Zo geef je monitorarch

Veel organisaties worstelen met het inrichten van hun monitorvoorziening om de afgesproken servicenormen meetbaar te maken. Hoe kan de monitorvoorziening onder architectuur worden vormgegeven? En hoe kunnen aan de hand van deze aanpak tien veelvoorkomende problemen worden opgelost?

Bart de Best

In *IT-Infra* nummer 2 en nummer 3 van dit jaar is uiteengezet hoe servicenormen voor ICT-services te bepalen ('Servicenormen gedefinieerd', B. de Best) en te meten ('Servicenormen meetbaar gemaakt', B. de Best). Dit artikel geeft aan hoe vanuit architectuur een kader gesteld kan worden aan het ontwerp en de inrichting van de monitorvoorziening om zo problemen tijdens het gebruik van de monitorvoorziening te voorkomen.

Veel organisaties richten een monitorvoorziening in door een product te kopen en aan de slag te gaan. Vaak worden vóór de aanschaf requirements opgesteld en wordt een vergelijking gemaakt van een aantal tools. Maar in de praktijk blijkt vaak dat de monitorvoorziening niet goed voorziet in de gewenste functionaliteit en de informatiebehoeften. Ook vormt het aantal monitortools in veel organisaties een onoverzichtelijk portfolio. Er wordt bij bezuinigingen naar hartenlust in gesneden, vaak zonder dat de consequenties bekend zijn. Dit artikel geeft aan de hand van een architectuurstappenplan een oplossing voor een aantal veelvoorkomende monitorknelpunten. Het kader dat nodig is om de monitorproblemen op te lossen wordt beschreven in de eerste drie stappen van dit stappenplan (beleid, architectuurprincipes en architectuurmodellen).

Oplossing

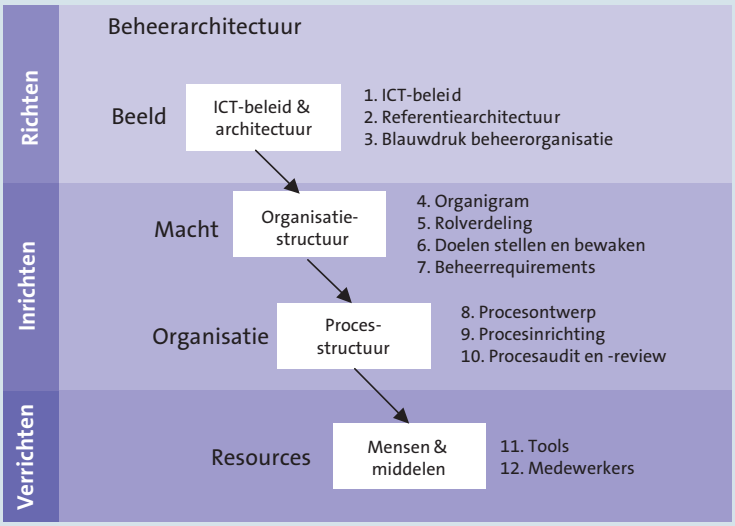
De genoemde problemen vereisen structurele tegenmaatregelen die hoog in de organisatie geborgd moeten worden. Een effectief middel is om afspraken te maken op managementniveau door beleidspunten op te nemen in het ICT-beleid en dit beleid te vertalen naar architectuurprincipes en architectuurmodellen. Dit kader moet door (beheer-)architecten bewaakt worden in zowel de lijn- als de projectorganisatie.

Tien problemen

Ondanks de tijd, geld en energie die gestoken wordt in het meetbaar maken van een ICT-service blijkt achteraf meer dan eens dat het beoogde resultaat niet is behaald. De volgende tien problemen zijn karakteristiek voor het falen van de monitorvoorziening:

1. **Verstoringen in de infrastructuur en applicaties worden niet waargenomen door de monitorvoorziening.**
2. **Het rekencentrum neemt infrastructuurverstoringen waar, maar weet niet welke ICT-services verstoord zijn.**
3. **De monitorvoorziening geeft aan dat alles 'zoemt' en dat de SLA-normen zijn gehaald, maar de gebruiker is ontevreden.**
4. **De robots die informatiesystemen end-to-end (E2E) doormeten stellen na ingebruikname perfect vast of de SLA-normen worden gehaald, maar werken niet meer na een aanpassing in de gebruikersinterface van de applicatie.**
5. **De events die worden waargenomen, zijn zo talrijk dat de filters van de monitorvoorziening zijn dichtgedraaid.**
6. **De monitortools staan maanden uit zonder dat het wordt waargenomen, omdat ze niet worden gemonitord.**
7. **De hiërarchie van tools die via koppelingen events aan elkaar doorgeven is zo complex dat niemand de totale werking ervan overziet, laat staan bewaakt en bestuurt.**
8. **De rapportages geven geen inzicht in wat de gebruikersorganisatie en beheerorganisatie nodig hebben qua procesbesturing.**
9. **Er zijn vele redundante tools, maar het is niet duidelijk waar geschrapt moet worden.**
10. **Het management stopt met de verdere inrichting van de monitorvoorziening vanwege bezuinigingen.**

itectuur vorm



Figuur 1 **Beheren onder architectuur (BEA-stappenplan).**

Naast deze strategische verankering is het belangrijk om de inrichting van de monitorvoorziening ook op tactisch niveau te borgen in het servicelevelmanagementproces en operationeel in een monitorproces.

Deze topdownbenadering is in figuur 1 uiteengezet. Links is de indeling richten, inrichten en verrichten te zien. Van boven naar beneden zijn de stappen beeld, structuur, vormgeving en resources weergegeven. Deze stappen zijn gelijk aan die van het paradigma van de verandermanager (beeld, macht, organisatie en resources). Dit paradigma geeft aan dat deze vier stappen van boven naar beneden moeten worden doorlopen. Bij een conflict moet de oplossing twee niveaus hoger worden gezocht.

De stap 'beeld' is het domein van de (beheer-)architecten. Deze functionarissen geven richting aan de monitorvoorziening door het beleid te vertalen naar architectuurprincipes en -modellen en deze vervolgens te borgen tijdens de inrichting van de monitorvoorziening en uitvoering van het monitorproces. In dit artikel gaat het alleen om de stap 'beeld', omdat dit de oplossingsrichting omvat voor de genoemde problemen. Wel wordt een aantal voorbeelden gegeven van hoe de aangegeven richting in de stappen 'structuur', 'vormgeving en 'resources' tot uitdrukking kunnen worden gebracht.

Stap 1 ICT-beleid

Het goed inregelen van een complete monitorvoorziening in een middelgrote tot grote organisatie blijkt in de praktijk meer dan eens een meerjarenplan te zijn. Helaas wordt gedurende die doorlooptijd nogal eens letterlijk en figuurlijk de stekker uit de voorziening getrokken vanwege bezuinigingen en uitblijvende resultaten. Daarom is het van belang dat de monitorvoorziening geborgd is in zowel ICT-beleid als -architectuur. In het ICT-beleid kunnen monitoraspecten opgenomen worden als monitorvolwassenheid, monitorportfolio, sourcing en partnership.

Voorbeeld volwassenheid (probleem nummer 10)

Het belangrijkste beleidsuitgangspunt is de volwassenheid van de monitorvoorziening. Dit bepaalt het ambitieniveau van deze voorziening in de gehele organisatie. Meestal worden minimaal de volgende volwassenheidsstadia onderkend: componentmonitoring, ICT-servicemonitoring en bedrijfsprocesmonitoring.

Het volwassenheidsniveau van de monitorvoorziening moet zorgvuldig worden gekozen. Deze keuze staat namelijk niet op zich. Zo vereist het monitoren van bedrijfsprocessen dat de gebruikersorganisatie deze processen onderkend heeft en de behoefte heeft om de doelstellingen van de geautomatiseerde ondersteuning van deze processen te meten en op de meetresultaten te sturen. Ook moet de beheerorganisatie een monitorvoorziening op bedrijfsprocesniveau kunnen inrichten en configureren, zoals het meten van businesstransacties en het kunnen waarnemen van trends. Eenmaal in productie genomen moet de beheerorganisatie samen met de business de meetresultaten kunnen interpreteren om verbeteringen aan te brengen in de beheerorganisatie en/of in de gebruikersorganisatie indien de doelstellingen van de bedrijfsprocessen niet worden gehaald. Hierbij geldt de randvoorwaarde van een businessalignment met de beheerorganisatie. Een onvolwassen beheerorganisatie die alleen productgeoriënteerd werkt zal immers niet in staat zijn om de ICT-servicenormen te monitoren die een meer volwassen gebruikersorganisatie stelt. De beheerorganisatie moet in dit geval in volwassenheidsniveau groeien om de businessalignment goed vorm te geven.

Ook komt het voor dat de beheerorganisatie volwassener is dan de gebruikersorganisatie. Dit kan leiden tot een spagaat waarbij de serviceafspraken op een lager volwassenheidsniveau worden gemaakt dan het niveau waarop de beheerorganisatie acteert. De rechtvaardiging van de extra kosten voor de monitorvoorziening is dan om aan te tonen dat de beheerorganisatie in ieder geval in control is (bijvoorbeeld vanwege wettelijke verplichtingen).

Het moeilijkste van de monitorvolwassenheid is het gekozen beleid effectueren. Vaak ontbreekt het aan architectuurcontrol en managementmandaat om het beleid te vertalen naar kaders en hieraan vast te houden. Een zwalkend beleid is het gevolg, net als geldverlies en frustratie op de werkvloer.

Voorbeeld monitorportfolio (problemen 7 en 9).

Veel organisaties zien door de bomen het bos niet meer als het gaat om monitortools. Om dit probleem het hoofd te bieden, wordt vaak gekozen voor een single vendor-beleid. Dit houdt in dat voor nieuwe tools één vaste leverancier wordt gekozen. De bestaande tools worden langzaam uitgefaseerd. Zo is een betere toolintegratie te bereiken. In de praktijk blijken altijd wel uitzonderingen op dit beleid nodig te zijn. Daarom is het belangrijk dat in de keuze van de vendor en de monitoroplossing aspecten als open architectuur en integratiemogelijkheden hoog scoren.

Andere voorbeelden

Ook de sourcing is een ICT-beleidspunt waard. Zo worden steeds meer monitorservices als een SaaS (software as a service) aangeboden. Het opnemen als beleidspunt is belangrijk, omdat in geval van nieuwe monitorbehoeften eerst gekeken moet worden of de gewenste functionaliteit als SaaS beschikbaar is in de markt. Hierdoor is het niet nodig om tooling aan te schaffen en hoeven kennis en kunde voor de nieuwe tool slechts ten dele te worden opgebouwd.

Afhankelijk van de grootte van de organisatie is het verstandig om een partnership met een monitortoolleverancier aan te gaan. Zo kunnen beide organisaties van elkaar leren. Het ICT-beleid kan dan worden afgestemd op de toekomstige mogelijkheden die een leverancier biedt.

Principe	AP1. Verstoringen die door E2E-metingen zijn waargenomen worden verklaard door componentmetingen.
Rationale	E2E-monitoring is maatgevend voor de metingen van SLA-normen. Daarmee worden echter niet alle verstoringen waargenomen. Tevens geeft de E2E-monitoring niet de exacte locatie weer. Componentmonitoring geeft wel invulling aan deze eisen, maar het is moeilijk om alle componenten van een ICT-service compleet te monitoren. Een combinatie van E2E-monitoring en componentmonitoring lost veel van deze problemen op.
Implicatie	Elk onderliggend infrastructuur- of applicatiecomponent waarvan de ICT-service gebruik maakt moet gemonitord worden voor alle van toepassing zijnde kwaliteitsaspecten zoals beschikbaarheid, performance, capaciteit en beveiliging.
Risico	Niet alle verstoringen worden waargenomen door E2E-monitoring, in ieder geval niet de verstoringen aan dubbel uitgevoerde infrastructuur- en/of applicatiecomponenten. Dit kan leiden tot grote verstoringen die voorkomen hadden kunnen worden.

Tabel 1 **Dekkingsgraad architectuurprincipes.**

Stap 2 Architectuurprincipes

Waar het ICT-beleid belangrijke beslissingen omvat, stippelt architectuur een migratiepad uit om vanuit de bestaande situatie (IST) te komen tot de gewenste situatie (SOLL). Hierbij worden architectuurprincipes en –modellen opgesteld ter kader en beeldvorming. Een principe wordt gedefinieerd door een oneliner die de gewenste richting geeft, de rationale die aangeeft wat bereikt moet worden, de implicatie die de gevolgen van het principe duidt en tot slot het risico dat beheerst moet worden. Ook is het belangrijk om de betreffende BEheren onder Architectuur (BEA)-stappen aan te geven (stappen 4 t/m 12 uit figuur 1), omdat hiermee geduid wordt welke architectuurcontrol het principe vereist.

Voorbeeld monitordekkingsgraad (probleem 1)

In tabel 1 is een voorbeeld van een architectuurprincipe opgenomen dat een oplossingsrichting geeft voor het eerste van de tien genoemde probleem. Het principe schrijft niet de oplossing voor in de vorm van een ontwerpeis, maar alleen het kader waarbinnen de oplossing gezocht moet worden. Dit is het fundamentele verschil met een requirement. Het benoemde risico weerspiegelt hier probleem 1.

Dit principe moet worden uitgewerkt in een aantal requirements waarin deze correlatie van E2E- en componentmonitoring is uitgewerkt (BEA-stap 6). Een voorbeeld is het vereisen van het hanteren van de Component Failure Impact Analyse (CFIA) van IBM, zoals ITIL die aanbeveelt, voor het bepalen van de bij een ICT-service betrokken componenten.

Een andere requirement is dat in de SLA-rapportage vermeld wordt welke gebreken aan de monitorvoorziening zijn aangetroffen en hoe deze opgelost worden. Hierbij is de monitorcontrolematrix zoals in tabel 2 een handig hulpmiddel.

Met het principe AP1 is probleem 1 goed te voorkomen of te beheersen. Vergeet echter niet dat er aan een probleemstelling verschillende oorzaken ten grondslag kunnen liggen. In dat geval zijn er wellicht ook verschillende architectuurprincipes nodig. Hierbij moet worden voorkomen dat er te veel architectuurprincipes worden opgesteld. Ook moeten architectuurprincipes kaderstellend zijn en niet voorschrijvend, anders verworden de principes tot requirements.

Monitor Controle Matrix		Componentgebaseerde metingen	
		Binnen normen	**Buiten normen**
E2E-metingen	**Binnen normen**	De servicenormen zijn gehaald.	Bepaal of en hoe de E2E-monitorfunctionaliteit aangepast moet worden.
	Buiten normen	Bepaal of en hoe de componentgebaseerde monitorfunctionaliteit kan worden aangepast.	Bepaal welke infrastructuur- of applicatiegebreken ten grondslag liggen aan deze verstoringen.

Tabel 2 **Monitorcontrolematrix.**

Voorbeeld decompositie ICT-services (probleem 2).

Om te voorkomen dat in geval van een verstoring aan een component niet bekend is welke ICT-service is geraakt, kan het AP2-principe worden gehanteerd: 'Van elke ICT-service zijn de onderliggende infrastructuur- en applicatiecomponenten bekend.' Hierdoor is het mogelijk om de oplostijd van verstoringen aan infrastructuur- en applicatiecomponenten te baseren op het belang van de business. Er zijn diverse requirements nodig om dit principe te borgen (BEA-stap 6). Zo moet de relatie tussen een ICT-service en de betrokken CI's in de configuratiemanagementdatabase (CDMB)-tool geadministreerd kunnen worden, net als eventuele relaties tussen ICT-services onderling. Daarnaast moet het monitorprocesontwerp de vereiste rapportages beschrijven (BEA-stap 7). Dit principe heeft ook grote gevolgen voor de keuze van de CMDB-tool (BEA-stap 11).

Voorbeeld ontevreden gebruiker (probleem 3)

Het gevaar van het monitoren van een ICT-service is dat deze niet aansluit op de serviceafspraken. Dat een AIX-host beschikbaar is, wil nog niet zeggen dat een gebruiker van een ERP-applicatie die op die host draait kan werken. Zelfs als in de SLA alleen een beschikbaarheid op hostniveau is afgesproken, wil dit niet zeggen dat de gebruiker ook tevreden is. Twee principes die dit borgen zijn 'AP3. Servicenormen in een SLA worden afgesproken in businesstermen' en 'AP4. Het niveau van ICT-serviceafspraken bepaalt het niveau en de monitorvoorzieningfunctionaliteit.' Natuurlijk kan het voorkomen dat er een technische service is en dat de klant een technische SLA wil, zoals de beschikbaarheid van het WAN. Het principe AP3 voldoet dan nog steeds. De businesstermen zijn in dat geval alleen technisch van aard, maar zijn wel de termen die de klant zelf hanteert. Het principe AP4 geldt ook nog steeds. De meting moet namelijk plaatsvinden op WAN-niveau en niet op routerniveau.

Voorbeeld robotonderhoud (probleem 4)

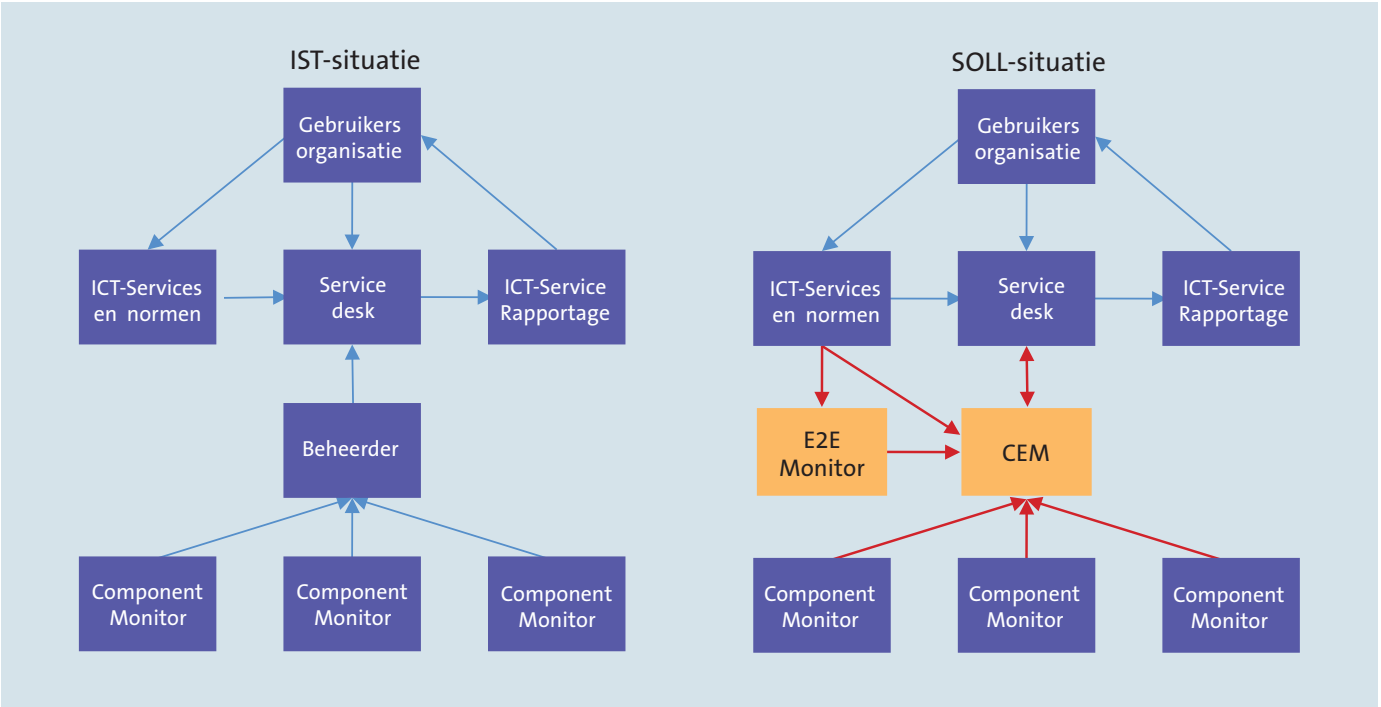
Vaak wordt vergeten dat een robot die een applicatie E2E meet gevoelig is voor aanpassingen aan de applicatie. De kleinste verandering aan de gebruikersinterface van de applicatie kan het robotscript onbruikbaar maken. De robotfunctionaliteit moet als onderdeel van de applicatie worden gezien. Een bruikbaar principe is in dit geval: 'AP5. De levenscyclus van de monitorvoorziening van de ICT-service is een integraal onderdeel van de levenscyclus van de ICT-service.' Dit principe impliceert dat de organisatie die verantwoordelijk is voor het functioneel beheer van de ICT-service ook het beheer van de monitorvoorziening voor zijn rekening neemt. Normaliter is dit de gebruikersorganisatie, want daar is de functionele kennis aanwezig om te bepalen welke aspecten van een ICT-service gemonitord moeten worden. De business moet dan ook van meet af aan betrokken zijn bij de opzet van de monitorfunctie.

Voorbeeld filters (probleem 5)

Veel organisaties zijn niet in staat om de events die door de monitorvoorziening worden waargenomen te verwerken en draaien de filters zo ver dicht dat alleen die events waarvan ze een alert willen ontvangen actief worden bewaakt. Dit leidt tot prachtige maar onbetrouwbare rapportages. In plaats van aan dit kraan-dichtprincipe moet er juist gewerkt worden aan een kraan-openprincipe: 'AP6. Alle events moeten worden geëvalueerd.' De events die onderkend zijn als schadelijk worden als incident aangemeld bij de servicedesk (negatief filter). De events die onderkend zijn als vertrouwd worden genegeerd (positief filter). Van events die alleen in bepaalde hoeveelheden schadelijk zijn, wordt op basis van een threshold een alert afgegeven (statistisch filter). Het residu aan events moet dagelijks worden geëvalueerd en opgenomen in een van de drie filters. Hierdoor zal het residu steeds verder slinken tot een behapbaar aantal.

Voorbeeld monitor de monitor (probleem 6)

Het gevaar van het kraan-dichtprincipe is dat het lang kan duren voordat geconstateerd wordt dat de monitorvoorziening überhaupt niet aan staat en/of verkeerd geconfigureerd is. Een principe dat dit voorkomt is: 'AP7. Elke monitortool wordt gemonitord op een juiste werking.' Dit kan bijvoorbeeld wrden ingevuld aan de hand van een E2E-monitoring.



Figuur 2 **IST-SOLL Monitorarchitectuurmodel.**

Voorbeeld bestuurlijke behoefte (probleem 8)

De bestuurlijke behoeften van zowel de gebruikersorganisatie als de beheerorganisatie vormen de basis voor de definitie van de ICT-services monitoring en de toegekende normen ('Beheren onder Architectuur', B. de Best, NGN, 2008 ISBN 9789081338011). Dit impliceert het principe: 'AP9. De meetpunten van de monitortools worden bepaald door de kritieke succesfactoren van de beheerprocessen en de bedrijfsprocessen.'

Stap 3 Architectuurmodellen

Architectuurmodellen zijn een uitstekend middel om de gewenste monitorvoorziening (SOLL) te schetsen. Door ook een model op te stellen van de huidige monitorvoorziening (IST) kan een duidelijk migratiepad van IST naar SOLL worden uitgestippeld. Figuur 2 toont een voorbeeld van zo'n IST/SOLL-monitorarchitectuurmodel. Een andere vorm van een architectuurmodel is een classificatiemodel. Ook dit is een handige gereedschap om de gewenste beeldvorming te bereiken. Een voorbeeld hiervan is het eerder gepubliceerde monitorlagenmodel in IT Beheer Magazine ('SPS brengt business & IT samen', B. de Best, IT Beheer Magazine, 2008, nr 5.)

Toelichting IST

In de huidige situatie is er een duidelijk onderscheid tussen servicemanagement en systeemmanagement. Vanuit servicemanagement zijn de ICT-servicenormen onderkend. Deze dienen als maatstaf voor de ICT-service, die bewaakt worden op basis van de meldingen die bij de servicedesk binnenkomen. Dit is tevens de basis voor de rapportages. De componentmonitortools geven events af die de systeembeheerder interpreteert. Als een beheerder het nodig acht, maakt hij handmatig een incident aan in de servicedesktool. Het moge duidelijk zijn dat in deze IST-situatie vele van de tien genoemde problemen zich kunnen voordoen. Om deze problemen op te lossen, biedt de in figuur 2 geschetst SOLL- situatie soelaas.

Toelichting SOLL

Net als in de huidige situatie stelt de servicelevelmanager in samenwerking met de gebruikersorganisatie de normen voor de ICT-services vast (AP3). Deze normen dienen als maatstaf voor de servicedesk medewerkers, de E2E-monitor (AP4) en de Centrale Event Manager (CEM). De CEM krijgt events binnen van de E2E-monitor en de componentmonitortools. In de CEM is de ICT-service gemodelleerd op basis van de onderliggende infrastructuur- en applicatiecomponenten (AP2). Hierdoor kunnen verstoringen die E2E worden gemeten verklaard worden door componentmetingen (AP1). Op basis van businessrules leidt een event wel of niet tot een registratie van een incident in de servicedesk. Op basis van de ingestelde servicenormen vindt de bewaking plaats in de servicedesk en wordt er een SLA-rapportage aangemaakt. Dit architectuurmodel verschilt per organisatie en kan vaak nog verder gedetailleerd worden. De detaillering moet beperkt blijven tot een kaderstelling en geen ontwerp worden.

De beheerder is in de SOLL-situatie zeker niet overbodig geworden. Zijn inzet is nu echter gericht op het uitbouwen en verbeteren van de monitorvoorziening in plaats van als monitortool te fungeren. Hij is nu in de gelegenheid de kwaliteit van de serviceverlening te verhogen en zorg te dragen voor business-alignment.

Toelichting migratiepad

Het verschil tussen de IST- en de SOLL-situatie is duidelijk te zien. De monitortools hebben in de bestaande situatie geen geautomatiseerde interface met de servicedesktool. Ook is nog niet voorzien in een E2E-monitorvoorziening. Het migratiepad om van IST naar SOLL te komen kan bijvoorbeeld bestaan uit de volgende 'volwassenheidsstadia':

1. Componentmonitoring
2. E2E-monitoring
3. Correlatie component- en E2E-monitoring
4. Bedrijfsprocesmonitoring.

Conclusie

Het inregelen van een goede monitorvoorziening vereist niet alleen een borging op operationeel en tactisch niveau. Juist op strategisch niveau dient een anker aanwezig te zijn om de inrichting van de monitorvoorziening te borgen. Het anker wordt gevormd door het vastleggen van de te varen koers aan de hand van beleidsuitgangspunten. Dit beleid dient voorzien te worden van een architectuurplan waarin de huidige en gewenste situatie inclusief migratiepad worden vastgelegd. Architectuurprincipes en -modellen zijn de instrumenten voor de (beheer-)architect om de uitgestippelde koers te borgen.

Hierbij dank ik Miranda Goossens van IIR voor de toestemming om materiaal van de training beheerarchitectuur in dit artikel op te nemen. Tevens dank ik Louis van Hemmen (Bitall), Robert de Koning (IBM), Carolien Glasbergen (UWV), Jack Jagt (SPS) en Linda Verweij (SPS) voor de review van dit artikel.

Literatuur

Artikel 'Beheerarchitectuur', B. de Best, IT Beheer Magazine 2007 nr 5.
Artikel 'Beheerarchitectuur in projecten', B. de Best, IT Beheer Magazine 2007 nr 8.
Artikel 'Beheerarchitectuur heeft nog een lange weg te gaan', B. de Best, IT Beheer Magazine 2007 nr 10.
Artikel 'Regie onder beheerarchitectuur', B. de Best, IT Beheer Magazine 2007 nr 10.
Artikel 'Business in control', Bart de Best, IT Beheer Magazine 2008 nr 6.
Artikel 'BPR voert regie onder architectuur', B. de Best, IT Beheer Magazine 2008 nr 7.
Artikel 'Beheerarchitectuur gepositioneerd', B. de Best en Pascal Huijbers, IT Beheer Magazine 2009 nr 8.

Bart de Best. E-mail: bartb@dbmetrics.nl

COLUMN SECURITY MATTERS

Privacy is PET

Als een knuffelbeertje, zo komt-ie over. Jacob Kohnstamm is van het College Bescherming Persoonsgegevens (CBP). Als Facebook onze privégegevens rondstrooit, dan bromt onze Jacob ze toe: 'Foei!' Als de politie ons rijgedrag te lang bewaart, dan spreekt het CBP. Medische dossiers rondpompen in EPD's – luistert naar Jacob. Als Jacob spreekt, dan luistert iedereen. Nou ja, een beetje.

Dus, luister mee. Jacob vindt dat het met de privacy beter kan. Het moet zelfs PET. PET staat voor Privacy Enhancing Technology. Het idee is heel simpel. In plaats van bang te zijn voor IT zetten we IT juist in ter bescherming van privacy. Er zijn drie eenvoudige principes. Allereerst worden de privacygevoelige gegevens losgeknipt van de identiteit. Vergelijkbaar met de auto: op je nummerplaat staat niet 'Pietje Puk' maar een kenteken, en alleen als er een aanleiding is wordt het kenteken gekoppeld aan de persoon. Het tweede principe is dat een gebruiker alleen die gegevens ziet die in zijn rol van belang zijn.

Als Jacob spreekt, dan luistert iedereen. Nou ja, een beetje

De doktersassistent ziet wel uw afspraakgegevens, maar niet of u voor uw druiper of uw linkerknie komt. De dokter ziet dat wel. Het derde principe is dat je persoonsgegevens beheersbaar maakt bij eerste opname, gebruik, doorgifte en verwijdering: een life cycle voor persoonsgegevens. Een slim idee dat in Europa is overgenomen als 'privacy by design'.

Het CBP vindt het tijd voor een andere koers. Een verschuiving van voorlichting naar handhaving. Dat vraagt echter een ander soort mensen en werkwijze bij het CBP. We hebben een privacywaakhond nodig, maar van de privacypoedel maak je nog geen privacypitbull. Het CBP wil zwaardere middelen voor handhaving: geloofwaardige boetes en flinke celstraffen. Maar daar wil de Tweede Kamer voorlopig niet aan. Dus blijft het CBP wat het is: een tandeloze teddybeer.

Dr. ir. Paul Overbeek RE

Combineert een eigen praktijk met docentschappen aan de universiteiten Erasmus, Tilburg en Amsterdam. www.ois-nl.eu of Paul.Overbeek@ois-nl.eu