

Een dementerende overheid?

**De risico's van digitaal beheer van
verantwoordingsinformatie bij de centrale overheid**

Rijksarchiefinspectie

27 januari 2005

RIJKSARCHIEFINSPECTIE

De hoofdinspecteur van de Rijksarchiefinspectie oefent ingevolge de Archiefwet 1995 toezicht uit op de naleving van deze wet door het Rijk, de zelfstandige bestuursorganen en de organen van publiekrechtelijke bedrijfsorganisatie.

De Rijksarchiefinspectie controleert de naleving van de archiefwetgeving en de kwaliteit van het archiefbeheer. Hiertoe voert de Rijksarchiefinspectie onderzoeken en inspecties uit. Daarnaast rapporteren de zorgdragers jaarlijks aan de Rijksarchiefinspectie over hun archiefbeheer.

De hoofdinspecteur rapporteert aan de betrokken overheidsorganen en, indien hiertoe aanleiding is, aan de voor het archiefwezen verantwoordelijke minister van Onderwijs, Cultuur en Wetenschap. Jaarlijks brengt de hoofdinspecteur schriftelijk verslag uit over het toezicht op het archiefbeheer aan de minister, die het verslag vervolgens aan de Tweede Kamer overlegt.

De Rijksarchiefinspectie is in Den Haag gevestigd en als volgt bereikbaar:

Rijnstraat 50
Postbus 16478
2500 BL Den Haag

Algemeen telefoonnummer	070-4124045
Fax	070-4124014
E-mail	info@rijksarchiefinspectie.nl
Website	www.rijksarchiefinspectie.nl

Inhoudsopgave

	Samenvatting	5
1	Inleiding	7
2	E-mail is ook archief	9
3	Oude wijn in nieuwe zakken?	13
4	De risico's	15
4.1	Documenten raken voortijdig verloren	15
4.2	Documenten zijn niet terug te vinden	16
4.3	Documenten zijn niet juist meer te interpreteren	18
4.4	Gegevens worden te lang bewaard	20
4.5	Documenten raken onbedoeld in de openbaarheid	21
5	Eilanden van informatie en kennis	23
5.1	Een oud probleem en nieuwe kansen	23
5.2	Iedereen beschrijft processen...	23
5.3	De Archiefwet: een last of een lust?	24
5.4	Onvoldoende professionaliteit	25
6	Aanbevelingen	27

Samenvatting

In sneltreinvaart ontstaat een gat in ons collectieve geheugen, omdat digitale informatie vaak onvoldoende zorgvuldig bewaard wordt. Dat is niet alleen een probleem voor de generaties na ons, maar ook voor overheidsorganisaties die over een professionele bedrijfsvoering moeten kunnen beschikken en zich over hun daden moeten kunnen verantwoorden.

De Rijksarchiefinspectie heeft de afgelopen jaren onderzocht op welke wijze digitale bedrijfsvoerings- en verantwoordingsinformatie bij de centrale overheid beheerd wordt. We hebben onderzoeken uitgevoerd bij drie omvangrijke overheidsorganisaties. Ook bij doorlichtingen van ministeries en kortere inspecties stonden we stil bij de beschikbaarheid, ordening en toegankelijkheid van digitale informatie. Hierdoor kunnen we een beeld schetsen van 'the state of the art' bij de centrale overheid, de knelpunten en de oplossingen. Daarover rapporteren we in deze publicatie.

Een belangrijk probleem is dat overheidsorganisaties vaak geen goed overzicht hebben van de plaatsen waar zij hun verantwoordings- en digitale informatie beheren. Een groot deel van deze informatie wordt op persoonlijke en gezamenlijke schijven beheerd, buiten de beheerafspraken om. Ook databases en andere bedrijfsapplicaties blijven buiten het archiefbeheersregime. We beseffen dat dit niet nieuw is voor de digitale wereld, ook essentiële papieren documenten worden vaak in bureauladen van medewerkers teruggevonden, en niet in het formele archief. In de digitale situatie is dit probleem echter vele malen complexer, onder andere omdat digitale bestanden actief onderhouden moeten worden om leesbaar en interpreteerbaar te blijven. En hoewel het om een oud probleem gaat, zijn er juist in de digitale omgeving nieuwe kansen om de problematiek professioneel op te lossen. Zo zijn veel organisaties, waaronder de ministeries, bezig op dit moment document management systemen en record management applicaties op professionele wijze in te richten, hetgeen we een positieve ontwikkeling vinden. We vragen in dit rapport aandacht voor het feit dat de inrichting van zulke applicaties nauw moet aansluiten op de primaire processen van overheidsorganisaties, dat er goede beheersafspraken moeten worden gemaakt, dat de juiste expertise beschikbaar moet zijn en dat de kwaliteiten van verschillende professies gebundeld moeten worden om dergelijke projecten te doen slagen. Gebeurt dit niet, dan zullen dezelfde risico's blijven bestaan als we in de praktijk zijn tegengekomen:

- documenten raken voortijdig verloren door misverstanden, bewuste en onbewuste schoonacties;
- documenten zijn niet terug te vinden omdat iedereen ze naar eigen inzicht heeft opgeborgen;
- documenten zijn niet juist meer te interpreteren doordat de juiste contextinformatie ontbreekt;
- gegevens worden langer bewaard dan op grond van de privacy- en archiefwetgeving is toegestaan;
- documenten raken onbedoeld in de openbaarheid.

Een aantal overheidsorganisaties - met name de ministeries - is de laatste jaren op het gebied van het beheer van digitale (verantwoordings)informatie de juiste weg ingeslagen. Toch is de Rijksarchiefinspectie er na haar onderzoeken, inspecties en

andere opgedane ervaring van overtuigd dat de incidenten over digitale informatie die in de afgelopen jaren de media hebben gehaald geen incidenten zijn, maar onderdeel uitmaken van een structureel probleem. Daarom vragen we onze staatssecretaris voor Cultuur, de minister voor Bestuurlijke Vernieuwing en het management van de organisaties van de centrale overheid om de verantwoordelijkheid voor deze problematiek op te pakken.

1 Inleiding

De twintigste eeuw is de best gedocumenteerde eeuw. Nog nooit werden er zoveel papieren en audiovisuele documenten geproduceerd en bewaard. Er zijn professionele archiefdiensten gekomen om deze informatie te bewaren in de periode nadat de documenten waardevol waren voor de (overheids)organisaties zelf. Ook de documenten die uit eerdere eeuwen bewaard waren gebleven, werden bij de archiefdiensten opgeslagen.

Vitale informatie ontbreekt

Maar wat gebeurt er de laatste decennia? De toevoer van overheidsdocumenten aan de archiefdiensten is niet langer volledig. Nog altijd is er weliswaar een aanbod van omvangrijke papieren bestanden aan de archiefdiensten, maar vitale informatie ontbreekt. Informatie die niet langer op papier te vinden is, maar uitsluitend bestaat zolang de geschikte software en hardware beschikbaar is: digitale informatie. Zo ontstaat er een sneltreinvaart een gat in het collectieve geheugen.

De sense of urgency is niet groot, het lijkt een probleem voor de generaties na ons. Maar is dit wel waar? Uit het NIOD-rapport over Screbrenica bleek dat communicatie tussen het ministerie van Defensie en de uitgezonden eenheden voor een deel via de e-mail plaatsvond. En e-mails, nee, die werden niet gestructureerd bewaard. Gelukkig waren er nog mensen die het gebeurde konden navertellen. Maar hoe objectief zijn mensen? Hoe volledig is hun geheugen? Konden zij zich nog werkelijk herinneren welke opdrachten zij op welk moment hadden gegeven of ontvangen?

Ambitie: de elektronische overheid

De laatste jaren heeft het kabinet de ambitie uitgesproken om zoveel mogelijk overheidsdiensten digitaal aan te bieden en overheidsinformatie actief openbaar te maken. Informatie ontvangen burgers tegenwoordig via internet, aanvragen voor vergunningen en subsidies kan men eveneens via de digitale snelweg indienen. Het zal niet lang meer duren voordat een transport met gevaarlijke stoffen via het internet gevolgd kan worden. Dat vergroot de transparantie van de Nederlandse overheid en zorgt voor een slagvaardigere overheid. Vaak zien de websites er overzichtelijk uit, de overheidssites ogen betrouwbaar. Maar wat gebeurt er met de verzonden informatie aan de achterkant, in de back office? Het is van het grootste belang dat overheidsorganisaties deze informatie op zorgvuldige wijze opslaan en beheren, zodat de primaire processen optimaal ondersteund worden en de informatie ook op een later moment ook weer geraadpleegd kan worden. Als dit niet gebeurt, zal uiteindelijk geen enkele overheidsorganisatie nog slagvaardig kunnen optreden en de betrouwbaarheid van de overheid als geheel afnemen.

De digitale back office: het terrein van de ICT

Tot op de dag van vandaag is de digitale back office het terrein van ICT'ers. Zij zorgen ervoor dat er genoeg schijfruimte beschikbaar is om alle digitale informatie op te slaan. Zij letten erop dat bestanden tijdig geconverteerd worden naar nieuwe bestandsformaten, dat er een handige zoekmachine draait en dat er een back-upprocedure beschikbaar is. Dat zijn allemaal belangrijke randvoorwaarden om informatie beschikbaar te houden. Maar we kunnen niet alles van technici verwachten. Zij houden zich in veel mindere mate bezig met de vraag welke documenten de authentieke archiefdocumenten zijn, met de vraag hoe processen op basis van documenten gereconstrueerd kunnen worden en hoe bestanden bewaard moeten

blijven. Deze vragen werden van oudsher beantwoord door een andere beroepsgroep: de archivariissen en de medewerkers voor de documentaire informatievoorziening. En deze beroepsgroep heeft weliswaar vanaf de zijlijn gewaarschuwd dat we zorgvuldiger met onze digitale informatie moeten omgaan, maar heeft hierin tot nu toe nauwelijks een actieve rol gespeeld of kunnen spelen.

Onderzoeken en inspecties Rijksarchiefinspectie

De Rijksarchiefinspectie heeft in de afgelopen jaren onderzoek gedaan naar de hierboven geschetste problematiek. We draaiden mee in een project om de digitale erfenis veilig te stellen bij de Arbeidsvoorziening¹, hebben een groot aantal medewerkers bij de Centra voor Werk en Inkomen (CWI) geïnterviewd en voerden een onderzoek uit bij het Kadaster naar het beheer van digitale bestanden. Ook bij doorlichtingen van ministeries en quick scans² bij kleinere organisaties stonden we stil bij de beschikbaarheid, ordening en toegankelijkheid van digitale informatie. Voor een deel hebben we onze bevindingen al eerder gepubliceerd. Ook ons jaarlijks verslag over het toezicht heeft regelmatig aandacht besteed aan het onderwerp digitale archivering. Maar door de onderzoeks- en inspectieresultaten samen te voegen kunnen we in dit rapport een beeld schetsen van de 'state of the art' bij de centrale overheid, de knelpunten en de oplossingen die aan de horizon verschijnen. Ook hebben we inmiddels een beeld van de mate waarin de Nederlandse wetgeving voldoet om de risico's weg te nemen. Onze bevindingen op dit punt hebben we niet opgenomen in dit rapport, maar zullen we melden aan de evaluatiecommissies van de regelingen *Duurzaamheid archiefbescheiden*, *Geordende en toegankelijke staat archiefbescheiden* en *Bouw en inrichting archiefruimten en archiefbewaarplaatsen*. In het algemeen kunnen we zeggen dat de bekendheid met de regelgeving nog te wensen over laat, dat het toepassen van met name de *Regeling geordende en toegankelijke staat archiefbescheiden* op archiefbescheiden die in het verleden gevormd zijn maar in beperkte mate mogelijk is, en dat de *Regeling bouw en inrichting archiefruimten en archiefbewaarplaatsen* niet specifiek gericht is op ruimten waarin digitale bestanden beheerd worden, zoals serverruimten.

Dit rapport

Tijdens gesprekken met managers, DIV-medewerkers en ICT'ers bleek er grote onduidelijkheid te bestaan over de vraag wat nu eigenlijk digitale archiefbescheiden zijn. Daarom besteden we het tweede hoofdstuk van dit rapport aan een afbakening van het onderwerp. Vervolgens stellen we ons de vraag of er nu eigenlijk wel zoveel verschil is tussen het beheren van papieren en digitale informatie. In het vierde hoofdstuk besteden we aandacht aan de risico's die we in de praktijk zijn tegengekomen bij het beheren van digitale bestanden. Hoofdstuk 5 bevat een analyse van de risico's: hoe kunnen ze ontstaan, maar ook: hoe zouden ze kunnen worden voorkomen? We sluiten af met een concluderend hoofdstuk en met aanbevelingen.

1 *Rijksarchiefinspectie, De digitale erfenis. Deelrapport 1: Arbeidsvoorziening (Den Haag 2003)*
2 *In 2004 voerde de Rijksarchiefinspectie 75 korte inspecties uit bij (onderdelen van) overheidsorganisaties. Het betrof 45 algemene quick scans, vijftien bezoeken met als onderwerp digitaal archiefbeheer en vijftien bezoeken met als onderwerp overbrenging. De rapportages zijn gepubliceerd op de website van de Rijksarchiefinspectie.*

2 E-mail is ook archief

Een groot deel van onze gesprekspartners verkeerde vóór ons bezoek ten onrechte in de veronderstelling dat zij in het geheel geen digitaal archief - en dus geen digitaal duurzaamheidsprobleem - hadden. We krijgen bij onze inspecties regelmatig te horen: 'Wij printen alles op papier en dat stoppen we in het dossier, dus hebben we geen digitaal archief.' Maar als we verder praten, blijkt zo'n organisatie wel degelijk digitaal archief te beheren, ook al is dit niet altijd in beeld.

Er bestaat veel verwarring over de reikwijdte en inhoud van het begrip (digitale) archiefbescheiden. Daarom besteden we in dit hoofdstuk aandacht aan de vraag wat de wet onder dit begrip verstaat.

Archiefbescheiden, wat zijn dat eigenlijk?

Elke organisatie bewaart de informatie die nodig is om de werkzaamheden te kunnen uitvoeren of om op een later moment verantwoording over die werkzaamheden te kunnen afleggen. De creatie en ontvangst van informatie gebeurt zowel binnen de beleidsprocessen als binnen de ondersteunende processen. Alle informatie die binnen deze processen gegenereerd en uitgewisseld wordt, vormt samen het archief van een organisatie. Het gaat dus ook om interne documenten en concepten, maar niet om eerste versies of persoonlijke aantekeningen die alleen de opsteller heeft gezien.

Vaak zien we dat een organisatie alleen de stukken die in een postregistratiesysteem zijn ingeschreven als het archief beschouwt. Maar als we vervolgens over de schouder van een medewerker meekijken naar de inhoud van zijn persoonlijke schijf, of in zijn bureaula, dan constateren we dat hij nog een heleboel andere documenten beheert, omdat die juist nodig zijn om zijn werk goed te kunnen doen. De kern is, dat ook die documenten – of het nu om uitgewisselde concepten gaat, om e-mail of informatie in databases - tot het archief van een organisatie behoren.

Bij procedurele uitvoeringsprocessen zien we vaak al dat organisaties elk document – want elke processtap - in het (papieren of digitale) dossier willen terugzien. Met een onvolledig dossier kan men immers niet goed werken en zich niet goed verantwoorden. Bij beleidsprocessen heeft dit besef zich nog niet vertaald in goede afspraken over de dossiervorming, hoewel het ook hier van belang is om na te gaan hoe men tot een oordeel is gekomen. Discussies over beleid vinden tegenwoordig vaak plaats via e-mail. We zien dan ook dat e-mail al een aantal keren gebruikt is om besluitvorming te reconstrueren. Denk bijvoorbeeld ook aan de Jamby-affaire, waarin het vermoeden bestond dat ambtenaren van het ministerie van OCW betrokken zouden kunnen zijn bij een fraudezaak. In de rechterlijke uitspraak in deze zaak wordt diverse malen verwezen naar uitgewisselde e-mails. Na de rechtszaak zijn er naar aanleiding van deze zaak Kamervragen gesteld over ontbrekende documenten. Uit het antwoord blijkt dat het ministerie van OCW aan het Openbaar Ministerie stukken heeft verstrekt over de zaak Jamby, afkomstig van een gezamenlijke schijf. Dit voorbeeld maakt duidelijk dat digitale informatie een grote rol kan spelen in de bewijsvoering.

Een ander voorbeeld vormen de tabellen, grafieken en getallen in jaarverslagen. Voor de onderbouwing van deze cijfers gebruiken organisaties (financiële) databases,

rekenprogramma's en andere hulpmiddelen binnen de kantoorautomatisering. Alle onderliggende documenten horen tot het archief van een organisatie – dus niet alleen het eindproduct. Het nut om over alle documenten goede afspraken te maken, blijkt wel uit het volgende voorbeeld: Bij het CWI kwam de interne accountant bij een beleidsmedewerker op de PC controleren waar de gegevens uit het jaarverslag vandaan kwamen. Op deze afdeling werd de digitale informatie zorgvuldig beheerd en kon de medewerker de accountant laten zien waar de uitkomsten op gebaseerd waren. Dit is helaas niet altijd het geval.

Concepten van brieven, nota's en verslagen horen ook bij het archief. Burgers kunnen zelfs een beroep doen op de Wet Openbaarheid van Bestuur om uitgewisselde concepten in te zien. Een aantal decennia geleden was het ook de normaalste zaak dat concepten werden opgenomen in een dossier. Maar wij hebben bij onze quick scans gezien dat juist deze stukken tegenwoordig vaak uitsluitend digitaal bestaan. Alleen de eindversies gaan een formeel traject in en worden uiteindelijk geregistreerd in het postregistratiesysteem. De concepten blijven ten onrechte buiten het formele archief van de organisatie vallen.

In het voorgaande hebben we willen aantonen dat overheidsorganisaties voor een efficiënte bedrijfsvoering en een goede verantwoordingsfunctie niet langer kunnen vertrouwen op hun archief, omdat een groot deel van de relevante informatie buiten dit formele archief wordt beheerd. Dat er desondanks niet direct van alles mis lijkt te gaan, komt doordat individuele medewerkers beseffen dat zij documenten beheren die nergens anders zijn, en deze worden – zoals eerder gezegd – in bureauladen en op persoonlijke schijven beheerd. De opluchting is vaak groot als blijkt dat een medewerker – na lang zoeken – nog een versie (welke versie?) van een brief tevoorschijn kan toveren. Dit is natuurlijk geen werkwijze waarop een professionele overheidsorganisatie mag vertrouwen én niet conform de archiefwetgeving. Bedrijfsvoerings- en verantwoordingsinformatie hoort op een zorgvuldige manier te worden beheerd.

Papier en digitaal naast elkaar

De risico's zijn op dit moment extra groot omdat overheden zich nog in een situatie bevinden waarbij er digitale en papieren archieven naast elkaar bestaan. Soms worden deze dubbel bewaard, soms of op papier of digitaal, en vaak noch op papier, noch digitaal omdat er geen goede afspraken zijn gemaakt. Deze hybride situatie zal ons inziens nog wel een tijd voortduren. Het is daarom voor overheidsorganisaties uitermate belangrijk om vast te stellen welke informatie op papier en welke informatie digitaal beschikbaar is. De realiteit wijst uit dat veel overheidsorganisaties nog geen goede voorzieningen hebben getroffen om verantwoord digitaal te kunnen archiveren en geen goed systeem hebben om bijvoorbeeld e-mail goed te beheren.

Sommige overheidsorganisaties, zoals bijvoorbeeld het ministerie van Financiën, hebben daarom de afspraak gemaakt dat het archiefbeheer zich slechts richt op het papieren archief en dat voor de formele zaken de e-mail niet gebruikt mag worden. Op zich is het positief dat er afspraken gemaakt worden om helder te houden wat wel en niet digitaal mag worden uitgewisseld. Maar we zijn van oordeel dat hiermee het probleem niet is afgedekt, omdat veel informatie alleen in digitale vorm kan bestaan. Denk bijvoorbeeld maar aan de gegevens in databases. Het feit dat overheidsorganisaties niet op tijd onderkennen dat zij beschikken over digitale

archiefbescheiden is schadelijk en risicovol, omdat juist bij digitale archiefbescheiden belangrijk is dat zij vanaf het begin binnen de juiste kaders beheerd worden.

Om terug te komen op het citaat uit de inleiding van dit hoofdstuk: ook het uitdraaien van digitale documenten is geen bevredigende oplossing. Want met het uitdraaien van een digitaal document kan bepaalde informatie verloren gaan waar in digitale vorm wel de beschikking over was. Hier gaan we in hoofdstuk 4 nader op in.

Conclusie: Er bestaan veel misverstanden over de reikwijdte en inhoud van het begrip archiefbescheiden. Deze onduidelijkheid is mede oorzaak van het feit dat een groot deel van de digitale informatie buiten het zicht van deskundigen wordt beheerd. Ook heeft deze situatie als gevolg dat organisaties niet beseffen dat zij een digitaal archiefprobleem hebben.

3 Oude wijn in nieuwe zakken?

Zojuist heeft u kunnen lezen dat de meeste organisaties nog een papieren archief hebben dat niet langer volledig en dus onbetrouwbaar is, terwijl er nog nauwelijks afspraken zijn gemaakt voor het beheer van documenten en gegevensbestanden in een digitale omgeving. De Rijksarchiefinspectie heeft in de praktijk ervaren dat digitale archivering als een ingewikkeld probleem wordt beschouwd wat sommige overheidsorganisaties het liefst nog even voor zich uit schuiven. Er zijn echter ook mensen die vinden dat er met de overgang naar digitaal archief niets fundamenteel verandert. In deze paragraaf inventariseren we in hoeverre er nu werkelijk iets verandert.

Overeenkomsten

Een aantal basisprincipes die gelden voor het papieren archief is direct toepasbaar op het digitale archief. Bijvoorbeeld dat de documenten op een logische plaats zijn opgeborgen, waarbij duidelijk is welke documenten bij elkaar horen. Het oplossen van het probleem van duurzaam digitaal bewaren heeft alleen zin als het basisprincipe van een deugdelijke ordening is gerespecteerd. Het is misschien nog wel moeilijker om het juiste document op een harde schijf vol ongeordende en onlogisch betitelde documenten te vinden dan op een zolder vol met papieren stukken. De digitale omgeving maakt het kortom nog belangrijker om bij het opzetten van een archief over de structuur na te denken. Hierbij denken we overigens niet zozeer aan classificatiecodes zoals deze in de papieren omgeving werden en worden toegepast. Vaak sluiten deze indelingen onvoldoende aan op de processen die daadwerkelijk in een organisatie spelen. Meer denken we aan een dossierstructuur die naadloos aansluit op de werkprocessen.

Verschillen

Het lijkt voor de hand liggend, maar het belangrijkste verschil tussen het papieren en digitale archief is allereerst dat digitale documenten uitsluitend met behulp van een computer gelezen kunnen worden. Een papieren document is direct te raadplegen. Bij digitale gegevens zijn hardware, software en opslagmedia nodig om de informatie weer leesbaar te maken.

Ten tweede vormen bij een papieren document, zoals een topografische kaart, de inhoud, vorm en de context vaak één onlosmakelijk geheel. Een kaartblad van het Amsteldiep laat bijvoorbeeld de geografische ligging van dit water zien ten opzichte van de omgeving. De kleuren geven aan waar water, groen of bebouwing gedacht moet worden. Er valt ook te lezen welke dienst de kaart heeft gemaakt en in welk jaar dat is gebeurd. In de marge is te zien dat de kaart deel uitmaakt van een groter geheel. Digitaal opgeslagen gegevens daarentegen kunnen los van de context bewaard worden waardoor het risico bestaat dat deze bij conversie of migratie verloren gaan. De kleuren van het kaartblad uit het voorbeeld kunnen bijvoorbeeld zo wijzigen, dat de kaart niet meer juist te interpreteren is. Of mogelijk is op een later moment niet meer vast te stellen uit welke periode de weergave op de kaart is. Daarom hebben digitale archieven op langere termijn alleen betekenis als deze contextgegevens (metadata) bewaard blijven. Het gaat dan niet alleen om inhoudelijke gegevens, maar ook om gegevens over de apparatuur en de programmatuur waarmee ze leesbaar te maken zijn.

Ten derde is het in de digitale omgeving veel meer de vraag of een document is wat het zegt te zijn. Bij digitale documenten is er een groter risico van manipulatie, wijziging en verwijdering van gegevens dan bij papier omdat dit bij digitale bestanden vaak geen direct zichtbare sporen nalaat. De aantasting van de authenticiteit gebeurt niet altijd met opzet. Ook bij conversie en migratie van bestanden kan een onbedoelde wijziging ontstaan van de context, inhoud, structuur of uiterlijk van een document.

Ten vierde vraagt het ene digitale bestand om een heel andere benadering dan het andere. Het beheer van een database waarin de openbare registers van het Kadaster worden bewaard vraagt om meer specialistische kennis dan een rapport wat is opgemaakt in een tekstverwerkingsprogramma. Er is in tegenstelling tot het eendimensionale vel papier dat we allemaal kennen sprake van verschillende 'soorten' digitaal archief. De documenten die in de kantoorautomatisering- en e-mail applicaties gemaakt worden lijken nog het meest op de vertrouwde papieren documenten. Maar we werken inmiddels ook met ingewikkelde rekenprogramma's, content management systemen, workflowmanagementtools, simpele maar ook zeer complexe databases waarvan de gegevens op allerlei manieren gebruikt worden en met andere databases in verbinding staan.

De kennis en vaardigheden voor al deze verschillende applicaties zijn zo specifiek dat binnen organisaties vaak onderscheid gemaakt wordt bij het beheer van de kantoorautomatiseringapplicaties en de bedrijfsapplicaties. Bij grote organisaties wordt er dan nog een onderverdeling gemaakt tussen de bedrijfsapplicaties die het primaire proces ondersteunen en databases voor de beleids- en ondersteunende processen. Er zijn kortom veel meer medewerkers betrokken bij het beheer van het archief dan vroeger het geval was.

Conclusie: Een kwalitatief goede ordening, die optimaal aansluit bij de werkprocessen van een organisatie, blijft een grondbeginsel voor zowel digitaal als papieren archief. Daarnaast hebben we in dit hoofdstuk geconstateerd dat er een fundamenteel andere benadering noodzakelijk is voor het beheer van digitale archieven.

4 De risico's

Welke risico's loopt een organisatie in de praktijk als digitale bestanden niet goed worden beheerd? Dit hoofdstuk behandelt de voornaamste risico's aan de hand van casussen die we tijdens onze onderzoeken en inspecties zijn tegengekomen:

- het voortijdig verloren raken van documenten;
- het niet terug kunnen vinden van documenten;
- het niet juist kunnen interpreteren van documenten;
- het te lang bewaren van documenten;
- het onbedoeld in de openbaarheid komen van documenten.

4.1 Documenten raken voortijdig verloren

In de vorige hoofdstukken heeft u kunnen lezen dat digitale archiefstukken vaak buiten de bestaande afspraken om beheerd worden. Binnen organisaties zijn er geen duidelijke afspraken over het bewaren en vernietigen van digitale documenten. In deze paragraaf leggen we uit dat het gevolg hiervan is dat er stukken voortijdig verloren gaan.

'Vriendelijk verzoek tot het schonen van schijven'

Digitale documenten zijn vluchtig en daardoor kwetsbaar. Zij gaan vaak al spoedig na hun creatie verloren. E-mail die vandaag wordt verstuurd wordt vaak morgen al vernietigd. Als een medewerker vertrekt besluit de afdeling ICT regelmatig om zijn persoonlijke bestanden voor altijd uit te wissen. Databases die niet dagelijks meer in gebruik zijn worden 'uitgefaseerd'. Er zijn over het algemeen geen afspraken gemaakt over de vernietiging van digitaal archief en medewerkers kunnen dat naar eigen inzicht doen. Hoe vaak komt het niet voor de afdeling systeembeheer de hele organisatie een bericht stuurt met het verzoek om de schijven te schonen in verband met de overbelasting van de server? Omdat er geen goede afspraken en procedures zijn voor de vernietiging van het digitaal archief is het voor medewerkers niet duidelijk dat er aan dit soort oproepen geen gehoor gegeven mag worden.

Het is natuurlijk niet zo dat digitale archiefdocumenten niet vernietigd mogen worden. De beslissing om archief te vernietigen mag echter niet bij een individu liggen of het gevolg van een tekort aan schijfruimte, maar moet gebaseerd zijn op de afspraken over bewaartermijnen die in een zogenaamde selectielijst³ zijn vastgelegd. Deze bewaartermijnen garanderen dat archiefstukken volgens afspraak voor een bepaalde tijd beschikbaar zijn.

In de praktijk is de Rijksarchiefinspectie nog nauwelijks tegengekomen dat de bewaartermijnen uit selectielijsten aan het digitale archief zijn gekoppeld.

We hebben tijdens onze onderzoeken geconstateerd dat het probleem van ongeoorloofde vernietiging urgenter is bij de bestanden die in de kantoorautomatisering en e-mail applicaties worden gemaakt dan in de bedrijfsapplicaties. De informatie in deze databases kent vaak een bepaalde structuur waardoor het makkelijker is om bewaartermijnen aan de gegevens te koppelen. De

³ Een selectielijst regelt welke categorieën archiefbescheiden voor altijd bewaard blijven, en welke categorieën op termijn vernietigd moeten worden. Aan de te vernietigen stukken kent de lijst bovendien een vernietigingstermijn toe.

vernietiging kan technisch zo geregeld worden dat niet iedere medewerker dit naar eigen inzicht kan doen. Maar ook bij het ontwerpen van bedrijfsapplicaties is niet altijd goed nagedacht over archivering en dat gegevens daarom in het dagelijks gebruik worden overschreven. Het achteraf oplossen van dit probleem heeft vaak grote financiële gevolgen.

De techniek biedt geen garanties

Veel organisaties vertrouwen erop dat bij het onbedoeld verloren gaan van informatie er een technische oplossing bestaat voor het probleem. Er is toch altijd wel een back-up voor handen? Back-upprocedures lijken inderdaad te borgen dat informatie nooit helemaal verloren gaat. We hebben bij onze onderzoeken bij het CWI en het Kadaster vastgesteld dat daar zorgvuldige afspraken zijn gemaakt voor het maken van back-ups. De back-ups bij het CWI worden elke dag gemaakt en op een aparte locatie bewaard. Maar in de praktijk is gebleken dat het maken van een back-up niet automatisch betekent dat de informatie ook altijd weer teruggeplaatst kan worden. Een probleem kan bijvoorbeeld een tekort aan beschikbare schijfruimte zijn, of dat de back-up toch niet volledig is.

Verder vinden conversie en migratie niet altijd tijdig plaats, waardoor bestanden na enige tijd niet meer beschikbaar blijken.

Dit is bijvoorbeeld ook aan de orde bij onvoldoende duurzame gegevensdragers. Er zijn meerdere onderzoeken verschenen waaruit blijkt dat cd's en dvd's slechts beperkt houdbaar zijn, waardoor de informatie al na korte tijd niet meer volledig kan worden weergegeven. Bij een test van bepaalde cd-rom's bleek onlangs bijvoorbeeld dat ze twee jaar na ingebruikname grote delen met onherstelbare fouten bevatten.

Tenslotte is de beveiliging van serverruimten is niet altijd voldoende. Betrokkenen bij het CWI wezen ons er zelf op dat de klimaatbeheersing en beveiliging bij de serverruimten van de vestigingen onvoldoende was. Men had dit probleem onderkend en werkte aan een oplossing.

Conclusie: Digitale archiefbescheiden worden meestal niet vernietigd op basis van een geldige selectielijst, maar op grond van een scala aan criteria, die meestal een individuele grondslag hebben. Vernietiging kan ook een gevolg zijn van technische problemen.

4.2 Documenten zijn niet terug te vinden

Eén van de grote voordelen van digitale informatie lijkt op het eerste gezicht dat zij voor iedereen binnen korte tijd toegankelijk gemaakt kan worden. De begrippen 'zoeken' en 'vinden' hebben met de introductie van zoekmachines in het digitale tijdperk een heel andere dimensie gekregen. Toch is een zoekmachine niet voldoende om informatie op de korte en langere termijn terug te vinden. In het vorige hoofdstuk wezen we er al op dat het nog steeds noodzakelijk is om structuur aan te brengen in de digitale informatie. Anders zijn de bestanden onvoldoende inhoudelijk toegankelijk. Onder inhoudelijke toegankelijkheid verstaan we niet alleen dat een afzonderlijk document terug te vinden is, maar ook dat de samenhang met andere documenten duidelijk is. Het gaat erom dat processen op basis van documenten te reconstrueren zijn en juist daarom is die samenhang zo belangrijk, evenals de context waarbinnen een document gemaakt of ontvangen is en binnen welk werkproces.

De praktijk

Uit de praktijk blijkt dat de meeste organisaties de kantoorautomatisering en e-mail applicaties gebruiken om digitale documenten te beheren. Zelfs grote organisaties als het CWI, het Nibra en de Sociale Verzekeringsbank bewaren een deel van hun beleidsdocumenten in de mapstructuur van de kantoorautomatisering. De informatie wordt op groepsschijven, maar ook op de talrijke persoonlijke schijven beheerd. De e-mail wordt bij vrijwel alle organisaties binnen het persoonlijke domein van de medewerkers beheerd.

Bij de indeling van de mapstructuur maakt men geen gebruik van de kennis van documentair informatiespecialisten, de medewerkers kijken zelf naar hun eigen behoefte. In beginsel is dit positief, een ordening moet aansluiten bij de mensen die ermee werken. De problemen ontstaan echter als een medewerker vertrekt en niemand kent de logica waarmee hij zijn documenten heeft geordend.

Ook als er wel een ordening is afgesproken leert de realiteit dat er weinig controle is op het plaatsen van stukken binnen bestaande indelingen. Stukken komen dan op plekken terecht waar niemand ze ooit nog terug kan vinden. Bij een organisatie als het CWI geldt overigens dat er bij sommige afdelingen afspraken zijn gemaakt over de indeling van de groepsschijven. Een medewerker ziet ook toe op de plaatsing van bescheiden, zodat iedereen toegang heeft tot de informatie die een medewerker op een schijf heeft geplaatst. Maar op een andere afdeling hebben wij geconstateerd dat de archiefbescheiden in het persoonlijke domein van de medewerkers werd beheerd.

Naar onze mening zijn de kantoorautomatiserings- en e-mailapplicaties over het algemeen niet geschikt voor het beheren van informatie. Dat geldt zeker voor grote organisaties. Sommige organisaties hebben daarom inmiddels systemen in gebruik die hen ondersteunen bij het beheer van documenten, de zogenaamde document management systemen (DMS). Dit kunnen heel eenvoudige systemen zijn die slechts verwijzen naar papieren archieven maar ook systemen waarin de documenten of dossiers geheel digitaal zijn opgenomen. Deze systemen zijn vaak in staat om op onderdelen overzichten te genereren.

Positieve ontwikkelingen

De meeste ministeries hebben inmiddels vergevorderde plannen om hun hele informatievoorziening onder te gaan brengen in een DMS, al dan niet gecombineerd met een Record Management Applicatie voor het beheer van documenten op langere termijn. Sommige ministeries zijn inmiddels zelfs al met de implementatie bezig. Uit deze projecten blijkt ook steeds weer hoe belangrijk het is dat goed wordt nagedacht over de aansluiting bij de primaire processen. Een aantal ministeries betreft daarom op een vroeg moment 'de werkvloer' bij de inrichting van dergelijke systemen. Op die manier ontstaat er een informatievoorzieningsfunctie die optimaal gericht is op het ondersteunen van de dagelijkse werkzaamheden. Bovendien schept dit ook de mogelijkheid om de besluitvorming achteraf te reconstrueren, veel beter dan met archief dat aan de hand van een statische, vaak verouderde, classificatiecode is geordend. Naar ons oordeel blijft het overigens wel noodzakelijk om de met de werkvloer afgesproken dossiervorming en –ordening vast te leggen in een plan.

Bedrijfsapplicaties in kaart

Naast de documenten die binnen de kantoorautomatisering- en e-mailapplicaties worden beheerd, bevindt zich ook veel informatie in bedrijfsapplicaties.

Hier is het beeld positiever dan het beeld wat we op veel plaatsen van de kantoorautomatisering gekregen hebben. We hebben in de praktijk gezien dat een groot aantal organisaties een inventarisatie hebben gemaakt van alle bedrijfsapplicaties die operationeel zijn. Dit is deels gebeurd naar aanleiding van het speerpunt uit 2003 van de Rijksarchiefinspectie dat elke overheidsorganisatie over een bestandsoverzicht moest beschikken. Vaker komt het voor dat deze overzichten van oudsher bestaan bij ICT-afdelingen. In dat geval zijn de overzichten vanuit een ander doel opgesteld dan het inhoudelijk beheer van de informatie die zich in de systemen bevindt. Overigens kan een van oorsprong technische inventarisatie van alle applicaties ook helpen bij het inhoudelijke beheer van informatie. Dat hebben we gezien bij het ministerie van VROM.

Het ministerie van VROM bleek eind jaren negentig over een enorme hoeveelheid bedrijfsapplicaties te beschikken die op verschillende plaatsen in de organisatie beheerd werden. De diverse applicaties zorgden zelfs voor een technisch infarct, het netwerk kon al deze applicaties niet aan. Er is op dat moment besloten om rigouze te saneren en standaardisering aan te brengen. Toen de applicaties werden geïnventariseerd bleken het er 1601 te zijn. Er zijn nu nog maar 500 applicaties. Het plan voor de aanschaf van een nieuwe applicatie moet tegenwoordig langs een team dat de aanschaf beoordeelt. Hierdoor is veel beter na te gaan bij welke processen welke applicaties worden ingezet, en binnen welke applicaties archiefdocumenten beheerd worden. Een DMS / RMA kan tot nog meer samenhang van de informatie die binnen de applicaties gevormd wordt leiden en ertoe bijdragen dat documenten duurzaam bewaard blijven. VROM gaat een dergelijk systeem ook invoeren.

Conclusie: Overheidsorganisaties beheren hun digitale documenten op dit moment nog hoofdzakelijk in de kantoorautomatisering- en emailapplicaties. De ordening is zodanig dat er een groot risico bestaat dat na verloop van tijd documenten niet meer terug te vinden zijn. Beter zicht is er op de bedrijfsapplicaties binnen organisaties. Een positieve ontwikkeling zien we verder bij de ministeries, bij de ingebruikname van DMS'en en RMA's.

4.3 Documenten zijn niet juist meer te interpreteren

In de vorige paragraaf maakten we duidelijk dat de meeste organisaties op dit moment medewerkers vrij laten in het plaatsen van documenten in de kantoorautomatiseringsomgeving en op de exchangeservers. In deze paragraaf gaan we door op deze problematiek, en leggen we uit dat dit niet alleen gevolgen heeft voor de terugvindbaarheid van documenten, maar ook voor de mate waarin documenten zijn te interpreteren.

Is dit het document dat ik zoek?

Wat zouden dit voor documenten zijn: BP1GB.doc, probeersel.doc, RW1999.xl, prWIN.ppt?

De eerste twee documenten stonden op een persoonlijke schijf. Het derde en vierde document vonden we op de gezamenlijke schijf. De enige manier om achter de inhoud van de documenten te komen, is ze te openen. Maar wat zou er met het beleidsplan dat Gerda van Bohemen heeft gemaakt zijn gebeurd? Is dit een definitieve versie?

Zou het document ook in een papieren dossier zijn opgenomen, of elders in de digitale omgeving zijn opgeslagen? We weten het niet. En dat 'probeersel', dat ziet er toch echt uit als een definitieve versie van een brief, met briefnummer en al. De registratie van werklozen in het Excelbestand, waar werd die voor gebruikt? En dat powerpointbestand, wie zou dat beveiligd hebben? Wat is het wachtwoord?

Bovenstaande voorbeelden maken duidelijk dat documenten, als ze al gevonden zijn, maar een beperkte waarde hebben omdat metadata - de contextinformatie - ontbreken. Dit hebben we ook moeten constateren bij ons onderzoek naar de digitale erfenis van de Arbeidsvoorziening. Hoewel er uiteindelijk een grote hoeveelheid van dit soort bestanden bewaard is gebleven, zal de bruikbaarheid bij de verantwoording van het handelen van de Arbeidsvoorziening en (op een later moment) voor historisch onderzoek, beperkt zijn. We kunnen immers niet meer achterhalen welke rol de documenten hebben gespeeld binnen het werkproces. We hebben gezien dat deze problemen niet alleen bij de Arbeidsvoorziening voorziening spelen. Tijdens de quick scans⁴ zagen we regelmatig dat grote hoeveelheden documenten alleen nog digitaal in een Windowsomgeving werden opgeslagen, zonder dat er goede afspraken waren gemaakt over het toekennen van metadata.

De vraag welke metadata moeten worden toegekend aan documenten is in verschillende gremia en vanuit verschillende invalshoeken beantwoord. Hierover zijn verschillende standaards en modellen voor ontworpen⁵. We hebben ook vast kunnen stellen dat deze standaarden en modellen in de praktijk worden toegepast. De ministeries hebben een samenwerkingsverband INTERLAB, waarbinnen onder andere aan een kernmodel van softwarefunctionaliteiten voor DMS/RMA-applicaties wordt gewerkt. Zij denken ook over de toepassing van een metadatamodel binnen de applicaties. Dergelijke applicaties bieden goede mogelijkheden om metadata aan documenten toe te kennen en die metadata door de tijd zorgvuldig te beheren.

De juiste metadata toekennen in een kantoorautomatiserings- of e-mailomgeving is bijna ondoenlijk. Er zouden duidelijke afspraken gemaakt moeten worden over het toekennen van namen aan documenten en mappen en over de wijze waarop versies worden beheerd. Hierop zou bovendien controle nodig zijn. Maar dan nog blijft het risico bestaan dat de verkeerde metadata aan een document hangen. Tot de metadata behoort bijvoorbeeld ook wie een document gemaakt heeft, informatie die bij Worddocumenten automatisch wordt opgeslagen als eigenschap van documenten. Dat dit niet toereikend is, blijkt bij hergebruik van een document in Word-formaat. Dan blijkt dat als auteur de naam van de maker van het brondocument blijft staan en niet degene die het nieuwe document gemaakt heeft.

Gevaren bij conversie en migratie

In de voorgaande paragraaf bespraken we het nut en de noodzaak van organisatorische metadata. Het zal echter ook noodzakelijk zijn om over technische metadata te beschikken om documenten juist te interpreteren. Tijdens onze quick scans kwamen we een organisatie tegen die alle vitale informatie in een database had staan. De informatie die tegenwoordig in de database was opgenomen, was deels afkomstig uit een oudere database. Onze gesprekspartners deden uit de doeken

⁴ Zie voetnoot 1.

⁵ Dublin Core, metadatamodel ReMANO, concept ISO-standaard

hoeveel complicaties er waren opgetreden bij de migratie. Niet alle gegevens konden worden meegenomen en uiteindelijk was er veel handwerk aan te pas gekomen om de database te herstellen. Na veel problemen kon de organisatie weer aan het werk, maar bleef achter met de vraag welke gegevens de betrouwbare, authentieke gegevens waren en welke gegevens later, in het heetst van de strijd, handmatig waren toegevoegd.

Om die analyse achteraf te kunnen maken, waren behalve een zorgvuldige documentatie van het migratieproces ook technische metadata nodig geweest. Technische metadata zijn ook nodig om bijvoorbeeld vast te kunnen stellen of een document altijd al een Worddocument was, of dat het geconverteerd is uit Wordperfect. En als dat gebeurd is: staan de karakters dan nog wel op dezelfde plaats als waar de auteur ze ooit geplaatst heeft?⁶

Het ontbreken van systeemdokumentatie

Veel overheidsorganisaties werken met databases die speciaal zijn ontworpen ter ondersteuning van de eigen bedrijfsprocessen. Dit heeft als voordeel dat de applicaties precies zijn toegesneden op de wensen van de gebruikers. Er zijn echter ook belangrijke nadelen aan verbonden. Het onderhoud van deze applicaties is specifiek werk, wat veelal wordt uitgevoerd door de ontwerper van de database. Dit kan een medewerker zijn van een professioneel ICT-concern waaraan het beheer is uitbesteed, die ervoor zorgt dat zijn collega's zijn werk eventueel kunnen overnemen, maar ook een ICT-specialist met een eenmanszaak of een beleidsmedewerker die een handige database ontwerpt voor de ondersteuning van zijn eigen werkproces. In de laatste gevallen ontstaat er een probleem als de ontwerper ermee ophoudt en niet meer te traceren is. Ook bij een grote organisatie als de Arbeidsvoorziening kon het gebeuren dat een projectplan voor conversie thuis werd opgediept door een medewerker van het bedrijf waaraan de ICT-diensten destijds waren uitbesteed. Het is absoluut noodzakelijk om op een later moment nog over de systeemdokumentatie te kunnen beschikken. Dit is belangrijk voor het onderhoud, bij conversie en migratie, maar ook om de gegevens uit de database überhaupt nog te kunnen interpreteren. Wat de gegevens betekenen die in de velden zijn opgenomen, weet de ontwerper en de hedendaagse gebruiker van de database misschien, maar is dat tien jaar later ook nog zo voor de hand liggend?

Conclusie: Het 'mer a boire' van digitale overheidsdocumenten zal van beperkt nut blijken voor zowel de bedrijfsvoering, verantwoording en als informatiebronnen voor historisch onderzoek. Zonder contextinformatie (in de vorm van metadata en systeemdokumentatie), zal de status, authenticiteit en rol van de documenten binnen een proces namelijk onduidelijk blijven.

4.4 Gegevens worden te lang bewaard

Bij het onderwerp 'digitale duurzaamheid' gaat de aandacht in het algemeen uit naar de vraag of documenten of gegevens niet voortijdig verloren raken. Maar het tijdig kunnen vernietigen van documenten is ook een punt van aandacht, al is het maar uit beheersoogpunt. Geen organisatie wil de beschikbare schijf- en serverruimte meer

⁶ *Het Testbed digitale bewaring heeft een aantal onderzoeken uitgevoerd naar de authenticiteit van digitale archiefbestanden. De onderzoeksresultaten zijn in de publicatie 'Van digitale vluchtigheid naar digitaal houvast' opgenomen (vier delen). De publicatie is te raadplegen op www.digitaleduurzaamheid.nl.*

belasten dan nodig is. Maar er zijn ook andere redenen om tijdig te vernietigen en die behandelen we in deze paragraaf.

Privacy

In verband met de privacywetgeving mogen persoonsgebonden gegevens vaak niet langer bewaard worden dan noodzakelijk is voor de uitvoering van werkzaamheden⁷. Organisaties die veel te maken hebben met privacygevoelige informatie, hebben hier soms iets voor geregeld in de applicaties die zij gebruiken voor de uitvoering van de primaire processen. Bij de analyse van oude bestanden van de Arbeidsvoorziening zagen we echter dat er geen voorziening was getroffen voor de (automatische) vernietiging van bestanden in de belangrijkste applicatie voor het primaire proces. Maar het grootste probleem was dat de kantoorautomatisering talloze zeer privacygevoelige documenten bleek te bevatten, zoals reïntegratieadviezen. In het project voor het veiligstellen van de digitale erfenis bij de Arbeidsvoorziening is getracht deze informatie te filteren uit de bestanden met behulp van een zoekmachine. We hebben geconstateerd dat deze selectie achteraf niet optimaal is en tot zeer hoge kosten leidt.

Vernietigen conform archiefwetgeving

Ook als het geen privacygevoelige informatie betreft, is tijdige vernietiging wenselijk en noodzakelijk. We noemden al het punt van de beschikbare schijf- en serverruimte. Een ander punt is dat de archiefwetgeving tijdige vernietiging van documenten voorschrijft. We hebben in het project Arbeidsvoorziening vastgesteld dat een echt zorgvuldige selectie en tijdige vernietiging alleen mogelijk is door bij de ontvangst of creatie een bewaartermijn te koppelen aan de documenten ('selectie aan de bron'). In paragraaf 4.1 merkten we al op dat, een enkele uitzondering daargelaten, de organisaties die wij in de afgelopen jaren bezochten geen vernietigingstermijnen in hun documentgenererende en -beherende applicaties hebben opgenomen. Dit moet wel gebeuren als organisaties gaan werken met een DMS/RMA.

Conclusie: We zijn tijdens onze onderzoeken en inspecties vrijwel geen voorzieningen tegengekomen voor het tijdig vernietigen van (privacygevoelige) informatie in de KA- en e-mailomgeving.

4.5 Documenten raken onbedoeld in de openbaarheid

Onlangs was veel ophef over het feit dat een officier van Justitie zijn computer, die vertrouwelijke dossierinformatie bevatte, bij het huisvuil had gezet. Deze informatie lag letterlijk 'op straat'. Een lid van de Tweede Kamer merkte daarop op: 'Mensen maken fouten, maar de systemen zijn ook niet goed beveiligd'.

De archiefwetgeving geeft geen specifieke eisen voor informatiebeveiliging. Toch is het van belang om alle aspecten rond informatiebeveiliging goed te regelen, omdat digitale informatie nu eenmaal kwetsbaar is. Afstemming met de archiefwetgeving is hierbij belangrijk, omdat documenten soms langer bewaard moeten blijven dan vanuit het oogpunt van informatiebeveiliging wenselijk lijkt.

7

Overigens mogen ook persoonsgegevens in het algemeen uitsluitend vernietigd worden als deze ook in een wettelijk voorgeschreven selectielijst zijn genoemd.

Bij informatiebeveiliging draait het om het regelen van de technische en organisatorische randvoorwaarden. Het is in de eerste plaats noodzakelijk om een beveiligingsbeleid vast te stellen en verantwoordelijken aan te wijzen. ICT-beveiliging kent naast managementverantwoordelijkheden ook een persoonlijke verantwoordelijkheid. Daarnaast is het bijvoorbeeld belangrijk dat er een goed doordachte autorisatiestructuur wordt ingericht.

Het Kadaster heeft een beveiligingsbeleid en een handboek vastgesteld waarin bovengenoemde zaken uitgebreid aan de orde komen. Het Kadaster schrijft in het handboek: 'Het grootste deel van onze informatie wordt met behulp van ICT-toepassingen geproduceerd en beheerd. Het gebruik van computers, internet en dergelijke wordt nog steeds uitgebreid. Hierdoor nemen de bedreigingen voor de informatieverwerking toe. Computervirussen, hackers, en andere storingen en rampen zijn ook voor het Kadaster reële bedreigingen. De trend is dat de gevaren zich verder uitbreiden en steeds ernstiger en geraffineerder worden. Wij worden tegelijkertijd steeds kwetsbaarder voor deze bedreigingen, gezien de intensieve inzet van ICT: de toename van het gebruik van internet, laptops en werken op afstand.'

Het CWI heeft er op meerdere manieren voor gezorgd dat de informatie binnen de systemen beveiligd is. In de eerste plaats worden back-ups gemaakt volgens een vast protocol. In de tweede plaats is de computerruimte van het CWI op een aantal manieren beveiligd.

Ondanks het feit dat organisaties al deze maatregelen nemen gaat het in de praktijk nogal eens mis. Niet altijd zijn gemaakte afspraken bij iedereen bekend of worden ze nageleefd. Dat bleek al uit het voorbeeld van de officier van Justitie: hij heeft de harde schijf van zijn computer niet conform de afspraken door specialisten laten vernietigen. Uit dit voorbeeld werd duidelijk dat afspraken over zorgvuldig informatiebeheer niet alleen moeten gelden binnen de vier muren van een organisatie. Steeds meer ambtenaren werken thuis en beheren derhalve procesgebonden informatie op hun eigen PC.

Conclusie: Grote organisaties hebben veel aandacht voor informatiebeveiliging. Uit de praktijk blijkt echter dat de bestaande afspraken niet altijd in alle haarvaten van een organisatie zijn doorgedrongen.

5 Eilanden van informatie en kennis

Eén van onze gesprekspartners zei tijdens een quick scan: 'De techniek is het probleem niet. Overal is wel een technische oplossing voor te bedenken.' Wij zijn het ermee eens dat waar het probleem technisch is, het probleem ook technisch is op te lossen. Maar het probleem zit hem niet altijd in de techniek. Met technische oplossingen is daarom slechts een deel van de risico's uit te sluiten. Goed beheer van (digitale) informatie is voor een belangrijk deel een organisatievraagstuk. Daarom besteden we in dit hoofdstuk aandacht aan verantwoordelijkheden en bevoegdheden. We kijken hierbij vanuit het perspectief: hoe konden de genoemde risico's uit hoofdstuk 4 ontstaan?

5.1 Een oud probleem en nieuwe kansen

We zijn ons ervan bewust dat de risico's die we hiervoor beschreven hebben niet helemaal nieuw zijn. In de afgelopen decennia is de documentaire informatie losgeweekt van het primaire proces als een postzegel van een enveloppe. De traditionele DIV-afdelingen bewaarden documenten vaak om het bewaren, 'omdat dit van de Archiefwet moet'. In eerdere inspectierapporten signaleerden we al vaak dat beleidsmedewerkers zelf hun informatie op persoonlijke schijven en in bureauladen bewaarden om hun werk goed te kunnen uitvoeren en om zich te kunnen verantwoorden.

Het is noodzakelijk dat deze twee werelden weer bij elkaar komen, zodat niet alleen de individuele medewerkers hun werk kunnen doen en zich kunnen verantwoorden, maar de organisatie als geheel.

Professionele oplossingen voor digitaal informatiemanagement bieden deze kansen. Kansen die verloren gaan als iedereen zijn eigen taal vanuit zijn eigen vakgebied blijft spreken. Hier besteden we aandacht aan in de volgende paragraaf.

Conclusie: De DIV-functie is teveel losgeweekt van het primaire proces. Vanuit andere professies wordt een oplossing gezocht voor het informatievraagstuk.

5.2 Iedereen beschrijft processen...

Het beschrijven van bedrijfsprocessen is 'in'. Dat is begrijpelijk, want een proces is pas goed te managen als duidelijk is welke stappen daarbinnen worden gezet. Kwaliteitsmanagers zullen daarom in een organisatie altijd beginnen met een deugdelijke procesbeschrijving. Als processen geautomatiseerd worden - tot voor kort gebeurde dit vooral met routinematige processen zoals vergunningverlening - dan is het ook belangrijk dat alle processtappen in kaart zijn gebracht. Ook ICT-ers bekwamen zich daarom in procesbeschrijving en in de vertaling van processen naar functionele eisen voor een op een proces toegesneden programma. Documentaire informatiespecialisten beschrijven processen om in kaart te brengen welke informatie binnen een proces wordt gegenereerd. Op die manier kunnen zij controleren of de informatie in dossiers volledig is en kunnen zij een deugdelijke archiefordening opzetten. Om dezelfde reden worden er handboeken administratie ondersteuning geschreven met daarin procesbeschrijvingen.

...met hetzelfde doel

Op die manier is het goed mogelijk dat de processen van een organisatie vanuit drie of vier verschillende invalshoeken beschreven zijn, en allemaal met een eigen taal. Gevolg hiervan is, dat niemand elkaar meer echt verstaat terwijl iedereen het over

dezelfde processen heeft. De belangen lijken hierdoor tegenstrijdig ('jullie willen vanuit het archief zo'n inrichting, maar wij willen een systeem waarmee we ons werk goed kunnen doen'), maar zijn dit in de praktijk niet. Alle procesbeschrijvingen, die vanuit record management perspectief inclusief, zouden ertoe moeten dienen dat het primaire proces optimaal kan worden uitgevoerd en dat hierover achteraf verantwoording kan worden afgelegd. Het archief moet deze kwaliteiten ondersteunen. Alleen op die manier kan ook later een juiste reconstructie van het gebeurde plaatsvinden.

Procesbeschrijvingen en digitaal archief

Waarom besteden we in een rapport over digitaal archief nu aandacht aan procesbeschrijvingen? In de praktijk zien we dat het communicatieprobleem kan leiden tot verschillende oplossingen van hetzelfde probleem, met het gevolg dat niet voor een geïntegreerde oplossing wordt gekozen.

Binnen het ministerie van VROM werd bijvoorbeeld over twee applicaties gesproken voor het stroomlijnen van de afhandeling van Kamervragen. Over een workflowsysteem dat vanuit de ICT-afdeling werd ontwikkeld, en over een DMS/RMA met workflowtoepassing vanuit de centrale DIV-afdeling. Enkel een workflowsysteem verbetert weliswaar de lopende procesgang structureel, maar biedt geen goede waarborg dat de documenten die erin worden opgenomen ook na verloop van tijd leesbaar en op een juiste manier interpreteerbaar zullen zijn.

Binnen het DMS/RMA zullen de digitale documenten van het ministerie, mits de applicatie op een goede manier wordt ingericht en de juiste procedures van kracht zijn, op een juiste manier beheerd kunnen worden. Dit systeem heeft voor de workflow net zulke kwaliteiten als het systeem dat de ICT-afdeling in gedachten had voor de Kamervragenapplicatie.

Conclusie: Er bestaan vanuit diverse invalshoeken verschillende oplossingen voor het informatievraagstuk. Er is een nieuw fundamenteel probleem ontstaan doordat de oplossers niet, of in een andere taal, met elkaar communiceren.

5.3 De Archiefwet: een last of een lust?

We komen vaak het misverstand tegen dat een DMS / RMA alleen handig is voor 'het archief'. Alleen documentair informatiespecialisten snappen de inrichting van de dossiers binnen zo'n applicatie, omdat zij een eigen 'archiefferichte' beschrijving van processen hanteren. Maar, zoals we hiervoor reeds duidelijk maakten, het archief is geen op zichzelf staand belang, het archief moet ertoe dienen dat de organisatie optimaal kan werken. De archiefwetgeving verzet zich niet tegen deze opvatting, maar ondersteunt deze juist. Wij hebben tijdens onze onderzoeken en inspecties geconstateerd dat er een wereld is gewonnen als we duidelijk kunnen maken dat alle betrokkenen bij procesbeschrijving, kwaliteitsmanagement en informatie- en recordmanagement dezelfde taal spreken en uitgaan van dezelfde belangen.

Conclusie: De archiefwetgeving en 'archiefbelangen' worden gezien als een lastige 'extra' in plaats van ondersteuning bij professioneel informatiebeheer.

5.4 Onvoldoende professionaliteit

De ministeries beschikken over een professionele DIV-organisatie die kan helpen bruggen te slaan tussen de verschillende disciplines. Bij veel andere overheidsorganisaties ontbreekt het aan de nodige expertise en slagkracht op dit gebied. Er zijn medewerkers belast met de dagelijkse uitvoerende werkzaamheden op het gebied van het (klassieke) post- en archiefbeheer, zoals het registreren van documenten, het vormen van dossiers en het beheren van het semi-statisch archief. Afdelingen die zich hiermee bezig houden, ressorteren meestal onder een facilitaire dienst. Hierbinnen is weinig ruimte om invloed uit te oefenen op het informatiebeleid van een organisatie. Vanuit deze positie is het niet eenvoudig om de problematiek van het beheer van digitale informatie aan te snijden. Vaak is een dergelijke afdeling niet op de hoogte van het ICT-beleid dat is geformuleerd. Men kan bijvoorbeeld constateren dat bepaalde informatie niet meer ter registratie wordt aangeboden, maar weet niet dat dit het gevolg is van de invoering van een workflowsysteem elders in de organisatie. Van ICT hebben de meeste overheidsorganisaties de laatste jaren het belang onderkend. Daarover wordt beleid geformuleerd met een directe lijn naar het management. Voor archivarissen en DIV-medewerkers blijft niets anders over dan vanaf de zijlijn waarschuwen dat ook digitale informatie duurzaam beheerd moet worden, zoals we in de inleiding op dit rapport al constateerden. Bij organisaties waar de benodigde expertise ontbreekt, zal het 'verdampen' van digitale informatie misschien in het geheel niet gesignaleerd worden als structureel probleem (maar mogelijk wel als dagelijkse ergernis). Tijdens onze quick scans hebben we met regelmaat (vooral kleinere) organisaties bezocht waar dit inderdaad het geval is.

Conclusie: Het ontbreekt aan professionaliteit bij - met name - kleinere overheidsorganisaties om het informatievraagstuk op te lossen en soms zelfs om het te onderkennen.

6 Aanbevelingen

1. Het is noodzakelijk dat het management van overheidsorganisaties zelf de verantwoordelijkheid oppakt voor een betrouwbare digitale informatievoorziening, en deze niet overlaat aan uitvoerenden. De onderstaande aanbevelingen bieden handreikingen voor de sturing op betrouwbare informatievoorziening.
2. Randvoorwaarde voor een betrouwbare informatievoorziening binnen de overheid is de aanwezigheid van voldoende kennis en expertise op het gebied van ICT, DIV, kwaliteits- en procesmanagement. Samenwerking tussen de verschillende professies is het sleutelwoord om een gemeenschappelijk doel - namelijk optimale ondersteuning van de primaire processen - te bereiken. De in hoofdstuk 5 genoemde 'eilanden van informatie en kennis' moeten bij elkaar komen.
3. Het is vereist dat overheidsorganisaties in kaart brengen welke digitale archieven zij beheren, op welke plaatsen zij deze bedrijfsvoerings- en verantwoordingsinformatie bewaren en vast te stellen of dit daadwerkelijk de plaatsen zijn waar deze informatie beheerd zou moeten worden. Deze inventarisatie kan plaatsvinden aan de hand van procesbeschrijvingen.
4. Nadat duidelijk is waar procesgebonden informatie gevormd en beheerd wordt, is het noodzakelijk een beheersomgeving te creëren voor de informatiebestanden. Goede beheersafspraken moeten onderdeel uitmaken van deze gecontroleerde beheersomgeving. Een zorgvuldig ingericht en onderhouden DMS / RMA is met name bij grotere organisaties onontbeerlijk voor een betrouwbare informatievoorziening.
5. Het is noodzakelijk dat overheidsorganisaties bij de inrichting van een DMS / RMA goed nadenken over de toe te kennen metadata aan de documenten (zoals de ministeries op dit moment al doen in het project INTERLAB). Zonder goede metadata zijn documenten niet juist te interpreteren, waardoor de betrouwbaarheid van de beheerde informatie sterk afneemt. Het onderhoud van metadata is ook van essentieel belang om documenten op de korte en langere termijn terug te kunnen vinden.
6. Voor het uitvoeren van de privacywetgeving is het vereist dat overheidsorganisaties zich bewust worden van het feit dat zich ook in de kantoorautomatiserings- en e-mailomgeving privacygevoelige informatie bevindt. Om privacygevoelige informatie tijdig te kunnen vernietigen, is een gecontroleerde beheersomgeving vereist. Volledigheidshalve merken we hier op dat vernietiging van privacygevoelige informatie geoorloofd moet zijn op basis van een vastgestelde selectielijst.
7. We vinden het essentieel dat beheersafspraken over de bedrijfsvoerings- en verantwoordingsinformatie, waaronder afspraken over informatiebeveiliging, goed binnen de gehele overheidsorganisatie worden gecommuniceerd. Daarmee kan onder andere voorkomen worden dat gevoelige informatie letterlijk op straat komt te liggen.
8. We bevelen onze staatssecretaris aan de regelgeving te toetsen op uitvoerbaarheid en handhaafbaarheid en mogelijk (nieuwe) aandacht te besteden aan voorlichting over de regelgeving. Concrete aanbevelingen hierover zullen we de evaluatiecommissies

van de regelingen *Geordende en toegankelijke staat archiefbescheiden*, *Duurzaamheid archiefbescheiden* en *Bouw en inrichting archiefruimten en archiefbewaarplaatsen* doen. Wij zullen aan de regelgeving blijven toetsen en daarnaast de handhaafbaarheid in het oog blijven houden.

9. Naar ons oordeel is het noodzakelijk dat onze staatssecretaris voor Cultuur en de minister voor Bestuurlijke vernieuwing het thema duurzaam beheer van digitale overheidsinformatie vanuit hun politieke verantwoordelijkheid oppakken. Hierbij denken we onder andere aan het faciliteren van praktische ondersteuning voor organisaties die hun digitale erfenis willen veiligstellen of een actieve digitaliseringsslag willen maken.