VIRTUALISATIE:

alleen maar **voordelen?** (deel 1)

'If it's there and you can see it – It's Real!
If it's not there and you can't see it – It's Gone!
If it's there and you can't see it – It's Transparent!
If it's not there and you can see it - It's Virtual!'
(Roy Wilks, 1983)

Virtualisatie van servers is een veelgebruikte manier om efficiency en effectiviteit binnen IT-organisaties te verhogen. In dit artikel wordt het concept van virtualisatie verduidelijkt, de positie van virtualisatie ten opzichte van de klassieke situatie met alleen een fysieke server in beeld gebracht en aandachtspunten worden aangekaart om risico's te kunnen beheersen. Het artikel verschijnt – in verband met de lengte – in twee delen.

ANGELO MONTERO

Door de toepassing van virtualisatiesoftwarepakketten worden mogelijkheden geschapen om (meer) voordelen te behalen uit de IT-systemen. Oftewel, virtualisatie op zich is geen wondermiddel, maar levert voordelen op 'in combinatie met'. Tegenwoordig is virtualisatie niet meer weg te denken uit IT-organisaties. Het onderzoeksbureau Gartner [PULT06] noemde virtualisatie een 'megatrend' en het beste hulpmiddel dat bedrijven momenteel hebben om efficiëntieverbetering en serveroptimalisatie te realiseren. IT-leveranciers zien ook toekomst in deze technologie en zijn bezig om allerlei virtualisatieproducten te vervaardigen. Op dit moment zijn al diverse virtualisatiesoftwarepakketten op de markt verkrijgbaar. Deze variëren van commerciële tot *open source*-producten, waarbij de virtualisatietechniek en implementatie verschillen. De voornaamste verschillen tussen deze producten zijn de toegepaste techniek, bijkomende functionaliteit en volwassenheid.

Maar hoe is het succes van virtualisatie te verklaren? In de klassieke situatie bestaat een server uit een stuk hardware en één besturingssysteem. Wanneer gebruik wordt gemaakt van virtualisatie bestaat een server – in zekere zin – alleen maar uit software. En software is meer te bewerken dan hardware. Technologisch gezien ligt de kracht van virtualisatie in het feit dat een stuk programmatuur zich gedraagt als hardware, waardoor er nieuwe deuren opengaan. Die nieuwe deuren zijn de verschillende toepassingen en *(proprietary) features* van de verschillende virtualisatieproducten. Deze toepassingen hebben direct of indirect invloed op de IT-organisatie en -processen.

De belangrijkste (beoogde) voordelen van virtualisatie zijn kostenreductie en flexibiliteit. Voor de IT-manager zijn deze voordelen zeker aantrekkelijk. Maar naast kosten dient de IT-manager ook rekening te houden met andere kwaliteitscriteria, zoals exclusiviteit, integriteit en beschikbaarheid. Hij dient zich bewust te zijn van alle mogelijke risico's die de toepassing van virtualisatie met zich meebrengt, om zo de nodige maatregelen te kunnen treffen. IT-auditors zijn vanwege hun expertise op het gebied van IT, advies en attesteren de aangewezen personen om de IT-manager van dienst te kunnen zijn tijdens het hele virtualisatietraject.

OPBOUW ARTIKEL

Het doel van dit artikel is tweeledig; het is de bedoeling om

1. inzicht te verschaffen in het concept van virtualisatie en in de mogelijke risico's die het gebruik van deze technologie met zich meebrengt; en
2. een raamwerk aan te reiken op basis waarvan beheersmaatregelen afgeleid en getroffen kunnen worden bij de invoering van virtualisatie.

In het eerste deel van dit artikel (in deze editie van *de EDP-Auditor*) gaan we in op het concept van virtualisatie en de mogelijke risico's. Het tweede deel van het artikel (in een volgend

nummer) heeft het raamwerk als onderwerp.

De volgende vragen worden beantwoord:

1. Wat is virtualisatie en hoe is het ontstaan?
2. Wat zijn de meest voor de hand liggende toepassingen van virtualisatie?
3. Wat zijn de gevolgen op IT-processen bij de implementatie van virtualisatie?
4. Welke risico's brengt het gebruik van virtualisatie met zich mee?
5. Wat is de ervaring in de praktijk betreffende de implementatie van virtualisatie?
6. Welke (delen van) bestaande beheersingskaders kunnen gebruikt worden bij een virtualisatietraject?

Het artikel is geschreven vanuit de optiek van een *allround* IT-auditor, waarbij de nadruk niet ligt op de technische implementatie c.q. inrichting van virtualisatie. Wel staan de aandachtspunten centraal die relevant zijn bij een virtualisatietraject, verwerkt in een managementcyclus.
In dit eerste deel van het artikel komt het concept virtualisatie, met de technische en de bedrijfseconomische begripsvorming, aan bod. Ook zal enige informatie verstrekt worden inzake de oorsprong van virtualisatie. Hierna worden toepassingen van deze techniek toegelicht. Om de behandelde theorie vervolgens te relateren aan de praktijk, wordt een casus beschreven.

Virtualisatie heeft ook enkele bijzondere aandachtspunten. Daarom zal tevens aandacht worden besteed aan aandachts- en knelpunten met betrekking tot de toepassing van virtualisatie. Om te illustreren wat voor invloed de toepassing van virtualisatie heeft op de IT-processen, worden de ITIL-processen onder de loep genomen. Er is voor ITIL gekozen, omdat ITIL in de IT-auditwereld een algemeen geaccepteerd referentiekader is, als het gaat om inrichting en beheersing van IT-processen.
In het tweede deel van dit artikel (in de volgende editie van *de EDP-Auditor*) wordt een raamwerk ontwikkeld, dat de IT-auditor moet helpen de risico's te identificeren bij een virtualisatietraject. ▶

CONCEPT EN DEFINITIE

Alvorens verder te gaan met de toepassingen van virtualisatie worden nu eerst in een notendop het concept en de definitie van virtualisatie uitgewerkt. In de praktijk komen verschillende vormen van virtualisatie voor zoals netwerkvirtualisatie, applicatievirtualisatie, servervirtualisatie en opslagvisrtualisatie. Waar het in dit artikel om gaat, is servervirtualisatie op X86-platformen [OTEY06]. Tot X86-platformen behoren onder andere de gebruikelijke Windows- en Linux-servers, maar ook de kantoordesktops. Uit de vele definities heb ik een eigen definitie afgeleid: *virtualisatie is de techniek die het mogelijk maakt dat besturingssystemen met bijbehorende applicaties softwarematig draaien op één fysieke computer, elk in hun eigen afgeschermde omgeving, gebruikmakend van een deel van de totale hardwarecapaciteit als 'eigen' resources en onafhankelijk van elkaar.*

Voor de eindgebruiker lijkt het alsof een softwarematige computer een echte fysieke machine is. Dit terwijl feitelijk slechts een deel van de fysieke machine gebruikt wordt om met behulp van software een virtuele machine op te zetten. In figuur 1 is een vereenvoudigde voorstelling gegeven van dit principe.

Op een fysieke server worden een besturingssysteem – hetzij compleet, hetzij uitgekleed – en de virtualisatiesoftware geïnstalleerd. Dit besturingssysteem wordt de *host* genoemd, terwijl de virtualisatiesoftwarelaag de *virtual machine monitor* (VMM) wordt genoemd. Bij sommige virtualisatieproducten vormen het besturingssysteem en de virtualisatielaag één geheel. Vervolgens worden op deze VMM-laag virtuele machines (VM's) gemaakt. Op deze VM's wordt vervolgens naar keuze een besturingssysteem – een zogeheten *Guest* – geïnstalleerd. De hardwarevoorzieningen worden verdeeld onder de VM's. Het betreft de harde schijf, de netwerkkaart, de CPU en het RAM-geheugen. Elke VM is logisch afgeschermd van de overige VM's en kan gezien worden als een aparte machine. Een VM die een besturingssysteem en applicatie(s) bevat, kan als een *encapsulated* eenheid gezien worden. Dit betekent dat een VM in zijn geheel verplaatst of gekopieerd kan worden en elders opnieuw kan worden geïnstalleerd. Deze VM-eenheid is onafhankelijk van de hardware. Deze vorm van virtualisatie wordt *full virtualization* genoemd.

Figuur 1 Vereenvoudigde voorstelling virtualisatieprincipe

Applicatie 1	Applicatie 2	Applicatie 3
Windows XP	Linux	Windows 2003
	virtual machine monitor	
	host operating system	
	hardware	

OORSPRONG VIRTUALISATIE

Virtualisatie vindt haar oorsprong in het laboratorium van IBM [CREA81] [COMP01]. De mainframes van IBM maken al lange tijd gebruik van deze techniek in de vorm *logical partitions*. Logical partitions staat voor logische partities, ofwel het opsplitsen van een volledige *mainframe* computer in meerdere logische delen, waardoor het voor de gebruiker lijkt alsof er sprake is van meerdere onafhankelijke besturingssystemen. Echter, een betere vergelijking met de nu in opkomst zijnde virtualisatievormen is de door IBM in 1972 geïntroduceerde VM/370. Door middel van de VM/370 was het mogelijk om softwarematig meerdere van elkaar onafhankelijke en afgeschermde machines te creëren op een mainframe. Tot voor kort konden alleen degenen die de beschikking hadden over een (duur) mainframe gebruikmaken van dit principe. Tegenwoordig zijn 'conventionele' x86-servers zodanig in kracht en mogelijkheden gegroeid, dat virtualisatie ook op deze hardware aantrekkelijk is. Ook de benodigde virtualisatiesoftware heeft grote ontwikkelingen doorgemaakt, waardoor er op dit moment betrouwbare virtualisatieproducten op de markt verkrijgbaar zijn.

BEDRIJFSECONOMISCHE BETEKENIS VAN VIRTUALISATIE

De voornaamste reden om over te stappen naar virtualisatie is kostenvermindering. De kostenvermindering is een gevolg van een verlaagde Total Cost of Ownership (TCO). De TCO bestaat uit alle kosten die gepaard gaan met het aanschaffen, gebruiken, beheren en buiten gebruik stellen van informatietechnologie door een organisatie gedurende de levenscyclus van de producten [FIJN05]. In dit specifieke geval van virtualisatie heeft de besparing op TCO betrekking op de hierna besproken componenten [VMWA05-1].

Besparing op hardwarekosten
- Minder fysieke servers in het *serverpark* nodig.

Besparing operationele ICT-kosten
- Reductie van stroom- en koelingskosten.
- Reductie van huurkosten in een datacenterruimte.
- Minder netwerkkosten door het gebruik van virtuele netwerkapparatuur.
- Beheerders hebben minder tijd nodig om servers op te zetten, te configureren en te migreren.

Besparing van downtimekosten
- Reductie van geplande *downtime*.
- Reductie van ongeplande downtime.

In de volgende paragraaf ga ik in op de meest voor de handliggende toepassingen van virtualisatie.

TOEPASSINGEN VAN VIRTUALISATIE

Om virtualisatie te realiseren zijn er verschillende producten op de markt. De meest bekende producten voor de servermarkt zijn VMware, Virtuozzo en Microsoft Virtual Server. Voor een uitgebreidere lijst van producten wordt verwezen naar [RECH06]. Hierna volgt een beknopt overzicht van veel voorkomende toepassingen van virtualisatie [OGLE05] [MARS06] WOLF05] [VMWA05-2] [VMWA05-3].

Serverconsolidatie
De huidige praktijk is om elke applicatie op een fysiek aparte server te installeren. Deze praktijk wordt gevolgd om voor kritieke applicaties een hoge mate van beschikbaarheid te realiseren. Het installeren van twee applicaties op dezelfde server wordt afgeraden, vanwege de kans op conflicten en wederzijdse beïnvloeding en afhankelijkheid door het gemeenschappelijke gebruik van het *operating system*. De oplossing is een *dedicated server* per applicatie. Het gevolg is dat dure hardware aangeschaft wordt, die niet optimaal benut wordt, omdat er slechts één applicatie op draait. Door gebruik te maken van virtualisatie kunnen alle applicaties via dedicated VM's geïnstalleerd worden op één fysieke machine. Zo wordt consolidatie gerealiseerd met een scheiding tussen de verschillende omgevingen.

Ontwikkel-, Test- en Acceptatiecyclus (OTA-cyclus)
Applicatieontwikkelaars hebben te maken met verschillende applicaties die op meerdere besturingssystemen moeten kunnen functioneren. Het kunnen beschikken over een eigen computer met in het algemeen één applicatie per besturingssysteem is dus wenselijk. Helaas levert dit nog altijd problemen op, omdat het een kostbare zaak is om zoveel fysieke servers aan te schaffen. Aan de andere kant is hergebruik van deze fysieke servers tijdrovend, omdat deze telkens anders geïnstalleerd en geconfigureerd dienen te worden. En in de tussentijd kunnen andere ontwikkelaars met andere behoeften geen gebruikmaken van deze fysieke machine.
Wat betreft het test- en acceptatieproces dienen er voldoende representatieve servers beschikbaar te zijn om tests uit te voeren of om problemen op te lossen alvorens bepaalde wijzigingen of installaties worden uitgevoerd in de productieomgeving. Het aantal applicaties kan flink oplopen in grotere organisaties. Ook hier is het aanschaffen van en het telkens opnieuw inrichten van servers niet effectief en ook niet efficiënt.

Door gebruik te maken van virtuele machines kunnen testomgevingen snel opgezet worden. Er kan namelijk een bibliotheek van verschillende virtuele machines gemaakt worden. De installatie van een besturingssysteem en het inrichten van de machine hoeft slechts één keer te gebeuren. Ook kunnen virtuele netwerken geconfigureerd worden om bijvoorbeeld *n-tier*-architecturen te testen. Een n-tier-architectuur is een *client-server*-architectuur, bestaande uit *n* lagen die via het netwerk met elkaar zijn verbonden. Een voorbeeld van een *three-tier*-model is een *webbrowser* die via het netwerk is verbonden met een webapplicatie. De webapplicatie is vervolgens via het netwerk verbonden met een database server. De winst zit in het kopiëren en klonen van bestaande virtuele machines en het bijhouden van een soort bibliotheek met alle mogelijke configuraties van virtuele servers. Dit principe kennen we al in de vorm van een *master image*, ofwel een *bit-by-bit copy* van een geïnstalleerde en geconfigureerde computer c.q. harde schijf. Echter, er zijn twee nadelen te noemen bij deze conventionele *image*: een image is hardwareafhankelijk en het is niet mogelijk om meerdere images tegelijkertijd te draaien op een fysieke machine. Een vergelijking tussen een VM-bestand en een image is ook niet terecht. Een image dient altijd op een machine geïnstalleerd te worden, terwijl een virtuele machine als het ware opgestart en afgespeeld wordt.
Een ander voordeel van virtualisatie is de mogelijkheid tot snelle *rollback* die aanwezig is bij de toepassing van virtuele machines. Deze rollback is mogelijk, omdat er *snapshots* – lees foto's – van een virtuele machine op een bepaald moment gemaakt kunnen worden. Dit is hetzelfde principe dat we doorgaans als *journalling* kennen bij filesystemen en databases. Door de verminderde noodzaak tot configuratie van hardware – te weten de diverse afzonderlijke fysieke servers – wordt de OTA-cyclus verkort, wat bijdraagt tot efficiëntere IT-projecten.

'De voornaamste reden om over te stappen naar virtualisatie is kostenvermindering'

High-Availability
In Service Level Agreements (SLA's) komt vaak de eis voor, dat een systeem voor 99.x procent van 24 x 7 uur operationeel moet zijn. Deze eis wordt in het algemeen aangeduid als *High-Availability*, ofwel een hoge beschikbaarheid. High-Availability heeft betrekking op componenten die kunnen falen, waardoor de beschikbaarheid in gevaar komt. Om dit probleem op te lossen worden systemen redundant uitgevoerd. Het dubbel uitvoeren van hardware heeft als gevolg dat de investeringskosten toenemen, terwijl de redundante systemen alleen maar *stand by* staan en feitelijk niet echt dagelijks gebruikt worden als productiemachine.
Om toch minder hardware te gebruiken, wordt gebruik gemaakt van virtualisatie. Virtualisatie is voordelig wanneer er CPU-marge is op de stand by machine wanneer deze actief wordt. Hierdoor kunnen fysieke of virtuele servers bij hardwareproblemen overgenomen worden door andere virtuele servers die op een andere fysieke machine draaien. De migratie van de falende server naar de virtuele server op een andere fysieke machine gebeurt *on-the-fly*. De downtime van een draaiende applicatie op een falende server is dan nihil. Bij deze techniek wordt gebruikgemaakt van gemeenschappelijke opslag, meestal in de vorm van een SAN-oplossing. SAN staat voor Storage Area Network en is een *high speed* dedicated lokaal netwerk van opslagsystemen, gekoppeld aan servers en transparant voor de eindgebruiker.

Disaster recovery
In IT-jargon wordt *disaster recovery* in één adem genoemd met *back-up* en *restore*. Het zijn echter twee ver-

schillende processen. Back-up- en restore-voorzieningen of -maatregelen bestaan voor het incidenteel herstellen van kleine 'fouten'. Bij de meeste organisaties is dit een integraal onderdeel van de dagelijkse werkzaamheden. Hierbij wordt gebruikgemaakt van periodieke back-ups. Bij disaster recovery is de ernst van de situatie en de schade veel groter. Een ramp kan als gevolg hebben dat hele computercentra opnieuw opgebouwd dienen te worden. Dit proces kan in de praktijk heel tijdrovend zijn, vooral omdat er nauwelijks tests worden uitgevoerd om dergelijke rampscenario's na te bootsen. Te lang uit de lucht zijn kan fatale gevolgen hebben voor een organisatie.
Door gebruik te maken van virtualisatie wanneer er geen *gemirrorde* uitwijklocatie is, kan het disaster recoveryproces versneld worden. Men hoeft niet eerst op alle hardware het besturingssysteem te installeren en daarna de applicaties en data. Door gebruik te maken van back-ups van alle VM's hoeven deze enkel op de VMM geïnstalleerd te worden, waarna alle applicaties weer draaien. De winst in termen van efficiëntie betekent dat een organisatie een snelle recovery van de IT-systemen kan realiseren na een ramp, wat bijdraagt aan een hogere *business continuity*.

Behoud legacy-systemen
Legacy-systemen zijn IT-systemen waarvan òf het besturingssysteem òf de applicatie niet meer door de markt ondersteund wordt en die om uiteenlopende redenen niet gemigreerd kunnen worden naar moderne (hardware)systemen. Deze redenen kunnen bijvoorbeeld zijn: incompatibiliteit, financiën of gebrek aan expertise. Helaas is legacy – vanwege hardwareafhankelijkheid – een nog vaak voorkomend verschijnsel in IT-organisaties. Virtualisatie kan echter uitkomst bieden. Door de legacy-systemen te converteren naar een VM, worden het besturingssysteem en de applicatie losgekoppeld van de hardware. Hierdoor kan de desbetreffende VM met het oude besturingssysteem en bijbehorende applicatie als een *appliance* op elke hardware geïnstalleerd worden. (Een appliance is een dedicated eenheid bestaande uit hardware, met daarop één applicatie geïnstalleerd die ook bedoeld is om één dienst aan te bieden. Bijvoorbeeld een spelcomputer.) Het voordeel in dit geval is portabiliteit en flexibiliteit. Hierdoor kunnen legacy-besturingssystemen toch op moderne hardware gedraaid worden.

CASUS

De organisatie geheten 'ZBO' is een uitvoeringsorganisatie binnen de Rijksoverheid. Binnen ZBO vindt massale gegevensverwerking plaats, ondersteund door de diensten en producten van de IT-organisatie. De IT-organisatie van ZBO kampte een tijdje terug met drie problemen.

1. De wens om uitwijk te realiseren bij eventuele calamiteiten werd tot dan toe belemmerd. De remmende factor hierbij waren de operationele, maar gedateerde, Windows NT-systemen (oftewel legacy-systemen). Een logische beoogde stap was om een kostenefficiënte uitwijk te implementeren, waarbij ook de Windows NT-legacy-systemen gemigreerd konden worden, omdat sommige applicaties alleen konden draaien op Windows NT.
2. De OTA-straat bij ZBO was ook aan vernieuwing toe. Er was sprake van een situatie waarbij op enkele fysieke servers een mix van OTA-omgevingen draaide. Ook het opzetten van 'teststraten' was een tijdrovend proces. De IT-organisatie van ZBO wilde de OTA-straat vernieuwen en herstructureren om een beter beheersbare situatie te creëren.
3. Het was binnen ZBO gebruikelijk om voor elke nieuwe toepassing een eigen nieuwe server aan te schaffen. Echter, 90 procent van deze servers was 98 procent van de tijd inactief. Dit werd niet erg gevonden, omdat 'toch maar een goedkope' server werd aangeschaft. Feitelijk was een nieuwe fysieke server echter nooit echt goedkoop. Een betere benutting van deze servers was daarom welkom.

Fasering
Nadat de IT-organisatie van ZBO vooronderzoek had gedaan, koos men uiteindelijk voor de implementatie van servervirtualisatie. De IT-manager maakte deze keuze puur op basis van de lage kosten. Deze keuze ging tegen het IT-beleid van ZBO in. Het beleid luidde dat ZBO *up-to-date* moest zijn wat betreft IT-oplossingen, maar niet voorop mocht lopen. Dit om te voorkomen dat een instabiele *non-proven technology* tot verstoringen zou leiden in de bedrijfsvoering. Ook de externe deskundigen raadden het gebruik van virtualisatie af, conform het beleid.

De uitwijklocatie werd gerealiseerd door middel van virtuele servers in combinatie met een SAN. Het gebruik van virtuele machines voor uitwijk betekende minder downtime bij een mogelijke calamiteit tegen lagere kosten, omdat er minder fysieke machines noodzakelijk zouden zijn. In de nieuwe OTA-straat werden virtuele servers ingezet in plaats van fysieke servers. Deze virtuele servers zouden snel en eenvoudig gekopieerd kunnen worden, waardoor het opbouwen van servers minder tijd in beslag zou nemen. Verder waren de verschillende virtuele servers volledig van elkaar afgeschermd, terwijl ze op dezelfde fysieke machine draaien. Enkele NT-systemen die nog niet uitgefaseerd konden worden, werden naar de nieuwe omgeving gemigreerd. De legacy Windows NT-machines werden door middel van virtualisatie hardwareonafhankelijk gemaakt en konden vervolgens op moderne hardware draaien. Als virtualisatieproduct werd VMware ESX aangeschaft. Dit omdat toentertijd dit het meest volwassen, functionele en stabiele product was. Ook de prijs was aantrekkelijk.

ZBO heeft ook geleerd van het hele virtualisatietraject. Zo kunnen de volgende punten genoemd worden als *lessons learned*.

- Een degelijk vooronderzoek is van essentieel belang. Zo kwam men er pas in een later stadium achter dat niet alle applicaties geschikt waren om op virtuele machines te draaien. Ook was Vmware ESX niet compatibel met alle hardwarecomponenten.
- De invloed van de techniek op de organisatie was onderbelicht. Zo ontstond er, om de nodige functiescheiding te realiseren, een nieuw cluster voor het beheer van Vmware ESX. Hierdoor werden andere clusters ingekrompen en moesten procedures intern worden aangepast.
- Migratie van alle machines in één keer doorvoeren is niet verstandig. Bij een geleidelijke migratie is er meer overzicht en controle.
- Versiebeheer van virtuele machines is lastiger dan het lijkt. Daarom is de werking van de procedures hiervoor van essentieel belang.
- Het is nodig om kritisch te blijven kijken naar virtualisatieproducten en de daarbij behorende marketing verhalen. Zo kwam men tot de conclusie dat het gebruik van virtuele netwerkcomponenten niet geschikt was voor de productieomgeving. Ten tijde van het project waren het beheer en de beveiliging van deze componenten lastig te realiseren.

Capaciteitsplanning wordt door het gebruik van virtualisatie nog belangrijker. De juiste balans dient gevonden te worden tussen de totale beschikbare CPU-capaciteit, belasting en aanschaf van hardware. Hierbij moet nog de juiste keuze gemaakt worden welke virtuele machines op dezelfde fysieke machine zullen draaien. Bij sommige applicaties is de belasting nooit constant en er moet voorkomen worden dat virtuele machines tegelijkertijd pieken of dat bij een enkele piek een tekort aan CPU-kracht ontstaat. Daarnaast is er nog een beperkende factor, namelijk het intern geheugen. Het geheugen bepaalt namelijk mede hoeveel virtuele machines op één fysieke machine geinstalleerd kunnen worden.

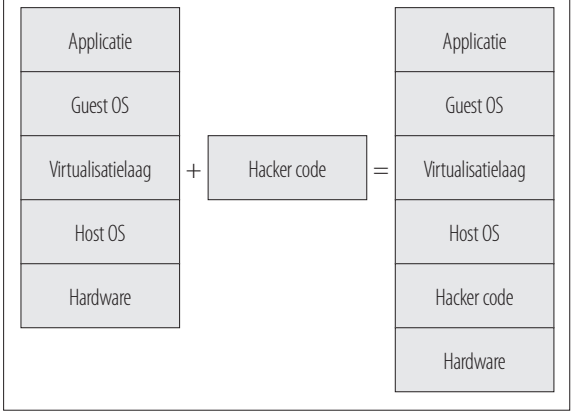
AANDACHTSPUNTEN BIJ HET GEBRUIK VAN VIRTUALISATIE

Zoals eerder vermeld werd, betekent virtualisatie in zekere zin functioneel zelfstandige hardware, maar dan in de vorm van programmatuur, oftewel software. Het gevolg is dat aan de techniek van virtualisatie naast een aantal voordelen ook een aantal nadelen kleeft. Hierna volgt een overzicht met aandachtspunten.

Omdat virtuele machines met bijbehorende applicaties als bestanden worden opgeslagen, zijn virtuele machines portabel. Hierdoor is het, in tegenstelling tot een grote fysieke server, in theorie makkelijker om ongeautoriseerd complete servers met bijbehorende applicatie en data te kopiëren en deze voor kwade bedoelingen te gebruiken. Daarnaast is er een verhoogd risico aanwezig op wildgroei van virtuele machines. Invoering van virtualisatie stelt daarom eisen aan versiebeheer en beveiliging van de VM-bestanden.

Alle software is per definitie *malware*-gevoelig. Zo is het bekend dat het kwaadaardige computerprogramma 'Blue Pill' [RUTK07] gebruikmaakt van de virtualisatieprincipes en zichzelf on-the-fly en ongemerkt als *host operating system* kan installeren op een fysieke server. Het oorspronkelijke host-besturingssysteem wordt dan een *guest*-besturingssysteem in een virtuele machine, dat op het nieuwe host-besturingssysteem draait. Hiermee heeft de *hacker* via zijn nieuwe host-besturingssysteem controle over het guest-besturingssysteem en dus over de applicaties die daarop draaien. De detectie van de aanwezigheid van de kwaadaardige code is mogelijk, maar om het te ontdekken, moet men zich wel bewust zijn van dit risico. In figuur 2 is het effect van Blue Pill geïllustreerd.

Figuur 2 Illustratie van de werking van de kwaadaardige code 'Blue Pill'



Een VM kan een besturingssysteem met bijbehorende applicatie bevatten. Deze applicatie kan van alles zijn, bijvoorbeeld een *firewall*. Tegenwoordig zijn deze kant-en-klare op virtualisatie gebaseerde applicaties van het internet te downloaden. De gebruiker hoeft zelf niets te installeren, te compileren of te configureren. Deze nieuwe vorm van *plug-and-play* is zeker aantrekkelijk voor de thuisgebruikers met weinig IT-kennis. Maar tegelijkertijd loopt men het risico VM's te downloaden waarvan niet bekend is wat voor functionaliteiten in de VM's verborgen zitten. Ook in deze VM's kan kwaadaardige code zitten.

Ondanks dat virualisatieproducten al in productieomgevingen gebruikt worden, dient men alert te blijven. De virtualisatielaag blijft kwetsbaar en hackers zullen voortdurend blijven zoeken naar hiaten in de software. Het is niet ondenkbaar dat in de toekomst deze hackers vanuit een virtuele machine kunnen inbreken in een andere virtuele machine op de fysieke server of zelfs in de fysieke server zelf. Degelijk *patchmanagement* kan deze risico's minimaliseren.

De *add-ons* die de verschillende virtualisatieleveranciers bieden en *third party tools* brengen ook risico's met zich mee. Het *live* migreren van virtuele machines van de fysieke host server A naar fysieke host server B kan problemen veroorzaken. Stel bijvoorbeeld dat de virtuele machine achter een firewall zit en ook nog verbonden is met een database server. Bij live migratie van de virtuele machine naar een andere fysieke machine dient ook aandacht te zijn voor de aansluiting van de firewall en de database server op de nieuwe fysieke machine. Bij deze live migratie gaat data met informatie ▪

Tabel 1 Invloed van virtualisatie op ITIL-processen

Tactische ITIL-processen	Operationele ITIL-processen
Financial Management: Verschuiving van investeringen. In plaats van meer fysieke servers aan te schaffen dient in de meeste gevallen geïnvesteerd te worden in een SAN.	**Servicedesk[1]:** Door gebruik te maken van virtuele machines kan de Servicedesk beschikken over meerdere applicaties en besturingssystemen waardoor op een efficiëntere manier kan worden gewerkt om vragen te beantwoorden. Er behoeven geen verschillende fysieke machines te worden ingericht met elk een eigen versie van besturingssysteem of applicatie. Ook kan snel een kopie worden gemaakt van de oorspronkelijke fysieke of virtuele server en kan een virtueel netwerk gebruikt worden ten behoeve van troubleshooting.
IT Service Continuity Management: De toepassing van virtualisatie in combinatie met een SAN resulteert in effectieve IT Service Continuity Management. Bij calamiteiten kunnen systemen tegen geringe kosten in weinig tijd met weinig inspanning worden opgebouwd. Hierdoor wordt een hogere continuïteit aan de afnemers aangeboden en blijft de ICT-dienstverlener gespaard van onder andere eventuele boeteclausules en imagoschade.	Incident Management: De processen Incident, Problem en Change Management zijn nauw met elkaar verbonden. Het gaat in principe om het oplossen van verstoringen, het testen van de oplossing en het vervolgens transporteren van de verbeterde applicatie naar een productieomgeving. De winst ten gunste van deze processen is divers: vermindering van storingstijd en downtime, vermindering in kosten van testomgevingen en verbetering van de reactietijd op meldingen. Doordat er minder tijd nodig is om systemen op te bouwen en te testen, kunnen de medewerkers meer in minder tijd doen. Doordat virtualisatie een nieuwe techniek is, zal, zeker in het begin, het aantal incidenten en problemen oplopen. Dit kan komen vanwege de niet-comptabiliteit tussen de virtualisatieproducten en de hardware en applicaties, maar ook door bijvoorbeeld door menselijke vergissingen of misconfiguraties. Door het ontbreken van een database van 'meest voorkomende problemen' bij virtualisatie, zal het trial-and-error proces in beginsel veel tijd in beslag nemen. Het gevolg is dat er meer meldingen zullen zijn en met langere doorlooptijden. Pas na een bepaalde leerperiode zullen de voordelen van virtualisatie zichtbaar worden.
Capacity Management: Met de toepassing van virtualisatie wordt dit proces kritiek. In de oude situatie waren de systemen overgedimensioneerd of onbenut. Bij het draaien van meerdere virtuele machines op een fysieke server is een gedegen capaciteitsplanning noodzakelijk om te voorkomen dat systemen CPU-kracht of RAM-geheugen tekortkomen. Omdat elk systeem een piekbelasting heeft, dient ook hiermee rekening te worden gehouden. Ook voorafgaand aan live migraties van virtuele machines naar andere fysieke servers dient aandacht te worden besteed aan de beschikbare capaciteit op de nieuwe fysieke server.	**Problem Management:** Zie Incident Management.
Availability Management: In de traditionele wereld van alleen fysieke servers dient extra geïnvesteerd te worden in extra hardware die in feite continu stand by staat en die niet echt benut worden. Ook moet bij een aantal *fail-over* oplossingen met fysieke servers de servers die stand by staan *gereset* worden of moeten de gebruikers hun pc's resetten alvorens verder te kunnen werken. Door toepassing van virtualisatie kan worden volstaan met minder fysieke servers. De servers die stand by staan zijn in dit geval virtuele servers. Virtualisatie is in dit geval alleen aantrekkelijk als er marge is in de CPU-belasting van de fysieke machine wanneer de stand by virtuele machine actief wordt. Bij een fail-over gebeurt dit on-the-fly en is het proces transparant voor de gebruikers waardoor er niets gereset hoeft te worden. Met virtualisatie kan ten behoeve van het proces Availability Management tegen geringe kosten een effectieve high availability gerealiseerd worden. Hierdoor neemt het aantal momenten van niet-beschikbaarheid en de duur van niet-beschikbaarheid af. Een gevolg hiervan is dat de nadruk verschuift van foutherstel naar serviceverbetering, hetgeen een kwalitatief betere dienstverlening inhoudt. Klanten zullen ook meer tevreden zijn. Wel is bij live migraties een aandachtspunt het feit dat alleen individuele virtuele machines gemigreerd worden. Zo is het niet vanzelfsprekend dat bij migratie van een webserver ook de via het netwerk aangesloten database server meegaat. Om dit toch op te vangen zijn complexere oplossingen nodig. Door het niet redundant uitvoeren van componenten kunnen verder bij een falende fysieke server in plaats van één machine – zoals in de traditionele situatie – meerdere virtuele machines *crashen*.	**Change Management:** Door de redenen genoemd bij Incident management zal het uitvoeren van veranderingen aanvankelijk veel tijd in beslag nemen. Ten gevolge van een toename in incidenten en problemen zullen ook de wijzigingen toenemen. Verder zal het proces Change Management een belangrijkere rol gaan spelen voor het proces Security Management: Samen met het proces Configuration Management moet Change Management ervoor zorg dragen dat alleen geautoriseerde wijzigingen worden doorgevoerd. Dit vereist speciale aandacht, omdat nu complete computers met besturingssysteem en applicatie en data als één bestand beschouwd kunnen worden. Dit betekent dat ze *portable* zijn en makkelijk zijn te kopiëren, aan te passen, te verplaatsen en te verspreiden. De drempel om aanpassingen in een server aan te brengen is lager en het feit dat geen fysieke toegang tot servers nodig is om een server met besturingsysteem, applicatie en data te vervreemden, maken de genoemde processen belangrijker dan voorheen. Hierdoor zijn er andere beheersmaatregelen nodig.
Service Level Management: Door lagere aanschaf-, beheer- en onderhoudskosten en de kortere doorlooptijden van projecten kunnen diensten tegen een aantrekkelijke prijs aangeboden worden. IT-projecten kunnen bij de toepassing van virtualisatie in bepaalde fasen minder tijd in beslag nemen, omdat van de meeste omgevingen actuele herbruikbare virtuele machines beschikbaar zijn. Het resultaat is een verbeterde Service Level Management. Aan de andere kant kan het voorkomen dat door gebrek aan kennis en praktische ervaring met de toepassing van virtualisatie en de gebruikelijke kinderziektes er aanvankelijk meer incidenten en problemen zijn. Dit kan van invloed zijn op naleving van de afspraken in de SLA .	**Configuration Management:** Door de toepassing van virtualisatie wordt het belang van hardware minder en worden virtuele machines als software geregistreerd en beheerd. Hierdoor kunnen virtuele servers en bijbehorende applicatie als één CI – oftewel appliance – worden geregistreerd, waardoor het proces minder complex wordt. Aan de andere kant is zelfs in de traditionele situatie een ontoereikend versiebeheer vaak de oorzaak van incidenten en problemen. In het geval van virtualisatie kunnen we dit vergelijken met versiebeheer van een word document, welke in de praktijk tegenvalt. Daarom moet aandacht besteed worden aan de procedures rondom versiebeheer en dienen deze ook nageleefd te worden.
Security Management: Virtualisatie introduceert nieuwe risico's. Voor een optimale invulling van dit proces zou opnieuw een gedegen risicoanalyse moeten worden gedaan voor de IT-systemen. Speciale aandacht dient te worden besteed aan de beveiliging van de bestanden van de virtuele machines in rust en in transitie, Change Management, versiebeheer en capaciteitsplanning. Ook het beheer van de virtualisatielaag is van belang om de integriteit van die laag te waarborgen.	

Noot

1 Service Desk is in feite een afdeling en geen proces. Overige processen zoals Incident en Problem Management starten met een melding bij de Service Desk. De Service Desk is vaak een soort *frontoffice* voor eindgebruikers die in contact staat met de *backoffice* van de aanbodkant.

over de huidige status van de virtuele machine via het netwerk. Deze data dient beschermd te worden, aangezien men al heeft aangetoond virtuele machines in transitie over het netwerk on-the-fly te kunnen wijzigen.
Virtualisatieproducten zijn op dit moment alle leveranciersgebonden. Er is nog geen universele standaard, waardoor de producten onderling niet compatibel zijn en de afnemer na de eerste investering in beginsel gebonden is aan een bepaalde leverancier.
Door de introductie van de virtualisatielaag wordt een nieuw object van beheer gecreëerd. De meeste beschikbare beheertools verschaffen de beheerders onbeperkt toegang tot alle VM's met bijbehorende inhoud en dus data. Aandacht dient te worden besteed aan de beheerbevoegdheden met betrekking tot de fysieke host server, de virtualisatielaag met bijbehorende VM's en het guest-besturingssysteem met de bijbehorende applicatie, door functiescheiding toe te passen.
Virtualisatie is een handig hulpmiddel, maar is niet voor alle toepassingen geschikt. Applicaties die een hoge *performance* moeten leveren, zijn niet geschikt om op virtuele machines te installeren. Het gaat hierbij om database managementsystemen en e-mail servers. Deze servers dienen veel I/O-aanvragen tegelijk te verwerken en benutten daarbij de volledige servercapaciteit. Het delen van die capaciteit over meerdere virtuele servers kan in deze situatie beperkend werken voor de performance. Met capaciteit wordt hier bedoeld de harde schijf, de CPU en het interne geheugen.
Nog een aandachtspunt is de zogenoemde *Single Point of Failure*. Dit betekent dat een systeem op een enkel punt zodanig kwetsbaar is, dat een defect gevolgen kan hebben voor de beschikbaarheid. Door meerdere fysieke servers te consolideren op één fysieke server heeft een hardwaredefect invloed op alle daarop geïnstalleerde virtuele servers. Dit probleem kan worden opgelost door gebruik te maken van redundante systemen. Hierbij worden op extra fysieke servers redundant meerdere virtuele servers geïnstalleerd.
Sommige licenties worden per CPU uitgegeven. Virtuele machines maken in principe gebruik van dezelfde CPU, terwijl de licenties meerdere malen gebruikt worden. Het is niet duidelijk wat de juridisch mogelijkheden en gevolgen hiervan zijn. Om boetes en imagoschade te voorkomen is het wel van belang dat organisaties hier rekening mee houden en dit laten uitzoeken.

IMPACT VAN VIRTUALISATIE OP ITIL-PROCESSEN

Zoals vermeld werd aan het begin van het artikel, heeft het gebruik van virtualisatie invloed op IT-processen [ITSM06]. Om de lezer een idee te geven welke invloed virtualisatie kan hebben op de IT-processen is tabel 1 opgesteld.

CONCLUSIE

Servervirtualisatie is geen nieuwe uitvinding. In feite komt het neer op het beter benutten van hardware resources, met als gevolg minder gebruik van hardware en dus ook minder kosten. Deze bekende techniek – een soort capaciteits*multiplexing* – is de laatste jaren populair geworden vanwege de bruikbaarheid op 'goedkope' *midrange* servers. In de traditionele situatie zonder toepassing van virtualisatie, wordt over het algemeen de fysieke servercapaciteit niet optimaal benut. Door de toepassing van virtualisatie kan het overschot aan capaciteit bij de fysieke servers over het algemeen beter worden benut.
Er worden nieuwe risico's geïntroduceerd door de hoofdkenmerken van virtualisatie, in de vorm van serverconsolidatie en servers die zijn opgeslagen als bestand. Bij virtualisatie draait immers elke virtuele machine op een stuk virtualisatieprogrammatuur en elke virtuele machine wordt als een bestand opgeslagen. Hierdoor is een virtuele machine net zo kwetsbaar als andere softwareprogrammatuur c.q. -bestanden. Dit betekent dat de virtualisatielaag kwetsbaar is voor hackers. Verder zijn de bestanden portable, gemakkelijk aan te passen, te kopiëren en te bewerken.
Omdat het doel is om capaciteit beter te benutten, is het van belang een goede capaciteitsplanning te hebben. Ook de portabiliteit en bewerkbaarheid van virtuele servers is een punt van aandacht. Een strak Configuratie- en Change Management is van essentieel belang om de exclusiviteit en integriteit van data te waarborgen. ■

Literatuur

[COMP01] Computer Economics, *IBM Mainframe Partioning:LPAR vs. VM Function and Efficiency,* www.compecon.com, 2001.
[CREA81] Creasy, R.J., *The Origin of the VM/370 Time Sharing System*, IBM, 1981.
[FIJN05] Fijneman, R., E. Lindgreen en P. Veltman, *Grondslagen IT-auditing,* Academic Service, 2005.
[ITSM06] ITSMF-NL, *Foundations of IT Service Management op basis van ITIL*, Van Haren publishing, 2006.
[MARS06] Marshall, D., W.A. Reynolds en D. McCrory, *Advanced Server Virtualization*, Auerbach Publications, 2006.
[OGLE05] Oglesby, R. en S. Herold, *VMware ESX Server: Advanced Technical Design Guide*, Brian Madden, 2005.
[OTEY06] Otey, M., *Virtualization Technologies,* Windows IT Pro, Penton Publication, 2006.
[PULT06] Pultz, J.E. en D. Scott, *IT Infrastructure and Operations,* Gartner, 2006.
[RECH06] Rechter, B., *Virtualisatie en IT-audit*, EDP Auditor, jaargang 14, Reed Business Information bv, 2005.
[RUTK07] Rutkowska, J., *Virtualization: the other side of the coin*, presentatie NLUUG Virtualisatie voorjaarsconferentie, 10 mei, 2007.
[VMWA05-1] VMware, *Reducing Server Total Cost of Ownership with VMware Virtualization Software*, www.VMware.com, 2006.
[VMWA05-2] VMware, *Making your business disaster ready with virtual infrastructure*, www.VMware.com, 2004.
[VMWA05-3] VMware, *Accelerate Application Development, Testing and Deployment with VMware Software*, www.VMware.com, 2005.
[WOLF05] Wolf, C. en E.M. Halter, *Virtualization: from the desktop to the enterprise*, Apress, 2005.

ir. M.J. (Angelo) Montero RE is sinds 1 maart 2009 werkzaam bij de Rijksauditdienst. Daarvoor werkte hij bij de EDP Audit Pool als IT-auditor. Het artikel is gebaseerd op de afstudeerscriptie van de auteur in het kader van de afronding van de IT-auditopleiding aan de Vrije Universiteit in Amsterdam. Dit artikel is op persoonlijke titel geschreven.