Ruimte voor beveiliging en continuïteit

Verslag van een integrale aanpak bij Bouwfonds en Stater

J. Acohen, A.J. de Boer, G. uit de Bosch, C. van Rinsum en E. Roos Lindgreen

Wat komt er in de praktijk bij een integraal beveiligingsproject zoal kijken? Dit verslag besteedt onder meer aandacht aan de projectorganisatie, ervaringen, kritische succesfactoren, bonuspunten en 'lessons learned'.

Inleiding

Voorjaar 1998. Half acht 's ochtends. De financieel directeur van een grote onderneming in het midden van het land komt terecht in een file die er eigenlijk niet hoort te zijn. In de verte, ongeveer ter hoogte van het hoofdkantoor, ziet hij donkere rookwolken, zwaailichten. Even schiet hem door het hoofd: het zou toch niet ... Al snel blijkt dat niet een uitslaande brand in het hoofdkantoor, maar een gekantelde tankwagen op de A28 de oorzaak van de commotie is. De chauffeur is met de schrik vrijgekomen. De directeur begint die dag iets later dan gepland aan zijn eerste meeting. Business as usual. Maar het ongemakkelijke gevoel blijft. Stel dat ... Wat dan?

Het is een goede traditie een artikel over informatiebeveiliging te beginnen met een opmerking over het toenemend belang van informatietechnologie in onze maatschappij en de toenemende afhankelijkheid die hiervan het gevolg is, waarna meestal wordt gemeld dat aan de nieuwe technologische ontwikkelingen niet alleen grote kansen, maar ook risico's verbonden zijn, risico's die op een verantwoorde manier moeten worden beheerst, enzovoort. We leven inderdaad in bijzondere tijden. Nog nooit heeft een technologie zo lang achtereen zo'n consistente verbetering van prijs en prestatie laten zien. Nog nooit is een technologie zo snel en zo geruisloos doorgedrongen tot in de haarvaten van onze samenleving. En nog nooit hebben we aan een nieuwe technologie zoveel economisch en sociaal plezier beleefd. De voorbeelden uit het leven van alledag spreken voor zich.

Al die ontwikkelingen hebben wel verstrekkende gevolgen voor het aandachtsgebied informatiebeveiliging[1]. Aan de ene kant hebben we door de toenemende koppeling van steeds kleinere, snellere en goedkopere componenten te maken met omgevingen die steeds moeilijker te beschermen zijn. Aan de andere kant geeft de nieuwe technologie ons middelen waarmee we de vierde productiefactor juist beter kunnen beschermen dan ooit en waarmee we steeds sneller van onze ervaringen kunnen leren. Kortom: het spel wordt steeds moeilijker, maar de spelers worden steeds beter en hun technieken steeds krachtiger. En wat is een betere manier om het spel onder de knie te krijgen dan te leren van de ervaringen van anderen?

Waarmee we zijn aangekomen bij de inhoud van dit artikel: een beschrijving van het project Beveiliging & Continuïteit, ofwel de wijze waarop Bouwfonds en Stater de afgelopen twee jaar de beveiliging van informatie en informatiesystemen ter hand hebben genomen. De opbouw van het artikel is als volgt. Eerst wordt ingegaan op de belangrijkste kenmerken van Bouwfonds en Stater. Vervolgens wordt de gehanteerde aanpak beschreven en wordt verslag gedaan van het project Beveiliging & Continuïteit, dat in de periode 1998-2000 is uitgevoerd. Daarbij wordt ingegaan op de projectorganisatie, de onderscheiden deelprojecten en de bereikte resultaten. 'Lessons learned' is de titel van een paragraaf die is gewijd aan onze positieve ervaringen, die anderen mogelijk tot voordeel kunnen strekken. Het artikel sluit af met enkele conclusies.

Bouwfonds en Stater

ABN Amro Bouwfonds Nederlandse Gemeenten N.V. (Bouwfonds) is in Nederland één van de grootste partijen op het gebied van de ontwikkeling, de financiering en het management van vastgoed. Het werkterrein strekt zich in toenemende mate uit buiten Nederland. Bouwfonds is georganiseerd in verschillende bedrijfsonderdelen, die zich richten op specifieke kernmarkten van Bouwfonds.

De activiteiten van Bouwfonds spelen zich af op de particuliere en de zakelijke markt. Op de particuliere markt betreft het de ontwikkeling en verkoop van woningen, de verstrekking van woninghypotheken en het beheer van woningen voor derden. Op de zakelijke markt ontwikkelt, financiert en beheert Bouwfonds kantoren en winkelcentra. Bouwfonds heeft ongeveer twaalfhonderd medewerkers, een omzet van *f* 3,8 miljard en een balanstotaal van ruim *f* 29 miljard. Op de Nederlandse onderhandse kapitaalmarkt trekt de onderneming per jaar meer dan *f* 4 miljard aan.

1) Informatiebeveiliging is in dit artikel gedefinieerd als het ontwerpen, invoeren en onderhouden van een stelsel van maatregelen om de kwaliteit van informatie en informatiesystemen te beschermen tegen specifieke dreigingen, waarbij het begrip kwaliteit is uitgewerkt in de aspecten vertrouwelijkheid, integriteit en beschikbaarheid.

In Nederland is Bouwfonds de grootste risicodragende ontwikkelaar van koopwoningen. Zijn marktaandeel in de relevante sector (koop en dure huur) bedraagt ongeveer tien procent. In toenemende mate is sprake van integrale gebiedsontwikkeling en samenwerking met andere marktpartijen.

Ten behoeve van eigenaar-gebruikers en beleggers ontwikkelt Bouwfonds kantoorgebouwen, winkelcentra en bedrijfsgebouwen. Het betreft niet alleen nieuw te ontwikkelen vastgoed, maar ook herontwikkeling van bestaand vastgoed.

Op de markt voor woninghypotheken in Nederland neemt Bouwfonds een vijfde plaats in met een marktaandeel van ongeveer vijf procent. Bouwfonds verkoopt naast eigen hypotheken ook hypotheken voor derden, waardoor een breed assortiment leningsvormen beschikbaar is. Met verzekeraars bestaan samenwerkingsverbanden waarbij Bouwfonds het hypotheekproduct levert en de partner de verzekering. Vastgoed- en financieringskennis wordt ook benut bij de dienstverlening aan fondsen zoals het Nationaal Restauratiefonds en het Nationaal Groenfonds.

In de afgelopen jaren is veel geïnvesteerd in het toepassen van state-of-the-art informatietechnologie bij kredietbeoordeling en portefeuillebeheer. Daarbij zijn zodanige competenties opgebouwd dat Bouwfonds als eerste partij in Nederland het portfoliomanagement als aparte dienstverlening op de markt heeft kunnen brengen.

Hiertoe is in 1997 Stater opgericht, een onafhankelijke dienstverlener in de hypotheekmarkt. Inmiddels is Stater uitgegroeid tot een internationale onderneming met meer dan driehonderd medewerkers, de hoofdvestiging in Amersfoort en een vestiging in Bonn, Duitsland. In het Stater Hypotheek Systeem (SHS) worden meer dan één miljoen hypothecaire leningen beheerd en daarmee is Stater marktleider op dit gebied.

Concernbrede IT-activiteiten zijn ondergebracht binnen de afdeling BITS (Bouwfonds IT Services). Op IT-gebied is binnen Bouwfonds een belangrijke rol weggelegd voor het Platform Informatiebeleid, een concernbreed overlegorgaan voor IT-zaken waarin de directeuren van de belangrijkste werkmaatschappijen vertegenwoordigd zijn.

Van analyse naar beveiligingsplan

Het beveiligingstraject vangt aan in de zomer van 1998, wanneer Bouwfonds een drietal adviesbureaus uitnodigt om hun aanpak toe te lichten en offerte uit te brengen. Na beoordeling van de offertes wordt besloten het traject uit te voeren op basis van het Corporate Information Security-programma van KPMG. Deze eenvoudige 'best practice'-aanpak bestaat uit acht fasen, die achtereenvolgens worden doorlopen (figuur 1).

Het project begint in het najaar van 1998 met het uitvoeren van de fasen 1 tot en met 5. Doel is het uitvoeren van een analyse, het opstellen van een beveiligingsbeleid, het uitvoeren van een self-assessment, een tussentijdse evaluatie en het opstellen van een beveiligingsplan.

Figuur 1. Fasering Corporate Information Security.

Hiertoe wordt een projectgroep geformeerd, die direct rapporteert aan het Platform Informatiebeleid. De projectgroep bestaat uit informatiemanagers uit enkele toonaangevende werkmaatschappijen, vertegenwoordigers van de IT-organisatie, de security manager en een extern adviseur.

Voorgesteld wordt de Code voor Informatiebeveiliging (British Standard 7799) als uitgangspunt voor het beveiligingstraject te kiezen. Deze standaard is uitgegroeid tot de breedst geaccepteerde de-factostandaard voor de beheersing van informatiebeveiliging binnen organisaties. De Code bestaat uit de volgende onderwerpen:

1. Beleid
2. Organisatie
3. Classificatie en beheer
4. Personeel
5. Fysieke beveiliging
6. Computer- en netwerkbeheer
7. Toegangsbeveiliging voor systemen
8. Ontwikkeling en onderhoud van systemen
9. Continuïteitsplanning
10. Toezicht

De Code voor Informatiebeveiliging heeft als doel het beveiligingsniveau binnen organisaties op een noodzakelijk minimumpeil te brengen en zo het wederzijds vertrouwen tussen organisaties en/of organisatieonderdelen onderling te bevorderen. De Code voor Informatiebeveiliging wordt algemeen beschouwd als de meest geschikte basis voor de certificatie van informatiebeveiliging binnen organisaties.

Na een beknopte analyse van bedrijfsprocessen en informatiesystemen stelt de projectgroep vast dat de Code voor Informatiebeveiliging voor Bouwfonds bruikbaar is. Voorwaarde is wel dat deze standaard voor Bouwfonds 'op maat gesneden' dient te worden, waarbij voor specifieke toepassingen – waaronder die voor treasury – aanvullende maatregelen getroffen moeten worden (en in feite reeds getroffen zijn).

De projectgroep komt elke twee weken bijeen en formuleert binnen twee maanden een nieuw informatiebeveiligingsbeleid op basis van de Code voor Informatiebeveiliging. Het beleid wordt in het najaar van 1998 formeel goedgekeurd door het Platform Informatiebeleid en daarna formeel geaccordeerd door de Raad van Bestuur.

Door middel van een self-assessment op basis van een vragenlijst stelt de projectgroep vervolgens vast op welk peil het stelsel van beveiligingsmaatregelen binnen de onderscheiden werkmaatschappijen van Bouwfonds zich bevindt. De resultaten van de self-assessment worden besproken en gebruikt voor het opstellen van een beveiligingsplan. In dit plan wordt een aantal deelprojecten met duidelijke doelstellingen gedefinieerd, waarbij op hoofdlijnen wordt aangegeven welke middelen nodig zijn voor de uitvoering van deze deelprojecten, welke randvoorwaarden van toepassing zijn en welke doorlooptijden moeten worden verwacht. Het plan wordt voorgelegd aan het Platform Informatiebeleid en in het voorjaar van 1999 formeel door de Raad van Bestuur van Bouwfonds geaccordeerd.

Ontwikkeling en implementatie

Voor de uitvoering van het beveiligingsplan, corresponderend met de fasen 6 en 7 uit het Corporate Information Security-programma, wordt een separaat project gestart. Dit project krijgt de naam Beveiliging & Continuïteit. Binnen het project worden in overeenstemming met het projectplan vijf verschillende deelprojecten onderkend. Aan deze projecten wordt in 2000 een zesde deelproject – Certificering – toegevoegd (zie tabel 1).

Projectorganisatie

De vijf deelprojecten worden relatief onafhankelijk van elkaar uitgevoerd. De projectorganisatie is stevig, maar eenvoudig van opzet: ervaren, deskundige, zelfstandig opererende deelprojectleiders rapporteren aan een algemeen projectleider, die verantwoording aflegt aan de Stuurgroep (figuur 2). Er wordt gekozen voor een pragmatische vorm van projectmanagement, waarbij onnodig papierwerk in de vorm van gedetailleerde planningen en verslagleggingen zo veel mogelijk wordt vermeden. Beslissingen van enig belang worden vooraf ter goedkeuring voorgelegd aan het Platform Informatiebeleid.

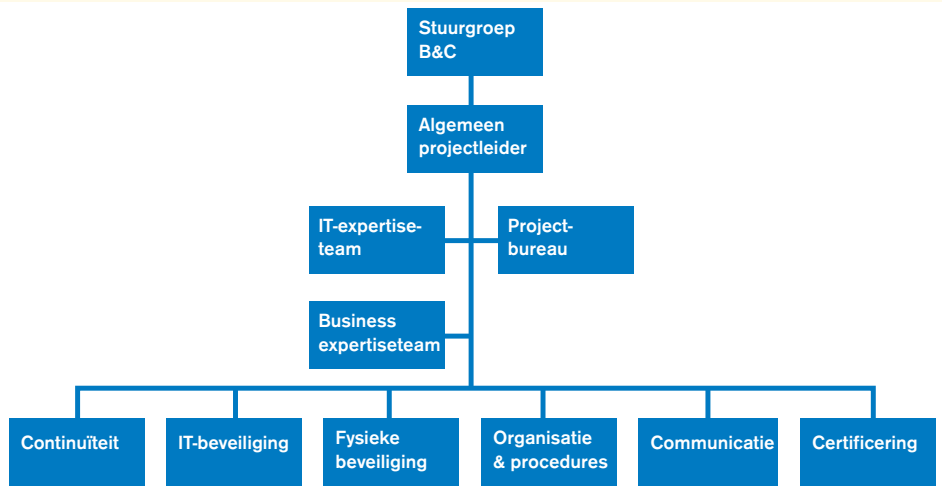
In de implementatiefase worden bovendien twee expertiseteams ingesteld om de kwaliteit van de opgeleverde producten te bewaken en tegelijkertijd draagvlak binnen de werkmaatschappijen te creëren. Deze expertiseteams bestaan uit deskundige vertegenwoordigers van enkele toonaangevende werkmaatschappijen. Het *business expertiseteam* richt zich hierbij op aspecten die de bedrijfsvoering raken; de samenstelling van dit team komt niet geheel toevallig overeen met de samenstelling van de projectgroep voor de fasen 1 tot en met 5. Het *IT-expertiseteam* richt zich op IT-specifieke zaken. Daarbij moet vaak worden overlegd over specifieke technische details die voor het algemeen management minder interessant zijn.

Resultaten

Kort samengevat kan worden gesteld dat alle projectdoelstellingen zijn bereikt, waarbij de oorspronkelijk geplande doorlooptijden in een aantal gevallen overschreden zijn. Hieronder worden de resultaten per deel-

Deelproject	Doelstelling
Continuïteit	* Het instellen van operationele continuïteitsvoorzieningen voor de informatiesystemen van Bouwfonds en Stater.
IT-beveiliging	* Een adequate beveiliging van de computernetwerken en besturingssystemen bij Bouwfonds en Stater.
Fysieke beveiliging	* Een adequate fysieke beveiliging van de gebouwen en terreinen van Bouwfonds en Stater.
Organisatie en procedures	* Het ontwerpen, toetsen, accepteren en invoeren van procedures en richtlijnen voor een aantal deelgebieden.
Communicatie	* Het uitvoeren van een gericht communicatieprogramma in het kader van awareness en voorlichting rond de invoering van procedures en richtlijnen.
Certificering	* Het certificeren van de werkmaatschappijen van Bouwfonds en Slater tegen de Code voor Informatiebeveiliging.

Tabel 1. De zes deelprojecten.



Figuur 2. Projectorganisatie Beveiliging & Continuïteit.

project beschreven, waarbij ook wordt ingegaan op de wijze waarop die resultaten tot stand zijn gekomen. Bijzondere aandacht gaat uit naar het deelproject Continuïteit, dat in elk opzicht de grootste impact had en ook de grootste inspanning gevergd heeft.

Deelproject Continuïteit

Het deelproject Continuïteit vangt aan met een inventarisatie van de eisen die aan de continuïteit van de informatiesystemen van Bouwfonds en Stater worden gesteld. Hier worden twee belangrijke uitgangspunten geformuleerd, die door het Platform Informatiebeleid worden geaccordeerd:

A. Voor de belangrijkste systemen geldt een maximale uitvalsduur van 24 klokuren.
B. Gegevens die ouder zijn dan één uur mogen niet verloren gaan.

Onder de maximale uitvalsduur wordt verstaan: de tijd die verstrijkt vanaf het optreden van een calamiteit tot volledig herstel van het operationele systeem.

Deze stringente eisen, die voortvloeien uit het feit dat Bouwfonds en Stater verantwoordelijk zijn voor kritische productiegegevens van derden, blijken verstrekkende gevolgen te hebben voor de te kiezen oplossing. Een korte analyse wijst uit dat met een traditionele uitwijkaanpak niet aan de gestelde eisen kan worden voldaan. Bij zo'n aanpak worden dagelijks back-ups gemaakt, die op een externe uitwijklocatie worden opgeslagen. Bij een eventuele calamiteit worden de back-ups op de uitwijklocatie teruggeladen, waarna de productie op de uitwijklocatie kan worden hervat. Doordat het terugladen van de back-ups gegeven de huidige hoeveelheid data langer duurt dan 24 uur, kan op deze wijze niet aan eis A worden voldaan. En doordat deze back-ups slechts eenmaal per dag kunnen worden gemaakt, kan niet aan eis B worden voldaan. Mirroring is de enige mogelijkheid. Hierbij worden de productiegegevens in real-time op een secundaire externe locatie opgeslagen. Bij een calamiteit hoeven geen back-ups te worden teruggeladen, maar kan de productie direct worden hervat.

De stroomvoorziening bleek aanvankelijk niet toereikend om alle apparatuur van stroom te kunnen voorzien.

De principebeslissing een mirroringoplossing te implementeren leidt direct tot een technische uitdaging. Zoals tegenwoordig vaak het geval is, zijn kritische productiegegevens en informatiesystemen van Bouwfonds en Stater verspreid over tientallen servers van uiteenlopende pluimage, van Windows NT op Intel-machines tot Unix en OpenVMS op het Digital Alpha-platform.

Het realiseren van een mirroringoplossing in deze heterogene omgeving blijkt vrijwel niet mogelijk zonder een ingrijpende wijziging in de IT-infrastructuur. Deze wijziging behelst het concentreren van de opslag van gegevens op een beperkt aantal storagesystemen met hoge capaciteit, hoge performance en hoge betrouwbaarheid.

Een aantal leveranciers wordt gevraagd offerte uit te brengen, en na een formele selectieprocedure op basis van objectieve criteria wordt gekozen voor de aanbieding van leverancier EMC. Deze aanbieding bestaat uit twee opslagsystemen van het type Symmetrix 3830, twee opslagsystemen van het type Symmetrix 3930, en een tweetal switches van het type Connectrix. Deze laatste zijn nodig om het grote aantal verschillende servers bij BITS en Stater op de opslagsystemen aan te kunnen sluiten. De technologie van EMC geldt als zeer geavanceerd en wordt door veel grote organisaties gebruikt voor de opslag van bedrijfskritische gegevens. Met de order is een bedrag van vele miljoenen guldens gemoeid. De totale opslagcapaciteit bedraagt circa 22.6 Terabyte.

Voor de rest van dit deelproject wordt een planning in drie fasen opgesteld. In fase 1 worden de primaire opslagsystemen geïnstalleerd, en worden de gegevens gemigreerd van de oude schijven naar de EMC-omgeving. In fase 2 worden de secundaire opslagsystemen geïnstalleerd, en worden de primaire en de secundaire systemen op elkaar aangesloten door middel van een snelle datacommunicatieverbinding. In fase 3 wordt de benodigde redundante processorcapaciteit aangeschaft en worden er continuïteitsplannen ontwikkeld.

In het najaar van 1999 installeert EMC de primaire opslagsystemen samen met IT-specialisten van Stater en Bouwfonds. De servers worden voorzien van speciale interfacekaarten, die aansluiting op de Symmetrix- en Connectrix-apparatuur mogelijk maken. In het traject doen zich diverse technische problemen voor, die in nauwe samenwerking met de leverancier worden opgelost. Flexibiliteit en improvisatievermogen blijken van groot belang.

Sommige problemen en oplossingen zijn min of meer gebruikelijk in een traject als dit. Zo worden bepaalde servers van een oud type niet door EMC ondersteund en moeten nieuwe servers worden aangeschaft. Andere problemen zijn opmerkelijker. Zo blijkt de stroomvoorziening in het Stater-gebouw aanvankelijk niet toereikend om alle apparatuur van stroom te kunnen voorzien. In afwachting van het uitbreiden van de voorzieningen door het energiebedrijf wordt een speciaal voor de millenniumwisseling gereserveerde dieselgenerator ingezet, waarop de keukenapparatuur in het bedrijfsrestaurant wordt aangesloten. Hiermee wordt voldoende capaciteit vrijgemaakt voor de EMC-apparatuur.

De installatie van primaire opslagsystemen vindt plaats zonder noemenswaardige problemen. Hetzelfde geldt voor de migratie van de productiegegevens, waaronder ook de softwarebestanden. Enige uitloop in de planning wordt veroorzaakt door de 'frozen period' voorafgaand aan de millenniumwisseling, een periode waarin geen aanpassingen aan de systemen meer toegestaan waren. Dit leidt in oktober en november tot een grote hoeveelheid noodzakelijk onderhouds- en beheerswerk, waardoor de beschikbare personeelscapaciteit onder druk komt te staan.

In december is de migratie een feit en is fase 1 voltooid. Op de valreep van het boekjaar wordt nog besloten tot een uitbreiding van de opslagcapaciteit. De millenniumwisseling verloopt ook voor Bouwfonds zonder kleerscheuren.

Fase 2 vangt aan met een onderzoek naar de meest geschikte uitwijklocaties voor Bouwfonds en Stater, en naar de meest geschikte datacommunicatieverbindingen tussen deze locaties. De locatiekeuze wordt bemoeilijkt door de gelijktijdige ontwikkeling van plannen om onderdelen van Bouwfonds en Stater naar een andere locatie te verhuizen. Maar uiteindelijk wordt gekozen voor een situatie waarbij Bouwfonds in Hoevelaken en Stater in Amersfoort als elkaars uitwijklocatie fungeren. Voor de datacommunicatieverbinding, over een afstand van een kleine zes kilometer, wordt een kostenonderzoek gedaan. Hieruit blijkt dat het laten aanleggen van een eigen glasvezelverbinding vele malen goedkoper is dan het huren van de benodigde capaciteit bij een grote leverancier, zo die al kan leveren; de jaarlijkse afschrijving op een investering van enkele honderdduizenden guldens is aanzienlijk lager dan de jaarlijkse huurkosten. De firma Van der Donk krijgt opdracht de benodigde vergunningen te regelen, het graafwerk te verrichten, de glasvezelkabel in te blazen en af te monteren. Vier maanden later is deze verbinding operationeel.

In juli 2000 zijn ook de noodzakelijke aanpassingen aan de rekencentra in Hoevelaken en Amersfoort gerealiseerd. De secundaire EMC-systemen worden geïnstalleerd en op de glasvezelverbinding aangesloten. Hierna vindt automatisch synchronisatie tussen de primaire en de secundaire Symmetrix-systemen plaats. In de zomer van 2000 is de koppeling operationeel. Real-time mirroring is een feit. In één opzicht is de oorspronkelijke doelstelling niet gehaald: het gegevensverlies bij een eventuele calamiteit is niet beperkt tot één uur, maar tot nul uur.

In fase 3 zal de benodigde redundante processorcapaciteit worden aangeschaft. Ook zullen de noodzakelijke continuïteitsplannen worden opgesteld. Fase 3 zal begin 2001 zijn afgerond.

Deelproject IT-beveiliging

Het deelproject IT-beveiliging begint met een quick scan, die wordt uitgevoerd door KPMG. De quick scan legt de belangrijkste kwetsbaarheden in de IT-infrastructuur bloot, waarbij de focus ligt op besturingssystemen en netwerken. Deze kwetsbaarheden worden geanalyseerd en in de maanden daarna stelselmatig weggenomen. Het gaat hierbij om het configureren van actieve netwerkcomponenten, het verwijderen van specifieke toegangsmogelijkheden en het installeren van speciale software voor veilige bestandsuitwisseling.

Een onderdeel van dit deelproject is het uitvoeren van een onderzoek naar nieuwe authenticatietechnieken, waaronder tokenoplossingen en digitale certificaten. Dit onderzoek wordt afgerond met als belangrijkste conclusie dat digitale certificaten in opmars zijn, maar dat de markt voor nieuwe authenticatietechnieken nog te zeer in beweging is om nu al te standaardiseren.

Deelproject Fysieke beveiliging

In dit deelproject worden de verschillende locaties van Bouwfonds en Stater bezocht, waarbij tekortkomingen in de fysieke beveiliging worden blootgelegd. In overleg met de verantwoordelijke gebouwbeheerder wordt een plan opgesteld om deze tekortkomingen weg te nemen. Realisatie van deze plannen vindt plaats in de maanden daarna.

Deelproject Organisatie en procedures

In dit deelproject worden procedures en richtlijnen op het gebied van informatiebeveiliging opgesteld, die worden gebundeld in een Handboek Informatiebeveiliging. De procedures en richtlijnen zijn voor een deel een formalisering van de bestaande praktijk. Onderdelen van het Handboek Informatiebeveiliging worden steeds beoordeeld en van commentaar voorzien door de leden van het business expertiseteam, zodat afstemming met de werkmaatschappijen gewaarborgd is.

In december 1999 is het Handboek Informatiebeveiliging voltooid. Het wordt begin 2000 formeel goedgekeurd door de Raad van Bestuur en overgedragen aan de concern security manager. Deze draagt zorg voor beschikbaarstelling in papieren vorm, op cd-rom en via het concernbrede intranet, Insite.

De verdere invoering van het Handboek is de verantwoordelijkheid van de onderscheiden organisatieonderdelen. Hiertoe wordt per werkmaatschappij een lokale information security manager aangesteld en ingewerkt.

Deelproject Communicatie

In dit deelproject wordt een communicatieplan ontwikkeld om enkele basisregels over te dragen en het algemeen beveiligingsbewustzijn te verhogen. Een eerste versie van het plan wordt door het Platform Informatiebeleid als te creatief beoordeeld. De tweede, sobere versie wordt goedgekeurd en na de formele goedkeuring van het Handboek Informatiebeveiliging uitgevoerd.

In april wordt een brochure met richtlijnen en handige tips aan elke Bouwfonds-medewerker verstrekt, vergezeld van een brief van de Raad van Bestuur. De brochure is opgesteld in de huisstijl van Bouwfonds en heeft de kunstcollectie van Bouwfonds als motief. In de maanden daarna installeert BITS screensavers met wachtwoordbeveiliging op de PC van elke Bouwfonds-medewerker.

Deelproject Certificering

Ook voor dit deelproject wordt een separaat plan van aanpak opgesteld, dat mede is gebaseerd op het gehanteerde certificatieschema. In het kader van dit deelproject voert de externe accountant, Ernst & Young, in de maanden juli en augustus 2000 een pre-certification audit uit. De audit is gebaseerd op self-assessments, die in juni door de lokale information security managers zijn uitgevoerd. De resultaten van de audit zullen tijdens de certificering in oktober 2000 worden gebruikt door de certificerende organisatie, KPMG Certification.

J. Acohen
is adjunct-directeur Innovation & Information Technology bij Stater. Rol in het project: voorzitter van het IT-expertiseteam.

A.J. de Boer
is Information Security Manager bij Bouwfonds. Rol in het project: voorzitter van het business expertiseteam.

G. uit de Bosch
is hoofd van Bouwfonds IT Services (BITS). Rol in het project: projectmanager IT-beveiliging.

C. van Rinsum
is zelfstandig adviseur en directeur bij Varmit. Rol in het project: projectmanager Continuïteit.

E. Roos Lindgreen
is partner bij KPMG Information Risk Management. Rol in het project: algemeen projectmanager.

Lessons learned

Zoals gebruikelijk in de laatste fase van een groot project heeft ook een evaluatie plaatsgevonden. Belangrijkste conclusie is dat de gevolgde aanpak tot de gewenste resultaten heeft geleid. De doelstellingen zijn gehaald.

Bij de planning en aansturing van de verschillende deelprojecten is, zoals gezegd, gekozen voor een snelle, pragmatische aanpak. Door deze aanpak bleek het mogelijk snel in te spelen op veranderende omstandigheden die zich tijdens het project voordeden. Zo werd het project beïnvloed door lopende ontwikkelingstrajecten, onvoorziene technische uitdagingen, de voorbereidingen voor de millenniumwisseling en, last but not least, de overname van Bouwfonds door ABN Amro in het najaar van 1999. (Tijdens het bijbehorende due diligence-onderzoek is overigens ook het project Beveiliging & Continuïteit doorgelicht; een waardevolle second opinion voor opdrachtgever en projectorganisatie, met positieve uitkomst.)

De belangrijkste keuzen die in het project zijn gemaakt, zijn achteraf juist gebleken. Het bleek goed de projectdoelstellingen in afzonderlijke, duidelijk afgebakende deelprojecten te beleggen. Deze modulaire aanpak maakte het mogelijk de verschillende activiteiten redelijk onafhankelijk van elkaar uit te voeren en heeft de communicatie tussen projecten onderling tot het hoogst noodzakelijke beperkt. Het commitment van de hoogste leiding, de inzet van de betrokken medewerkers, de kwaliteit van de projectmanagers en de samenwerking tussen de verschillende betrokken organisatieonderdelen en externe partijen (EMC, KPMG, Ernst & Young, Van der Donk) worden door alle betrokkenen als positief beoordeeld. Aandachtspunten daarbij zijn kwaliteitsbewaking in de relatie met de leveranciers en het omgaan met heterogene belangen van verschillende werkmaatschappijen.

De continuïteit van een kritische, heterogene IT-omgeving is blijvend gewaarborgd.

Naast het feit dat de beoogde doelstellingen gehaald zijn, heeft het project ook een aantal welkome bijeffecten gehad. De belangrijkste bonuspunten zijn:
* *betrouwbaarheid:* door de mirroringoplossing raken bij een calamiteit in het geheel geen gegevens meer verloren;
* *uniformering:* de IT-infrastructuur is gestandaardiseerd en up-to-date gebracht;
* *centralisering:* bij het uitvoeren van dit project zijn enkele lokaal beheerde servers onder centraal beheer gebracht;
* *performance:* installatie van de EMC-apparatuur heeft voor bepaalde toepassingen geleid tot een meetbaar betere performance; bij batchverwerking ligt deze verbetering tussen de dertig en vijftig procent.
* *flexibiliteit:* door de nieuwe opslaginfrastructuur is het eenvoudiger gebleken een toename van de benodigde opslagruimte op te vangen;
* *efficiency:* de nieuwe opslaginfrastructuur leidt tot een efficiënter gebruik van opslagcapaciteit en lagere beheerkosten.

Een en ander betekent overigens niet dat het project volstrekt rimpelloos verlopen is. Net als bij elk ander project was ook in dit geval sprake van de gebruikelijke technische problemen, politieke overwegingen en menselijke aspecten – zaken die in een artikel als dit wel nooit voldoende aan bod zullen komen en die het uitvoeren van een project als dit zo boeiend maken.

Conclusies

De gestructureerde en consistent door de hoogste leiding gedragen aanpak heeft bij Bouwfonds tot aansprekende resultaten geleid. De beveiliging is op vrijwel alle fronten op peil gebracht. Daarnaast is een organische uitwijkoplossing gerealiseerd, waarbij gebruik is gemaakt van mirroring op basis van zeer geavanceerde opslagtechnologie. Hierdoor is de continuïteit van een kritische, heterogene IT-omgeving blijvend gewaarborgd.

Ook in dit project is gebleken dat informatiebeveiliging geen op zichzelf staand specialisme meer is, maar onderdeel uitmaakt van de dagelijkse bedrijfsvoering. Bij een integraal beveiligingsproject als dit bestaat het risico dat beveiliging als een geïsoleerd probleem wordt gezien. In het geval van Bouwfonds heeft de gekozen aanpak er juist toe geleid dat het probleem inmiddels op de meeste niveaus in de organisatie wordt onderkend en aangepakt.

De menselijke factor blijft ook hier één van de belangrijkste aandachtspunten. Waar de technologie steeds complexer en het arsenaal aan hulpmiddelen steeds krachtiger wordt, groeit de afhankelijkheid van de kennis, discipline en zorgvuldigheid van gebruikers en beheerders. Het uitvoeren van een centraal geleid communicatieprogramma is daarbij niet voldoende. Passende aandacht en een positieve attitude van het management zijn minstens zo noodzakelijk. Hetzelfde geldt voor het uitvoeren van systematische controles op naleving van het beleid.

Dankwoord

Het beschreven project had niet uitgevoerd kunnen worden zonder de inzet en gedrevenheid van een groot aantal personen. Bijzondere erkentelijkheid is onder meer verschuldigd aan, in alfabetische volgorde: R. van Aart, G. Bos, J.H. Deesker, R. Douwes, J. Gerkema, T. Heusdens, P. Hoffman, H. Kleinhoven, L. van der Meché, F. van Meijgaarden, P. Lissenburg, G. Peters-Meijer, M. Pouw, F. Schuit, A. Spruitenburg, J.P. de Smeth, J. Veenstra, de betrokken medewerkers van EMC, KPMG, Ernst & Young en Van der Donk en de bestuurder van de tankwagen.