Steeds vaker gaan bedrijven samenwerkingsverbanden aan met andere bedrijven. Vaak is het dan nodig om de ICT-systemen van de partners op elkaar aan te sluiten zodat er electronische berichten van de ene organisatie naar de andere gestuurd kunnen worden. Wanneer er geen sprake is van een bedrijfsnetwerk zijn er situaties waarin het noodzakelijk is de systemen op een veilige en betrouwbare wijze via het internet te koppelen. Dit kan worden bewerkstelligd door twee Microsoft-producten in te zetten: Biztalk 2002 en Exchange 2000. Dit artikel gaat wat dieper in op de integratieproblematiek en een mogelijke oplossing hiervoor.

thema

Koppeling van stand-alone systemen

Integratie met Biztalk en Exchange

Een probleem bij het koppelen van verschillende systemen van de verschillende organisatie is de incompatibiliteit van de systemen onderling: ze gebruiken bijvoorbeeld niet hetzelfde protocol, of de systemen kunnen slechts een exportdump maken naar een ASCII bestand. Dit wordt vaak veroorzaakt doordat er in het verleden bij de ontwikkeling van een systeem geen rekening is gehouden met bestaande standaarden. Een bekende organisatie die standaarden ontwikkeld en bewaakt is het W3C consortium (http://www.w3c.org). De eXtended Markup Language (XML) standaard is hier een duidelijk voorbeeld van. XML werd, na de ontwikkeling ervan, door het World Wide Web Consortium (W3C) tot standaard verheven. Op dit moment is XML een de facto standaard voor het uitwisselen van gegevens. Bijna alle versies van Microsoft serverproducten die de laatste twee jaar zijn op de markt zijn verschenen voldoen aan deze standaard. Ook het .NET framework van Microsoft is volledig op XML gebaseerd.

BIZTALK EN EXCHANGE Er zijn op het moment van schrijven een aantal softwareleveranciers die producten als berichtenmakelaars, of in het Engels 'message brokers', leveren. Deze zorgen er voor dat systemen die incompatibel zijn en dus geen berichten aan elkaar kunnen sturen, dat met een dergelijk (server)product wel kunnen. Biztalk Server is het antwoord van Microsoft. Exchange is een voor velen bekend product dat al een lange geschiedenis heeft. In de basis is Exchange een mailserver. Daarnaast zijn er in de loop van de tijd veel meer functies aan toegevoegd, waar in dit artikel niet verder op in wordt gegaan. In onderstaande uiteenzetting wordt er alleen gebruik gemaakt van de mailserver-functionaliteit van dit product.

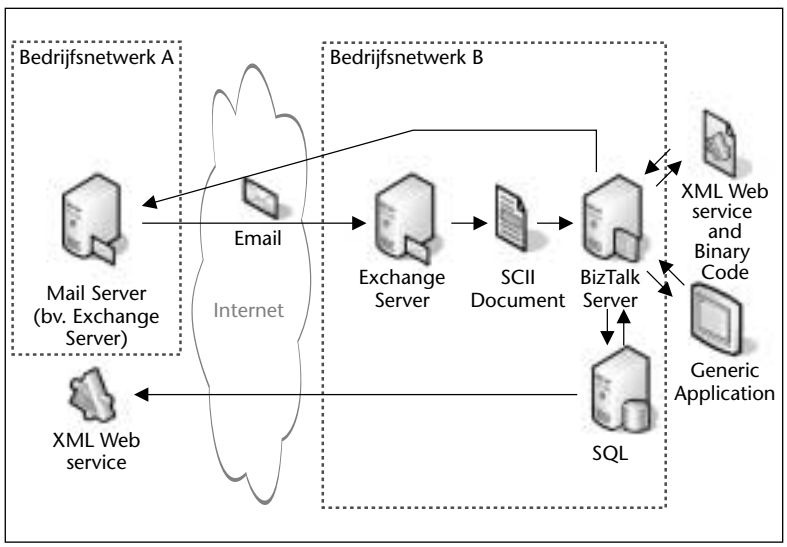
BERICHTENVERKEER Om systemen met elkaar te kunnen koppelen is het een voorwaarde dat Biztalk toegang heeft tot die systemen. Dit kan op een aantal manieren, waaronder op fileniveau via een UNC (*Universal / Uniform Naming Convention, te herkennen aan de volgende vorm \\server\share*), en via het HTTP (*Hypertext Transport Protocol*) en een URL (*Uniform Resource Locator; een internetadres, bijvoorbeeld http://www.mycompany.com*). Biztalk ondersteunt meer mogelijkheden voor uitwisseling van informatie (waaronder SOAP, SMTP, MSMQ, Web Services) maar die worden hier buiten beschouwing gehouden. Maar ook als Biztalk geen directe koppeling heeft met het te koppelen systeem is dit op te lossen. Dit kan het geval zijn wanneer er geen sprake is van een gedeeld (Windows)-netwerk of een extranet waarover in een afgesloten omgeving berichten uitgewisseld kunnen worden.

Een manier om dit op te lossen is door gebruik te maken van Microsoft Exchange om van het ene netwerk naar het andere e-mails te sturen met daarin de over te zenden berichten. Een bericht wordt verzonden van de initiator naar de mailserver op het bedrijfsnet-

werk waar Biztalk server staat (in de afbeelding bedrijfsnetwerk B). Een Exchange agent kan de inhoud van het e-mailbericht uit het bericht halen en dit in een ASCII bestand zetten en dit ASCII bestand vervolgens weer in een zogenaamde polling map plaatsen. Biztalk pollt deze map continue, en wanneer hier een bestand wordt geplaatst, gaat Biztalk dit bericht verwerken.

DOCUMENT DEFINITIES Voor de verwerking van berichten binnen Biztalk, wordt gebruik gemaakt van XML. Om die reden is het noodzakelijk dat niet-XML berichten die Biztalk binnenkomen eerst geconverteerd worden naar XML. Biztalk maakt gebruik van zogenaamde documentdefinities om deze conversie uit te voeren. Een documentdefinitie in Biztalk kan worden vergeleken met een XML-schema. Een XML-schema is een blauwdruk voor een XML-document en vastgelegd door het W3C. Ze beschrijft welke informatie in een XML-document gespecificeerd moet zijn en bepaalt tevens de structuur van de informatie. Ook wordt hierin vastgelegd welke informatie verplicht en welke optioneel is. Ook in een document definitie in Biztalk zijn deze zaken vastgelegd.

Om aan de documentdefinitie te voldoen is het dus noodzakelijk dat een niet-XML bericht, bijvoorbeeld een tekstbestand, uniform is. Alleen op die manier is het mogelijk de inhoud van het tekstbestand met een documentdefinitie om te zetten naar een XML-bericht waar Biztalk mee gaat werken. Is het formaat van het e-mailbericht niet uniform, dan voldoet het bericht niet aan de gedefinieerde document definitie en het gevolg hiervan is dat het bericht niet te verwerken is. Deze berichten komen in een verzamelbak terecht, de zogenaamde *suspended queue*. Er kan worden geanalyseerd wat de oorzaak is, en zo nodig kan er actie worden ondernomen om het bericht alsnog aan de specificaties te laten voldoen. Het bericht kan hierna wederom aan Biztalk worden aangeboden voor verwerking.



FIGUUR 1

AUTHENTICATIE Aangezien de e-mails in bovenstaand verhaal over een "open" internet verbinding worden verstuurd is authenticatie nog belangrijker dan in een gesloten netwerkomgeving. Het is van vitaal belang te weten wie de afzender van de berichten is. Daarbij moet de betreffende afzender ook rechten hebben om berichten te sturen die door de Biztalk server verwerkt moeten gaan worden. Er zijn verschillende manieren om te zorgen voor:

1. *Digitale ondertekening van de e-mails*
   Door e-mail digitaal te ondertekenen kan de herkomst van het bericht worden verzekerd. Een digitale handtekening bestaat uit een digitaal certificaat dat door een zogenaamde onafhankelijke certificeringinstantie. Uit het certificaat blijkt de identiteit van de persoon aan wie het certificaat is uitgegeven. Door dit certificaat aan de e-mail te "hangen" wordt het bericht ondertekend, en kan de ontvanger van het bericht de herkomst verifiëren.
2. *Encryptie van de e-mails*
   Door de berichten te encrypten wordt het voor alle personen of systemen, behalve voor de geadresseerde zeer moeilijk om het bericht te lezen. Degene aan wie het bericht wordt geadresseerd genereert een sleutelpaar, bestaande uit een private key en een public key. De public key wordt gedistribueerd naar alle partijen die een geëncrypt bericht willen sturen; de e-mail wordt met behulp van deze sleutel vergrendeld. Nadat de e-mail bij de geadresseerde is aangekomen kan deze met behulp van de private key het bericht decrypten, en zo het oorspronkelijke bericht terughalen. Het is zeer belangrijk dat de private key dus niet uit handen wordt gegeven.
3. *Exchange configuratie*
   Exchange kan zodanig geconfigureerd worden dat alleen e-mails die afkomstig zijn van aangegeven SMTP-servers worden geaccepteerd. Op die manier worden e-mails die niet via "vertrouwde" SMTP-server verstuurd zijn, geweerd, en dus wordt de inhoud van die berichten niet verwerkt.
4. *Netwerkconfiguratie*
   Naar analogie van de Exchange configuratie kan ook het netwerk zodanig worden aangepast dat communicatie over een bepaalde configuratiepoort alleen wordt toegestaan als dit van een vertrouwd netwerkadres afkomstig is.

Vaak wordt een aantal beveiligingsmogelijkheden tegelijk gebruikt omdat geen van de manieren afzonderlijk voldoende veiligheid biedt. Afhankelijk van de betrouwbaarheid en gevoeligheid van de te versturen informatie zal een afweging moeten worden gemaakt of

en welke maatregelen worden genomen. Natuurlijk zullen hierbij andere factoren, zoals ontwikkelingstijd en budget, ook een rol spelen.

De praktijk Veel overheidsinstellingen, zoals ministeries en gemeenten, hebben client-server maatwerkapplicaties draaien. Aangezien veel van de taken van bijvoorbeeld een ministerie zeer specifiek zijn, kunnen de gebruikte applicaties hiervoor niet op de markt gekocht worden. Om die reden zijn ze speciaal voor die organisaties gemaakt. Omdat de 'elektronische overheid' nog niet zo lang een gemeen gedachtegoed is werd er tijdens de bouw dan ook geen rekening gehouden met het feit dat deze toepassingen met andere toepassingen van een andere instelling moet kunnen communiceren. Met andere woorden: deze systemen zijn niet compatibel. Veel van deze instellingen hebben bepaalde informatie over burgers, waarvan het makkelijk is als die informatie wordt gedeeld. Doordat de systemen niet compatibel zijn is het delen van die informatie geen eenvoudige zaak. Daarbij komt dat de netwerken van de verschillende instellingen onderling veelal niet met elkaar in verbinding staan. De enige verbinding die voorradig is, is doorgaans een internetverbinding: HTTP is alom vertegenwoordigd en bijna elke pc en server heeft de mogelijkheid een internetverbinding te maken.

Het tijdperk van puur en alleen HTML aanbieden via het internet is voorbij: met de huidige beschikbare (.NET) technologie voor internetapplicaties en webservices is het zeer goed mogelijk om bedrijfsprocessen tussen de verschillende organisaties te koppelen met het internet als medium. En dus om een workflow van de ene overheidsinstelling elektronisch naadloos aan te sluiten op de workflow van een andere instelling. Kortom, de systemen moeten daadwerkelijk worden gekoppeld. Nog niet zo lang geleden kon dit in een aantal gevallen worden opgelost door het gebruik van diskettes die informatie, geïmporteerd uit het ene systeem, konden overbrengen naar het andere systeem. Maar nu bijna alle ministeries en gemeenten een continue internetverbinding hebben, en de hoeveelheid informatie die van het ene naar het andere ministerie getransporteerd moet worden in de afgelopen tijd sterk is toegenomen, blijkt dat dit geen werkbare oplossing meer is. Nee, informatie moet direct vanuit het ene systeem naar het andere systeem 'geschoten' kunnen worden zonder enige vorm van human interaction.

Een zeer groot deel van de informatie die digitaal tussen de verschillende organisaties wordt verstuurd (zonder gebruik te maken van media als diskettes en cdroms) wordt getransporteerd in e-mail. Hier kan dan ook handig gebruik van worden gemaakt bij het koppelen van systemen. Er moet voor worden verzorgd dat elk te koppelen systeem de informatie die gedeeld moet worden met andere organisaties "af wordt gegeven" aan de mailserver (Exchange) op het eigen bedrijfsnetwerk. Nadat het bericht digitaal ondertekend en eventueel versleuteld is, wordt het als een e-mail naar Exchange van de andere organisatie die naast de mailserver een berichtenmakelaar (Biztalk)op het bedrijfsnetwerk heeft. Het bericht wordt vanuit de mail server aan Biztalk gegeven, waarna Biztalk de distributie naar de andere systemen voor zijn rekening neemt. Nadat alle transacties zijn gedaan, kan er een melding - via e-mail - terug naar de bronorganisatie met een terugkoppeling.

In bovenstaande case wordt ervan uitgegaan dat de informatie wordt gedeeld tussen twee organisaties. Echter, met Biztalk als broker kan er een veelheid aan partijen en hun worden gekoppeld. Hierbij is Biztalk de linking pin bij de verwerking van de berichten. Exchange neemt hierbij de versturing van de berichten voor zijn rekening neemt wanneer er slechts een open netwerk aanwezig is.

Conclusie Een voordeel van de aangeboden oplossing is dat de bestaande systemen niet omgebouwd behoeven te worden om met XML om te kunnen gaan. De informatie die uit deze systemen wordt geëxporteerd - bijvoorbeeld in ASCII formaat - kan in Biztalk met behulp van een documentdefinitie worden omgezet in XML en vice versa. Hierdoor kan deze informatie op eenvoudige wijze met andere systemen worden gedeeld. Een tweede voordeel is het feit dat het versturen van de informatie zeer eenvoudig te bewerkstelligen is. E-mail is immers een van de meest gebruikte toepassingen op het internet. Omdat het versturen van de informatie over het "onveilige" internet geschiedt is het wel noodzakelijk om de nodige aandacht te besteden aan de zekerstelling van de herkomst van het bericht en eventueel de inhoudelijke vertrouwelijkheid.

Bronnen

http://www.microsoft.com/biztalk/
http://www.microsoft.com/exchange/
http://www.w3c.org/

Dennis Ham is werkzaam bij de practice Warp11 Next Generation van Cap Gemini Ernst & Young als Senior Consultant (e-mail: dennis.ham@cgey.nl).