IT-BEHEEROPLOSSING: SOFTWARE OF HARDWARE?

De huidige trend van IT-outsourcing illustreert dat veel organisaties in toenemende mate worstelen met het operationele beheer van hun automatiseringsinfrastructuur. De praktijk wijst uit dat puur het uitbesteden van het beheer de problematiek niet in zijn geheel oplost.

EVA POTAPPEL

Je kunt geen vakblad openslaan of er staat wel een artikel in over de zegeningen van outsourcing. Het lijkt allemaal heel betrouwbaar. De verantwoordelijkheden van beide partijen, uitbesteder en service-provider, worden vastgelegd in een SLA (Service Level Agreement). Maar dragen de vele varianten van outsourcing wel bij aan het verminderen van de zorgen om IT-beheer? Op het moment dat haar reputatie wordt aangetast, als gevolg van niet werkende geldautomaten door netwerk-problemen, heeft een bankinstelling weinig aan de boeteclausule in een SLA. Die zal ongetwijfeld bepalingen bevatten die de nadruk leggen op het voorkomen van het falen. Maar hoe kan gemeten worden dat beide partijen daadwerkelijk de afspraken nakomen? Met andere woorden: hoe kan IT-infrastructuurbeheer in de praktijk worden uitgevoerd?

Monitoring van IT

In het computertijdperk waarin wij leven, kunnen mensen zich steeds minder een wereld voorstellen zonder computers. Elke minuut dat een e-mailserver niet functioneert of het netwerk down is, kost vele euro's. Omzetverlies, verloren manuren en de verdere gevolgen in de keten zijn slechts een paar voorbeelden hoe onderzoeksbureaus tot schrikbarende kostencalculaties komen. Daarnaast dreigen dagelijks virussen, spyware, hackers en andere bedreigingen steeds vaker een ramp te veroorzaken. Meer dan ooit is IT-beheer nodig. Ook overheden zijn bezorgd over de grote risico's die de samenleving loopt met complexe bedrijfsprocessen, waarvan de meeste zwaar leunen op ICT-voorzieningen. Zij proberen de risico's te beperken door compliance wet- en regelgeving op te stellen (Sarbanes-Oxley Act, Basel II, HIPAA, et cetera). Maar hoe kan de naleving hiervan worden bewezen en vastgelegd? Het antwoord op deze vraag is ironisch genoeg: nog meer IT-hulpmiddelen!

Een platte pizzaoos herbergt alle elektronica en software om als een thermometer op elk gewenst moment de prestaties van de IT-infrastructuur te meten en te kijken of de beveiliging volstaat.

Op mainframe-architecturen gebaseerde software vormt de basis van het IT-beheer, zowel bij organisaties met een eigen IT-afdeling als bij MSP's (Managed Service Providers). Deze softwareoplossingen zijn meestal duur (licenties, updates), de implementatieperiode is lang (inclusief het installeren van agents) en ze vragen goed getrainde gebruikers.

Een goed en betaalbaar alternatief van softwareoplossingen zijn monitoring hardware-faciliteiten. Enkele fabrikanten hebben monitoringtoepassingen ontwikkeld die systeembeheer, kwetsbaarheidsmeting, opsporen van indringers, beheer van systeembronnen, netwerkbeheer en netwerkanalyse in één box integreren. Bovendien worden, met één druk op de knop, rapporten en loggegevens gegenereerd. Deze functionaliteit is uiterst nuttig voor het stroomlijnen van intern organisatiemanagement en accountingprocedures. In tegenstelling tot de meeste softwareoplossingen vereist deze hardwareoplossing geen installatie van (software)agents op servers en werkplekken, wat de installatie en het beheer ervan vereenvoudigt. Er zijn bovendien geen extra investeringen nodig voor de training van IT-personeel. Net als bij access & control hardwareoplossingen, kan - door het bouwsteenprincipe - extra apparatuur worden toegevoegd. Er wordt dus rekening gehouden met de behoefte aan schaalbaarheid.

De monitoring 'appliance' kan zeer goed stand-alone functioneren. Het kan ondernemingen ondersteunen in het voldoen aan best practices zoals ITIL (IT Infrastructure Library), het voldoen aan (IT) compliance regelgeving en het genereren van 'network traffic' rapporten. Deze laatstgenoemde rapporten kunnen uitermate geschikt zijn voor prestatiemetingen van SLA's. De combinatie van een IT-beheeroplossing voor access & control en monitoring maakt IT-beheer tot één geheel. Immers, wanneer een incident geconstateerd is, kan het probleem direct

verholpen worden en zijn soortgelijke problemen in de toekomst te voorkomen.

Het is een monitoringbox die een uitkomst kan zijn voor zowel organisaties die zich willen ontdoen van een gespecialiseerde IT-staf en afdelingen van bedrijven die nog niet over een monitoringoplossing beschikken. Voorbeelden hiervan zijn HP Openview, IBM Tivoli en CA Unicenter.

Ook Service providers en MSP's verrichten hun diensten graag zo efficiënt mogelijk. Het maakt geen verschil of IT-processen en/of beheerdiensten zijn uitbesteed. Zowel MSP als de uitbestedende partij kan over een monitoring functionaliteit beschikken. Op deze wijze hebben beide partijen de beschikking over gedetailleerde informatie over de IT-infrastructuur, de actuele processen en de beveiliging daarvan.

Een hardwareoplossing is kostenefficiënt en gemakkelijk in het gebruik. Het is een uitstekend en objectief instrument voor het controleren op de naleving van SLA-bepalingen en compliance regelgevingen, omdat het feitelijk correcte informatie genereert over de status van de IT-infrastructuur. Het IT-beheer wordt door deze monitoring faciliteit dermate vereenvoudigd dat de IT niet langer een kostenpost is, maar bijdraagt aan de winstgevendheid van organisaties. •

eva@raritan.com (010 284 40 53)
www.raritan.com