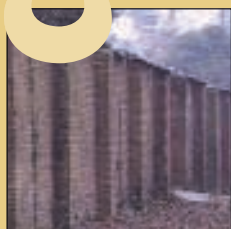
Stap over bij een verandering

Hoogstwaarschijnlijk zal het nog een tijd duren voordat u een beslissing neemt voor de daadwerkelijke aanvang van de migratie van uw netwerk naar IPv6. Zolang uw IPv4-netwerk goed functioneert, is er geen reden om te gaan migreren. Maar zodra u om een of andere reden tegen de limieten of tekortkomingen van IPv4 aanloopt, overweeg dan implementatie van IPv6. Die situatie kan zich bijvoorbeeld voordoen bij een tekort aan publieke adressen, als u NAT en lokale IP-adressen gebruikt en u wilt beveiligde end-to-end-verbindingen opzetten of als uw netwerk verder uitgebreid moet worden met een geheel nieuw segment. Staat u op het punt grote investeringen te doen in nieuwe complexe netwerkconfiguraties, kies dan voor de toekomst en investeer in IPv6.

Noten

1. Zie RFC2893 – *Transition Mechanisms for IPv6 Hosts and Routers*.
2. *Neighbor Discovery* is een complex protocol dat wordt gebruikt om adressen te vinden van hosts en routers op hetzelfde netwerk. Zowel hosts als routers gebruiken dit protocol.
3. Tip: Microsoft heeft voor de Windows Sockets API-applicaties een tool ontwikkeld dat potentiële IPv6-fouten kan opsporen: `checkv4.exe`.
4. In het thans gebruikte DNS worden domeinnamen alleen gekoppeld aan IPv4-adressen. Deze koppelingen worden opgeslagen als zogenaamde A-records. Als een netwerksysteem een IP-adres van een bepaalde domeinnaam wil weten (bijvoorbeeld een computer wil een netwerkverbinding opzetten met een server), zal dit systeem het adres aan een DNS vragen. Het DNS zal het bijbehorende IPv4-adres opzoeken in zijn tabellen met A-records en vervolgens het antwoord terugsturen naar de aanvrager.

Marco van der Kraan is Sr. consultant bij Vanveen informatica. Hij is bereikbaar via vdkraan@vanveen.nl.



Beheer op basis van rollen noodzakelijk

Integreren van nieuwe applicaties in veilige omgeving

Informatiebeveiliging is veel meer dan alleen wat softwarepakketten installeren waarmee intrusion detection of anti-virusvoorzieningen worden geregeld. Wie in een goede technische beveiliging wil voorzien, dient de gehele technische infrastructuur te onderzoeken op zwakke plekken en risico's. Bovendien zullen procedures ontwikkeld moeten worden die het mogelijk maken om nieuwe systemen en applicaties op een gecontroleerde manier in deze veilige omgeving te installeren. De auteurs beschrijven een methodiek die zij samen met Hewlett-Packard hiervoor ontwikkelden.

Een goed georganiseerde technische beveiliging is veel meer dan een defensief mechanisme. Het biedt niet alleen mogelijkheden voor e-business, maar maakt het natuurlijk ook mogelijk met geografisch gespreide vestigingen te werken, werkprocessen desnoods over meerdere kantoren te spreiden of bijvoorbeeld met 'terminal services' over een virtual private network (VPN) te werken.

Maar een infrastructuur die volzit met beveiligingsgaten is met de beste security tools niet veilig te maken.

De gehele technische infrastructuur zouden we dus willen doorlichten. Door dat op een gestructureerde manier te doen, is het mogelijk om een veilige systeemomgeving te maken. We hebben deze manier van werken uitgewerkt voor onder andere ABN Amro, voor wat betreft Unix- en NT-omgevingen, en hier gaan we er dieper op in.

Vormen van informatiebeveiliging

Het bekende gelaagde security-model is opgebouwd uit een groot aantal lagen. Wij richten ons vooral op de lagen *network security*, *operating system security*, *management layer security* en een klein gedeelte van *application security*. In dit

laatste geval gaat het vooral om die beveiligingselementen die aan de orde komen als een applicatie op het besturingssysteem wordt gehost; zie figuur 1.

Wie met deze eisen in het achterhoofd naar de gehele infrastructuur kijkt, ontkomt er niet aan te beginnen bij het begin: de eisen die de organisatie aan beveiliging stelt (zie figuur 2). Zij kent doorgaans een zakelijk belang toe aan het goed en veilig functioneren van een toepassing, en daaruit zijn de security-eisen af te leiden. Aan de hand van deze eisen moet vervolgens een analyse plaatsvinden van de beveiligingsproblemen. Dat gebeurt onafhankelijk van het te gebruiken platform.

Daarmee is in feite een vergelijking mogelijk van enerzijds het gewenste security-niveau en anderzijds het daadwerkelijk aanwezige niveau van veiligheid. En zo kan ook een plan worden uitgewerkt voor de manier waarop dit verschil tussen aanwezige en gewenste security kan worden weggevoerd. Dit behelst het opstellen van een reeks van procedures om ervoor te zorgen dat de vastgelegde *security requirements* ook daadwerkelijk zijn te realiseren. Denk aan het configureren van het door de leve-

rancier geleverde besturingssysteem, waarbij alle functionaliteit die niet nodig is wordt verwijderd of uitgeschakeld (minimale configuratie). Op dit punt aangekomen kunnen *hardening scripts* – zelf geschreven of opgehaald via internet – er

op een geautomatiseerde manier voor zorgen dat resterende gaten gedicht worden.

Niet zelden zullen meer maatregelen nodig zijn. Als de omgeving nog niet voldoet aan het door de business gewenste beveiligingsniveau, zullen een selectie en implementatie moeten plaatsvinden van op de markt beschikbare software of andere producten. Het resultaat van dit alles is dat uiteindelijk een *secure system* ('veilig systeem') ontstaat, dat geheel tegemoetkomt aan de beveiligingseisen van de organisatie.

Beheer met rollen

In figuur 3 is dit schematisch weergegeven voor een Unix-omgeving. De basis van de 'secure Unix'-omgeving bestaat in dit geval uit Sun Solaris 8.0 dan wel HP-UX 11.0. Beide besturingssystemen zijn uitgekleed. Dat wil zeggen dat alle niet relevante functionaliteit is verwijderd. Vervolgens is een reeks van hardening scripts toegepast. De eerdergenoemde functiescheiding tussen uitvoerende en controlerende partij is gerealiseerd met behulp van de eTrust Access Control-programmatuur van Computer Associates. Strong authentication wordt gerealiseerd met behulp van SecurID-tokens van RSA. Het netwerkverkeer, gerealiseerd door de zakelijke toepassingen, wordt versleuteld via SSH (secure shell). Via een login-procedure krijgen eindgebruikers toegang tot de applicaties. Flankerend hieraan wordt met enerzijds ESM (Enterprise Security Manager) van Symantec en anderzijds PentaSafe's VigilEnt de integriteit van de systeemomgeving gecontroleerd. Auditing vindt plaats via eTrust en PentaSafe.

Het is natuurlijk niet voldoende om alleen maar een dergelijke secure systeemomgeving te creëren. Deze zal ook beheerd moeten worden, bij voorkeur via een op rollen gebaseerde vorm van systems management. Daarin dient een aantal functies te worden onderkend, met de daaraan gekoppelde rechten en plichten. In figuur 4 is dit weergegeven. Zijn deze rollen eenmaal gedefinieerd, dan is het vervolgens eenvoudig om functionarissen aan een van deze rollen toe te voegen.

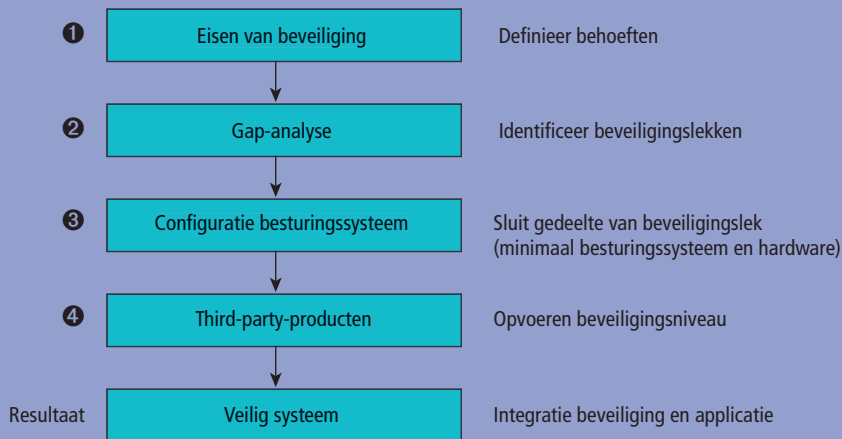
De functiescheiding leidt tot het creëren van de functie van zowel security officer als security administrator. Het zal duidelijk zijn dat deze security admin de uitvoerende partij is als het om beveiliging gaat. De

Layered Security Model

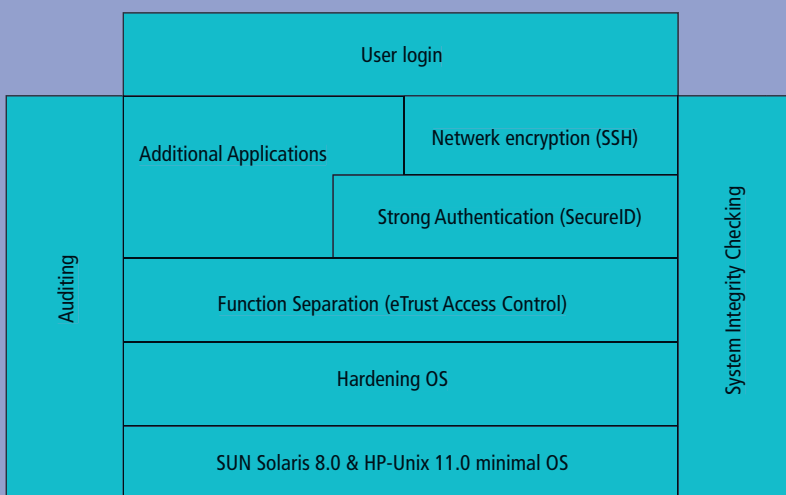
- Physical Security
- Network Security (network management traffic, SSH)
- Operating System Security
- Management Layer Security
- Application Security (from OS point of view)
- End-user Security [SSO]

figuur 1 Om tot een veilige systeemomgeving te komen, richt men zich vooral op het netwerk, het OS, de beheeromgeving en het applicatiebeheer, voorzover dit op het besturingssysteem betrekking heeft

Hoe informatiebeveiliging afdekken?



figuur 2 Van beveiligingseisen ('security requirements') tot veilig systeem ('secure system')



figuur 3 Het security-model

security officer is in principe geen ICT-functionaris, maar iemand die in de lijnorganisatie werkzaam is. Liefst zo hoog mogelijk, op directieniveau of dicht daartegenaan. Deze security officer is verantwoordelijk voor het opstellen van de richtlijnen en procedures en controleert de correcte uitvoering ervan. De security admin heeft een actieve uitvoerende rol. Het gaat hier om een medewerker met een ICT-achtergrond, maar die verder geen andere operationele taken heeft. Tot het takenpakket behoren onder andere gebruikersbeheer, gebruikersauthenticatie, het uitreiken van tokens en bijvoorbeeld het beoordelen van meldingen die door eTrust Access Control en andere beveiligingssoftware worden gegenereerd.

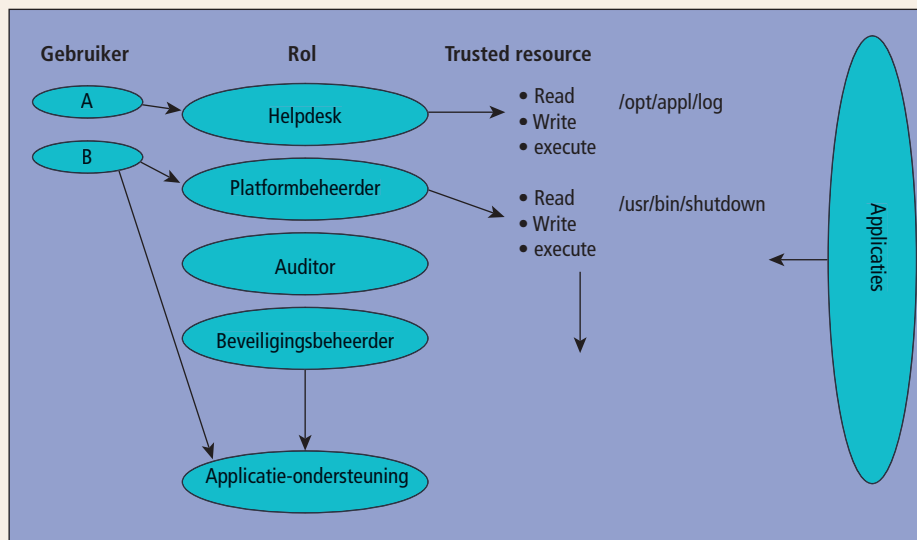
Veilig houden

De volgende stap is het op een gecontroleerde manier toevoegen van nieuwe applicaties in deze beveiligde omgeving. Daarvoor is per toepassing een security assesment nodig. Dit is uit te voeren via een stappenplan. Daarbij worden voor iedere applicatie de vereiste system resources vastgesteld en vervolgens de eventuele beveiligingsrisico's in kaart gebracht. Daarna kunnen de installatie van de applicatie en het oplossen van eventuele beveiligingsproblemen worden aangepakt.

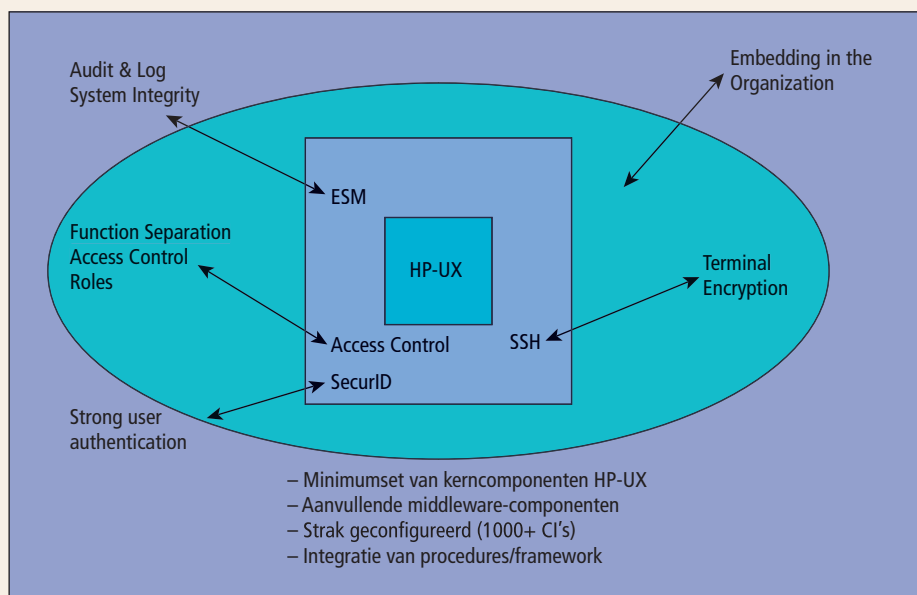
Hierbij ontstaat een interessant additioneel effect. Iedere in de systeemomgeving opgenomen component zal eerst geanalyseerd en gecertificeerd moeten worden. Dit goedkeuringsproces duurt al gauw enkele weken. Het is dan ook vaak veel handiger om reeds eerder bekeken en in orde bevonden componenten toe te passen dan per project of applicatie bijvoorbeeld een nieuwe databaseomgeving of een messaging-programma te kiezen, die vervolgens eerst weer op beveiligingsaspecten onderzocht moet worden. Zo ontstaat een zekere mate van standaardisatie.

De procedure die leidt tot integratie of hosting van een nieuwe applicatie vereist uiteraard de nodige aandacht, omdat een nieuwe toepassing niet onverhoopt nieuwe beveiligingsrisico's mag introduceren. Het eerdergenoemde stappenplan omvat de volgende acties:

- controle op de minimale eisen die aan een installatie zijn verbonden;
- invullen van een beveiligingsvragenlijst door een productspecialist;
- maken van eerste security snapshot met de ESM-software;



figuur 4 Role-based beheer – ook voor security



figuur 5 De complete 'secure Unix'-omgeving

- installatie van de applicatie en maken van een definitieve snapshot;
- analyse van beide rapportages, waarbij de aandacht met name zal uitgaan naar de geïnstalleerde bestanden, de gebruikte directory's, de betrokken users en dergelijke. Ook de file-attributen zijn aan onderzoek onderhevig;
- opnemen van vragenlijst en snapshot-rapportage in een integratiegids. Deze dient als basis voor toekomstige installatie van nieuwe applicaties of componenten.

Controle staat centraal

Centraal in deze gehele aanpak staat het woordje *gecontroleerd*. Het is van groot belang controle te behouden over een secure bevonden systeemomgeving. Een goede analyse van de eventuele beveiligingsrisico's die een nieuwe applicatie of

component kan opleveren, maakt het mogelijk deze risico's één voor één af te dekken, op te lossen of bewust te accepteren. Met als doel dat de nieuwe applicatie geen afbreuk doet aan het bestaande beveiligingsniveau. Op die manier is nieuwe software op een veilige en gecontroleerde manier in een 'secure system' te introduceren.

Hans Spaander en René Klootwijk zijn werkzaam bij Quinse en bereikbaar via hans.spaander@quinse.nl en rene.klootwijk@quinse.nl.

Auteurs, welkom aan boord

IT Beheer Magazine wil graag in contact komen met schrijvende praktijkmensen. Wij zoeken ervaringen met:

- toolimplementaties,
- meten en beheersen van performance,
- inrichting van continuïteit en security,
- opstellen van contracten zoals SLA's,
- inrichting van beheergroepen,
- koppeling van ITIL-processen en implementatie ervan in kleinere organisaties,
- bereikte kostenbesparingen met het inrichten van procesgericht werken,
- optimale combinaties van procesgericht en afdelingsgericht werken binnen de IT-dienstverlening,

— afspraken maken bij outsourcing, en meer.

Kortom, er zijn talloze onderwerpen waarvoor u binnen uw organisatie creatieve oplossingen hebt gevonden en die de moeite waard zijn om er anderen over te vertellen.

De redactie van IT Beheer Magazine legt bij artikelen sterk de nadruk op wat praktisch, concreet en doelgericht is.

Kijk voor meer informatie op www.itbeheermagazine.nl (klik door op "Schrijven").



Draag uw steentje bij om het beste beheer-magazine van Nederland te maken!

Thema's en deadlines 2003

Nr.	Thema	Deadline kopij	Deadline advertenties	Verschijnt
7	Security en continuïteit (Buyers' Guide Security)	15-7	20-8	12-9
8	Outsourcing, trends en ontwikkelingen (Buyers' Guide Outsourcing)	12-8	17-9	10-10
9	Datamanagement en gegevensbeheer (Buyers' Guide Storage)	16-9	22-10	14-11
10	Service management (Buyers' Guide Tools)	14-10	19-11	12-12

Adverteerdersindex

Exin 28	Kender Thijssen 22	OGD Software 40
Glidepath 30	Mercury Interactive 51	RSA 2
ISES International 52	Microsoft 26/27	The Tooling Event 36
IT Beheer Magazine 42	MProof 46	

Mercury
pagina 51

Atos O
pagina 52