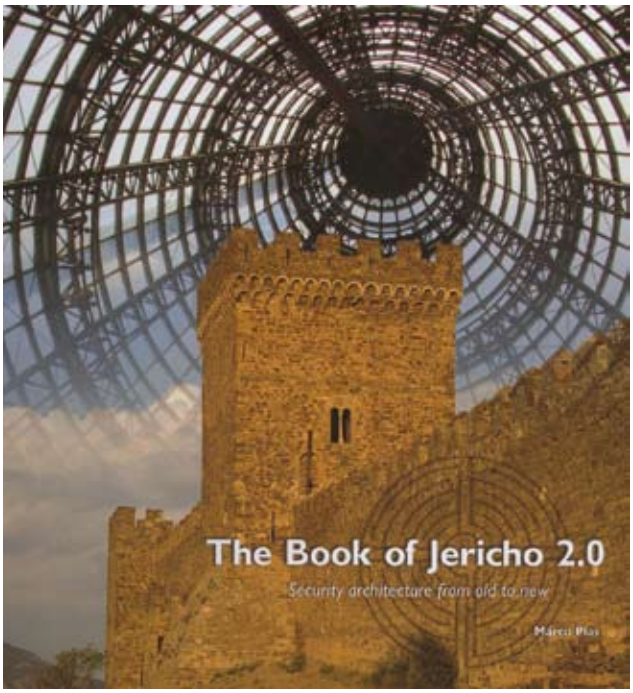
JERICHO-CONCEPT STAAT CENTRAAL

Business continuity schreeuwt om ketenbenadering

In de huidige context van marktturbulentie en razendsnelle technologische ontwikkelingen is het steeds belangrijker dat de juiste informatie, op de juiste plek en op de juiste tijd voorhanden is. Sterker nog, het is een noodzakelijke voorwaarde om als bedrijf te kunnen overleven.

Door John Schmeitz

Informatie dient veilig te zijn, wat steeds lastiger wordt, gezien de wens en noodzaak om steeds vaker in ketens samen te werken. Deels is beveiliging een technologisch probleem, maar het is tevens een organisatorisch issue, dat ook buiten de bedrijfsgrenzen nadrukkelijk zijn uitwerking heeft. In dit artikel behandel ik een aantal aandachtspunten voor business continuity. Hoe kan ik als bedrijf of keten overleven in een turbulente markt? En hoe belangrijk is een integrale benadering van organisatie, proces en technologie voor het waarborgen van business continuity?



Veranderde businessmodellen

Er komen steeds meer ketens. Ook de voorspelde groei van outsourcing, ongeveer 8,1 procent dit jaar, draagt zijn steentje daaraan bij. Verder veranderen in de markt de businessmodellen door internettoepassingen en nieuwe technologische mogelijkheden. Enerzijds kunnen ketens kleiner worden door on-demand diensten te gebruiken, die onder controle staan van de contenteigenaar. Denk bijvoorbeeld aan een auteur of muzikant, die zijn content direct in de markt wil zetten. Anderzijds wordt een totaalproduct steeds vaker geleverd door een keten van leveranciers en dienstverleners, die van elkaar afhankelijk zijn en bedrijfsoverschrijdende informatie nodig hebben om adequaat te kunnen reageren. Een goed voorbeeld hiervan is de gezondheidszorg. Samenwerking tussen onder andere ziekenhuizen, zorginstellingen, verzekeraars, thuiszorgorganisaties, huisartsen en apothekers is onontbeerlijk. Hierbij hoort ook informatie-uitwisseling, die via het landelijk schakelpunt van NICTIZ, het Nationaal ICT Instituut in de Zorg, moet gaan lopen. Om de keten goed te laten functioneren, zijn duidelijke afspraken nodig over gedragsregels, processen en procedures. Daarom stelt NICTIZ onder andere de NEN7510 verplicht om aan te mogen sluiten op het schakelpunt. NEN7510 gaat vooral over de procesinvulling die nodig is voor validatie en beveiliging van informatie. Zoals zo vaak is de mens de zwakste schakel in de beveiligingsketen. Voorbeelden zijn er legio. Het verdwijnen van informatie via een verloren USB-stick, of de aan de straat gezette PC van officier van justitie Tonino, het zijn slechts enkele voorbeelden. Vaak gebeurt het lekken van vertrouwelijke informatie onbewust. Uit onderzoek van onder andere Security.nl blijkt dat 23 procent van de managers het eigen personeel ziet als de grootste bedreiging. Van de managers geeft zelfs 16 procent aan dat het wel eens is voorgekomen. Niet alleen de Engelse Belastingdienst, ook het kantoorpersoneel in het Verenigd Koninkrijk verliest op grote schaal vertrouwelijke informatie van klanten, leveranciers, collega's en financiële gegevens. Meer dan een miljoen Engelsen zijn hun laptop, PDA, USB-stick, cd of diskettes met vertrouwelijke gegevens wel eens kwijtgeraakt en twaalf procent van alle mensen zegt dat dit een collega is overkomen. Inmiddels heeft 17 procent van al het personeel een laptop van de zaak en is thuiswerken al lang geen trend meer, maar een vast gegeven. Toch gebruikt slechts 25 procent van alle thuiswerkers encryptie om informatie te beschermen. Verder gebruiken meer dan 11 miljoen Engelsen een PDA, USB-stick of cd om ge-

John Schmeitz *(john@schmeitz-advies.nl) is onafhankelijk organisatiedeskundige telecom en gespecialiseerd in (telecom)strategie, (interim)procesmaßnagement en mobiliteitsconcepten.*

gevens mee naar huis te nemen. Volgens de onderzoekers moeten bedrijven duidelijk naar het personeel communiceren welke informatie wel en niet op laptops en ander apparaten thuishoort. Een ander aspect is dat informatiewerkers afhankelijk zijn van informatie en indien de ICT-afdeling uit beveiligingsoogpunt op de rem trapt, dan zijn ze vaak heel creatief en gaan ze hun eigen koers varen om toch toegang tot de benodigde informatie te krijgen. Het spreekt voor zich dat zo nauwelijks controle en gestructureerde beveiliging mogelijk is.

Open architectuur

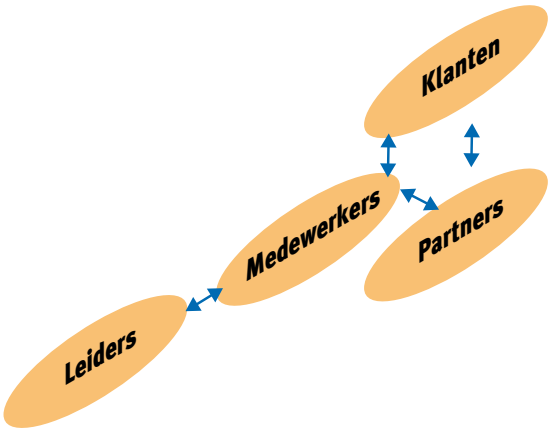
De noodzaak van open architectuur neemt toe. Het is steeds belangrijker geworden om open te zijn; zelfs Microsoft is recent tot dit inzicht gekomen. Een open architectuur heeft zowel een technische als een organisatorische component. Allereerst is er een andere organisatorische samenhang in de keten, waarbij het niet alleen om de directe schakels in de keten gaat, maar om de totale set van verbindingen. Marco Plas, security domain leader bij Cap Gemini, heeft dit in zijn boek: *The Book of Jericho 2.0* beschreven. Volgens hem zijn er vier soorten relaties in de waardeketen, namelijk die tussen de organisatieleiders en medewerkers, medewerkers en klanten, leiders en partners en de relatie tussen partners en klanten. Dit wordt het ecosysteem genoemd waar de business plaatsvindt (zie figuur 1).

De nieuwe slag om Jericho

De nieuwe businessmodellen en de noodzaak samen te werken in ketens vragen om een totaal andere aanpak van technische beveiliging. Tot nu toe beveiligden bedrijven zich door dikke muren in de vorm van firewalls aan te leggen rondom hun bedrijfsnetwerk. Dit bemoeilijkt echter de uitwisseling van informatie tussen ketenpartners. Een oplossing is om VPN-tunnels te graven onder de muren, maar dat verlangt wel het nodige beheer en is een potentieel gevaar voor de beveiliging. Wat doe je als de 140.000 medewerkers van Philips wereldwijd informatie met elkaar en met 400.000 ketenpartners gaan uitwisselen? De traditionele manier om te beveiligen met firewalls en VPN's is dan op zijn zachtst

Driekwart van de beroepsbevolking in de VS werkt straks draadloos

gezegd onhandig. Philips heeft er daarom voor gekozen om de kleinste groep, de eigen medewerkers, samen te voegen met de grootste groep, de ketenpartners, op basis van internettechnologie. De nieuwe situatie vraagt dus om een mechanisme die geen dikke muren om het eigen bedrijfsnetwerk bouwt, maar ze juist afbreekt. In dat licht moet de oprichting van de *The Open Group* binnen



Figuur 1. Het ecosysteem van de waardeketen.

het *Jericho Forum* worden gezien, die bestaat uit veiligheidsdeskundigen van belangrijke organisaties wereldwijd. Hun doel is *network deperimeterazation* tot stand te brengen op basis van open standaarden, door gebruik te maken van het open karakter van internet. De naam Jericho slaat op de onneembare muren uit het bijbelse verhaal, waarin God het volk Israël door de Rode Zee leidde en de muren van Jericho liet omvallen. De poorten van Jericho werden zorgvuldig gesloten gehouden, omdat de inwoners bang waren voor de Israëlieten; niemand mocht naar binnen of naar buiten. Het leger moest zeven dagen lang met veel lawaai om de stad heen trekken, waardoor de muren van Jericho uiteindelijk instorten.

Veiligheid van gegevens

Een maatschappelijk probleem is de publieke veiligheid die het noodzakelijk maakt dat de diverse overheidsinstanties samenwerken. In dit verband is communicatie cruciaal voor die samenwerking en is er een totaal andere manier van samenwerking nodig en dus ook technische ondersteuning. Communicatie is niet alleen van belang tijdens een ramp, maar juist ook bedoeld om rampen en terroristische daden te voorkomen. Daartoe moet informatie worden uitgewisseld, en analyses worden gemaakt op basis van patroonherkenning, waarbij persoonsgegevens worden uitgewisseld. Dat hierbij goed moet worden opgelet dat de privacy gewaarborgd blijft, spreekt voor zich, maar is niet simpel en soms zelf niet mogelijk. Om persoonsgegevens te beschermen, zijn allerlei beveiligingsmechanismen ontworpen, maar steeds vaker zijn er meldingen dat de beveiliging gekraakt is, zodat op naam én op kosten van een ander, diensten kunnen worden afgenomen. Hoe sterk de beveiliging is, blijkt in de praktijk vaak af te hangen van het kostenplaatje. Een voorbeeld is de OV-chipkaart op basis van 48 bits encryptie, ontworpen door NXP en geleverd door Trans Link. Uit kostenoverwegingen is er door de opdrachtgever waarschijnlijk niet gekozen voor een sterkere beveiliging. Nu staat het hele concept ter discussie, aangezien er te grote beveiligingsrisico's zouden zijn. Met andere woorden: de business continuity zou in gevaar komen. De reputatieschade is er niet alleen voor de leverancier, maar voor de hele keten en wellicht dat soortgelijke concepten in de toekomst met de nodige argusogen zullen worden bekeken. Alles heeft te maken met vertrouwen en goedkoop is duurkoop. Voor business continuity is vertrouwen en het waarborgen daarvan cruciaal. Vertrouwen moet daarom moet in de hele keten gewaarborgd zijn.

De keten van vertrouwen

Er zijn de laatste tijd verschillende ideeën geopperd hoe je goed kunt communiceren, samenwerken en toch de situatie kunt beheersen. De visie van het Jericho Forum is dat iedereen via internet op een open en transparant netwerk is aangesloten. Door nu een vertrouwde partij in de keten op te nemen, die alle diensten met elkaar verbindt, kan op vertrouwensbasis informatie worden uitgewisseld en kunnen ook transacties worden uitgevoerd. Hiervoor is een standaard nodig op basis waarvan gebruikers kunnen worden geïdentificeerd. *Identity Federation* is in dit verband een verzamelterm voor alle processen, standaarden en technologieën die het mogelijk maken om op een gecontroleerde ma-

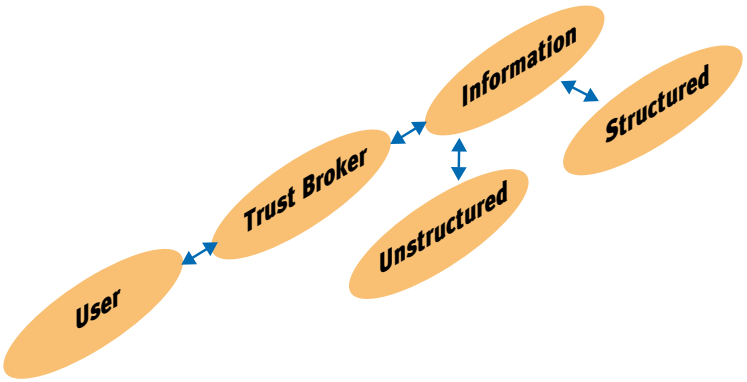
nier identiteitgegevens uit te wisselen over organisatiegrenzen heen. Identity Federation is opgesteld door The Liberty Alliance en wordt verder uitgewerkt in het zogenoemde Circles of Trust-model van Jericho (zie figuur 2).

In het Jericho-concept gaat het vooral om het beveiligen van de informatie en niet van het netwerk. Hierdoor is het internet eveneens als netwerk te gebruiken. Door de technologische ontwikkelingen in de telecommunicatie is internettoegang voor iedereen mogelijk. Het aantal mobiele werkers wereldwijd klimt bijvoorbeeld naar 1 miljard en driekwart van de beroepsbevolking in de VS is straks draadloos. Doordat de informatie door bijvoorbeeld end-to-end encryptie wordt beveiligd, ontstaat er een grote vrijheid, niet alleen in soorten accessmethoden en apparatuur, maar ook in samenwerkingsverbanden. En daar was het allemaal om begonnen. Voor het probleem van de ongebreidelde stroom van ongestructureerde data is, moet nog wel een oplossing worden gezocht. Denk bijvoorbeeld aan het versturen van een e-mail met bijlage. De bijlage staat dan meestal op de lokale PC van de zender, bij sent items in het mailprogramma, op de mailserver, bij de ontvanger in de mailbox en vaak wordt ook nog een kopie lokaal op de PC van de ontvanger gezet. Er bestaan dus vijf kopieën van hetzelfde bestand. Wie bewaakt nu welke het origineel is en de meeste recente data bevat? Dit probleem zal door processen en procedures, ondersteund door technologie, moeten worden opgelost. De hele structuur staat of valt namelijk niet alleen met de Trust Broker, maar ook met de betrouwbaarheid en validiteit van de informatie en wat hiermee wordt gedaan. De risico's hangen vaak samen met het type informatie, waar acties aan zijn gekoppeld. Maar wat te doen als cruciale informatie via de e-mail wordt verstuurd, terwijl bijvoorbeeld afgelopen Kerst 83 procent van de e-mail spam was? Als daardoor je mailbox volloopt en je een cruciale e-mail mist over het verplaatsen van een meeting van Londen naar Parijs, dan was een andere manier van communiceren waarschijnlijk te prefereren geweest. Dit zijn voornamelijk procesmatige vragen, die echter wel sterk verbonden zijn met de organisatie en de gebruikte technologie.

Niet security van het netwerk staat centraal, maar beveiliging van informatie

Conclusie

Business continuity hangt in de huidige tijd steeds meer af van de waardeketen, die steeds vaker bestaat uit bedrijfsoverschrijdende schakels. Daarbij is overal en altijd toegang tot de juiste informatie cruciaal om te overleven. Dat dit niet meer kan volgens het traditionele concept van bedrijfsnetwerken afgeschermd door firewalls, is duidelijk. Er zal nog veel water door de zee moeten gaan voordat de technische (software)componenten volgens het Jericho-concept alle functies, die nodig zijn, hebben afgedekt. Maar dat het die kant uitgaat, dat is wel duidelijk. In de tussentijd is het voor elk bedrijf noodzakelijk om integraal en kritisch te kijken naar de eigen organisatie, processen en gebruikte technologieën, zodat duidelijk wordt of en hoe transformatie naar een nieuwe samenwerkingstructuur moet worden ingevuld. Het begint met het opstellen van een overall informatie- en telecomstrategie. Pas als de eigen informatie en communicatie betrouwbaar is en kan worden vertrouwd, kunnen derden hiervan eveneens gebruikmaken. Dat geldt bij fusies en bedrijfsovernames in versterkte mate. Alleen dan is er sprake van een beheersbaar proces en kan business continuity worden ingevuld en bewaakt. ■



Figuur 2. Het trust concept volgens Jericho.