gemeente Neder-Betuwe

Onderzoek & advies Informatiebeveiliging

(Nul meting)

Gemeente Neder-Betuwe

21 november 2011

Inhoud

1. Inleiding

Het voorliggende informatiebeveiligingsonderzoek is uitgevoerd door Nico de Vos-Schipper RI in opdracht van Berthie Roukens-Bogaards.

Het doel van de opdracht was vast te stellen wat het huidige niveau van informatiebeveiliging is en welke maatregelen er genomen moeten worden om de informatie beveiliging op orde te krijgen voor onder andere de invoering van Het Nieuwe Werken. .

Bij dit onderzoek is de Code voor Informatiebeveiliging gehanteerd (ISO 27001 / ISO 27002). Alle beveiligingsprogramma's binnen de overheid zijn gebaseerd op deze code en vormen daar deelverzamelingen van zoals bijvoorbeeld voor GBA, digitalisering van archieven (RODIN), rechtmatigheidsonderzoek (art 213), etc.

Er is gekeken wat de risico impact van inbreuk op vertrouwelijkheid, integriteit en beschikbaarheid van gegevens is op de continuïteit van de dienstverlening door de gemeente. Op basis van deze risico impact analyse is het Basis Beveiligingsniveau gedefinieerd. Dat heeft weer geleid tot een subset aan eisen uit de Code voor Informatiebeveiliging, waartegen de organisatie is onderzocht.

Op basis van de bevindingen is een aantal verbetermaatregelen benoemd die in een verbeterplan zijn opgenomen.

2. Samenvatting

Basis beveiligingsniveau
De informatiebeveiliging binnen de gemeente Neder-Betuwe is vanuit ICT met name gericht op de handhaving van continuïteit bij langdurige uitval, virusbeveiliging en netwerkbeveiliging en in minder mate op de bescherming van gegevens. Het grote probleem is, dat er bijzonder weinig structureel is vastgelegd wat betreft de processen en de controles daarop en dat het derhalve erg moeilijk zo niet onmogelijk is om na te gaan wat de werkelijke status van de beveiliging is.

In dit rapport komt naar voren dat de organisatie m.u.v. misschien het GBA niet werkelijk 'in control' is over de informatiebeveiliging. Derhalve voldoet de gemeente niet aan de eisen voor o.a. financiële rechtmatigheid (art 213) en de eisen voor het verkrijgen van een substitutiebesluit voor het digitaliseren van archieven (RODIN).

Omdat, zoals uit de eerste alinea blijkt, de belangrijkste zaken wel geïmplementeerd zijn, maar niet gedocumenteerd zijn, is het toch mogelijk om relatief snel (binnen 3 maanden) een basis niveau van beveiliging te bereiken door zaken te documenteren en controleerbaar te maken.

Dit kan worden aangepakt door eerst aandacht te geven aan het opzetten van een integraal informatiebeleidsplan en een ondersteunende informatiebeveiligingsorganisatie.
Vervolgens dienen de bestaande basisinformatiebeveiligingsmaatregelen geëvalueerd, waar nodig verbeterd en gedocumenteerd te worden. Verdere verbetermaatregelen kunnen worden opgenomen in een Verbeterplan. Deze komen daarmee 'in control' mits de uitvoering van het verbeterplan permanent op de agenda van het MT komt en wordt opgevolgd.

Bewustwording en preventie
De grootste bedreiging voor de veiligheid is in alle gevallen het eigen personeel, dat geldt ook voor de gemeente. Dat is altijd een vervelend onderwerp en wordt liefst vermeden, maar de geschiedenis leert dat fraude, diefstal en sabotage vrijwel altijd het werk is van eigen (ex-)medewerkers. De screening van personeel laat bij de gemeente te wensen over, maar is sowieso nooit meer dan een moment-opname. Immers het is altijd mogelijk dat medewerkers uit rancune of onder externe druk ongewenste handelingen verrichten. Dat geldt overigens niet alleen voor de gebruikers, maar ook voor de beheerders van de informatiesystemen. Dus ook de controleurs moeten gecontroleerd worden. Bovendien ontstaat door Het Nieuwe Werken een structuur van minder sociale controle op de werkplek, waardoor de kwetsbaarheid van de informatiebeveiliging toeneemt

Zonder een 'Stasi-cultuur' te willen invoeren is het wel belangrijk dat het bewustzijn over informatie-beveiliging toeneemt en dat medewerkers het melden als zij vreemd gedrag van collega's waarnemen of situaties ontdekken die een potentiële bedreiging vormen voor de informatiebeveiliging.

Een belangrijke preventieve maatregel is het documenteren van processen, het inbouwen van controles in de processen en het managen van wijzigingen in processen en de onderliggende informatiesystemen, dat wil zeggen: testen, borgen en documenteren. Door regelmatige management-rapportages, interne audits en doorlopende verbeteracties kan het huidige reactieve klimaat veranderen in een preventief klimaat en kan het 'oog hebben' voor informatiebeveiliging onderdeel worden van het normaal dagelijks handelen.

3. Risico impact analyse

Onderstaand onderzoek is gebaseerd op het SPRINT-model voor bedrijfsmatige risico-inventarisatie.

Waardering	Ernst	Schade (in € * 1000)
E	Bedrijfscontinuïteit in gevaar	>1.000
D	Zware schade	>100
C	Aanzienlijke schade	>10
B	Lichte schade	>1
A	Verwaarloosbaar	<1

Vertrouwelijkheid: waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Gevolgen van inbreuk op vertrouwelijkheid	Waardering					Opmerkingen
Concurrentieverlies	**A**					Niet van toepassing
Direct verlies van business	**A**					Niet van toepassing
Extern imago			**C**			Negatieve publiciteit Politieke consequenties
Extra kosten	**A**					De materiële schade t.g.v. van een vertrouwelijkheidsbreuk is zeer beperkt
Aansprakelijkheid		**B**				Schadeclaim van benadeelde partij
Interne moraal		**B**				Onder druk van negatieve publiciteit kan moraal tijdelijk beschadigd raken
Fraude		**B**				Gezien de achterlopende interne organisatie is er een beperkte kans dat kleinschalige fraude ongemerkt blijft
Management beslissingen	**A**					Niet van toepassing
Verstoring bedrijfsproces	**A**					Niet van toepassing
Overall rating			**C**			Hoogste waarde is bepalend

Integriteit: het waarborgen vat de volledigheid en vertrouwelijkheid van informatie en verwerking

Gevolgen van inbreuk op Integriteit	Waardering					Opmerkingen
Concurrentieverlies	**A**					Niet van toepassing
Direct verlies van business	**A**					Niet van toepassing
Extern imago			**C**			Negatieve publiciteit Politieke consequenties
Extra kosten	**A**					De materiële schade t.g.v. van een integriteitsbreuk is zeer beperkt
Aansprakelijkheid		**B**				Schadeclaim van benadeelde partij
Interne moraal		**B**				Onder druk van negatieve publiciteit kan moraal tijdelijk beschadigd raken
Fraude		**B**				Gezien de achterlopende interne organisatie is er een beperkte kans dat kleinschalige fraude ongemerkt blijft. De kans op fraude met uitgifte van identiteitsdocumenten is gezien de genomen maatregelen verwaarloosbaar
Management beslissingen		**B**				Het communiceren van foutieve informatie kan beslissingen van burgers en bedrijven beïnvloeden en politieke consequenties hebben.
Verstoring bedrijfsproces		**B**				Dubbel werk om fouten te hertellen
Overall rating			**C**			Hoogste waarde is bepalend

Beschikbaarheid: waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

Gevolgen van inbreuk op beschikbaarheid	Impact bij uitval					Opmerkingen
	1uur	1dag	3dgn	1wk	1mnd	
Concurrentieverlies						Niet van toepassing
Direct verlies van business						Niet van toepassing
Extern imago				X		Gemeenten hebben niet het imago van snelle dienstverlening maar de kans op kritische vragen in de Raad, met eventuele consequenties voor management en bestuur is groot
Extra kosten			X			Overwerk en externe inhuur om achterstand weg te werken
Aansprakelijkheid					X	Mogelijke vertragingen die klanten of bedrijven oplopen t.g.v. het uitblijven van vergunningen, subsidies of uitkeringen kunnen tot schadeclaims leiden.
Interne moraal			X			Alleen in geval van calamiteiten
Fraude			X			Omdat transacties handmatig afgehandeld gaan worden, is controle minder goed mogelijk.
Management beslissingen				X		Managementbeslissingen zijn meestal niet tijdkritisch.
Verstoring bedrijfsproces		X				Niet alle transacties kunnen handmatig worden verzorgd

4. Basis Beveiliging Niveau (BBN)

Gezien de Wet Openbaarheid Bestuur is alle gemeentelijke informatie openbaar met uitzondering van persoonsgebonden informatie (burgers en personeel).

Uit de risico impact analyse in het vorige hoofdstuk blijkt dat de impact van een vertrouwelijkheids-breuk of een integriteitsbreuk op de continuïteit van het bedrijf relatief gering is. Alleen imago en bestuur leiden er onder.
Dien ten gevolge is het ook niet nodig om meer dan de algemeen gebruikelijke maatregelen te nemen voor bescherming van de toegang tot informatie, zoals:

- Autorisatiecontrole op gebruik van netwerk, applicaties en gegevens
- Virusbescherming
- Fysieke toegangsbeveiliging.

Het afbreukrisico van het niet beschikbaar zijn van informatie is groot gezien het feit dat vrijwel alle transacties alleen nog maar geautomatiseerd afgehandeld kunnen worden en de dienstverlening aan de burger bij gemis hieraan dien ten gevolge vrijwel stil komt te liggen. Grote aandacht dient er dus te zijn voor:

- Back-up en restore procedures (o.a. tests)
- Uitwijkplannen en tests

Op organisatorisch niveau moet er een beveiligingsbeleidsplan zijn, een gedocumenteerd beveiligingshandboek met daarin het stelsel van geïmplementeerde beveiligingsmaatregelen en een in een beveiligingsorganisatie belegde Plan–Do–Check–Act cyclus voor de uitvoering, controle en verbetering van die maatregelen.

Extra maatregelen boven de gecombineerde eisen van het GBA en van het RODIN (**R**eferentiekader **O**pbouw **D**igitaal **IN**formatiebeheer) van het Landelijk Overleg van Provinciale Archiefinspecteurs zijn niet nodig.

6. Onderzoeksresultaten

De informatiebeveiliging is geaudit tegen het Basis Beveilgingsniveau zoals bedoelt in hoofdstuk 4. De resultaten bevinden zich hieronder.

6.1. Documentatie

Constatering
- Alle documentatie met betrekking op informatiebeveiliging is onbeheerd, niet bestaand of onvindbaar. Er is geen centrale bibliotheek of beheerder, het is onduidelijk wat de laatste versie van een document is of wie dat document geautoriseerd heeft. Medewerkers handelen routinematig hun werkzaamheden af en zijn vaak niet in staat om de beschrijving van die werkzaamheden boven tafel te halen.

Risico
- Dit heeft een negatieve impact op de kwaliteit van dit onderzoek en in de inzichtelijkheid en overdracht van werkzaamheden, taken en verantwoordelijkheden. Behalve op een deelgebied als GBA is het geheel feitelijk niet goed auditeerbaar. Dit staat het verkrijgen van een substitutiebesluit voor het mogen vernietigen van archiefstukken alsmede het verkrijgen van een goedkeurende verklaring van de accountant in de weg.

NB Bij GBA moet overigens de kanttekening gemaakt worden dat er maar 1 persoon is die geautoriseerd is voor toegang tot de documentatie, die zich op een externe website bevindt.

Mogelijke verbetermaatregelen
- Opzetten van een kwaliteitssysteem voor informatiebeveiliging waarin alle actuele procedures en documenten zijn opgenomen die beschikbaar zijn.
- Opzetten van een beheerstructuur voor een documentatiesysteem voor informatiebeveiliging inclusief en procedures voor versiebeheer, autorisatie en distributie.

6.2. Beveiligingsbeleid en -organisatie

Constatering
- Een recent geautoriseerd beleidsplan voor een integraal beveiligingsbeleid ontbreekt. Er is wel een themagericht informatiebeleidsplan voor GBA en reisdocumenten, dat alleen bij de teamleider van de Gemeentewinkel en de ICT-coördinator bekend is.
- Het informatiebeveiligingsbeleid is geen regelmatig terugkerende punt op de agenda van het management en staat als zodanig dan ook niet bij het management op het netvlies.
- Er is geen informatiebeveiligingsorganisatie zoals bedoeld is de Code voor Informatiebeveiliging.

Risico
- De informatiebeveiliging heeft niet die aandacht van het management die nodig is voor een goede handhaving. Dit vormt een latente bedreiging voor de dienstverlening aan de burger en voor de bescherming van diens privacy. Dit maakt de gemeente bestuurlijk en politiek kwetsbaar.

Mogelijke verbetermaatregelen
- Opstellen van een integraal informatiebeleidsplan en inrichting van een informatiebeveiligings-organisatie om de continue aandacht voor de beveiliging en de verbetering te borgen.

6.3. Personele beveiliging

Constateringen
- Noch in functiebeschrijvingen, noch in arbeidscontracten wordt aandacht besteed aan beveiliging. Wel wordt overwogen om dat bij de invoering van HR21 (VNG) mee te nemen. Eventuele invoering is niet voorzien eerder dan de 2e helft van 2012.
- De diepgang van de screening van personeel vindt gevoelsmatig plaats, niet op basis van vastgelegd beleid. Alleen voor gevoelige functies worden sinds 2009 referentiechecks gedaan en wordt een VOG gevraagd. Diploma's en certificaten worden nooit gecontroleerd. Wel wordt uiteraard altijd de ID gecontroleerd.
- Sinds 2009 is het tekenen van een geheimhoudingsverklaring verplicht. Medewerkers van voor 2009 hebben dat dus niet gedaan.
- Er worden geen beveiligingstrainingen gegeven.

Risico
- De kans op het binnen halen van fout personeel is aanwezig.

Mogelijke verbetermaatregelen
- Opstellen van gebruikersprofielen voor toegang tot informatie en profielen aan koppelen aan de functies en personen (beveiligingsmatrix).
- Iedereen die dat nog niet gedaan heeft alsnog een geheimhoudingsverklaring laten tekenen.
- Screening nieuwe medewerkers verbeteren
- Organiseren beveiligingsbewustwordingstrainingen voor alle medewerkers.

6.4. Fysieke beveiliging

Constateringen

<u>Algemeen</u>
- Intern en extern personeel krijgt een zgn. druppel (toegangsbatch) voor toegang tot de gebouwen (en de printers). Leveranciers worden in principe begeleid door een medewerker.
- Er is een aanwezigheidsregistratiesysteem, BigBen, dat de uren registreert van intern personeel middels het in- en uitchecken met de toegangsbatch. De uren van externe medewerkers worden niet gecontroleerd

<u>Kesteren</u>
- De fysieke beveiliging van kantoor Kesteren is nihil. Voor- en achterdeur staan open en zeker aan de achterzijde, 'de rokershoek', kan iedereen vrij in en uit. Vooral op vrijdag is er weinig bezetting en kan men lang onopgemerkt blijven.
- Back-up tapes en ongebruikte computerapparatuur liggen opgeslagen in de ruimte van ICT. Deze ruimte gaat op slot, maar naast ICT-personeel hebben ook de schoonmakers daar toegang toe. Daar schoonmakers onder de categorie personeel vallen die niet gescreend wordt door PZ, wordt hier dus een potentieel risico gelopen.

<u>Ochten</u>
- De fysieke beveiliging bij kantoor Ochten bestaat uit een receptioniste en na openingstijd een batchreader.

<u>Opheusden</u>
- Er is geen plan voor de fysieke beveiliging van de het nieuwe kantoor.

Risico
- In de praktijk kan iedereen die dat onopvallend doet relatief eenvoudig zijn gang gaan in het tijdelijke kantoor in Kesteren, zeker op vrijdag als de bezetting minimaal is. Het uitblijven van een sluitend plan voor de beveiliging van Opheusden (scheiding burgers / personeel, afhandeling

leveranciers) maakt het mogelijk dat de huidige ongedisciplineerde situatie in Kesteren straks gemeen goed wordt in Opheusden.

Mogelijke verbetermaatregelen
- Zorg er voor dat de achterdeur van Kesteren dicht is en alleen met de druppel open kan.
- Sla back-up tapes op in een kluis of extern.
- Zorg voor een sluitend beveiligingsplan voor Opheusden.

6.5. ICT beveiliging

6.5.1. Autorisatie

Constateringen
- Op netwerkniveau kan geconstateerd worden dat het autorisatiesysteem werkt, maar een heldere beschrijving van hoe het werkt ontbreekt of kon niet worden teruggevonden.
- Voor een nieuwe medewerker bepaalt de desbetreffende manager wie op basis van zijn/haar functie tot welke applicatie en welke gegevens toegang krijgt. Systeembeheer zorgt vervolgens voor toegang tot de applicatie via het netwerk. Applicatiebeheer zorg voor toegang tot de gegevens.
- Als medewerkers weggaan is de omgekeerde procedure van toepassing, echter de discipline is niet van dien aard dat dit ook in alle gevallen gebeurt.
- De USB-poorten op de PCs zijn open, waardoor het kopiëren van informatie eenvoudig mogelijk is.
- Als een PC ongebruikt staat valt hij na enkele minuten uit en is opnieuw inloggen noodzakelijk.
- Gebruikerswachtwoorden voor toegang tot het netwerk vervallen om de 3 maanden en kunnen dan een jaar lang niet hergebruikt worden.
- Op gegevensniveau zijn geen autorisatiemaatregelen genomen anders dan die rechtstreeks aan de applicatie gekoppeld zijn. Voor een algemene applicatie als Decos (centraal archief) betekent dit dat als men eenmaal toegang heeft tot de applicatie men doorgaans bij meer informatie kan dan voor de functie nodig is. Interessant is te weten dat ook de GBA van de vorige dag in Decos staat, terwijl er voor het GBA strenge veiligheidseisen zijn.

Risico
- Ongeautoriseerde toegang tot gegevens is mogelijk door gebrek aan beheer en discipline enerzijds en gebrek aan beveiligingsbewustzijn anderzijds. Bovendien is het mogelijk om informatie via USB-sticks te vervreemden.

Mogelijke verbetermaatregelen
- Documenteren van procedures.
- Opstellen beveiligingsprofiel per functie.
- Herzien van autorisatie procedures.
- Trainen van managers en andere verantwoordelijken.

6.5.2. Antivirus

Constateringen
- Niet op alle PCs zit een virusscanner
- Het is op PCs mogelijk om USB-sticks in te voeren.
- De update van de virusscan verloopt automatisch, maar er vindt geen structurele controle plaats of de update succesvol gelopen heeft.

Risico's
- De actualiteit van de virusscan kan ongemerkt achterlopen met alle gevolgen van dien.
- Het is theoretisch mogelijk om via PCs mte open USB-poort en zonder virusscanner foute software te importeren.

Mogelijke verbetermaatregelen
- Vastleggen en verbeteren van het proces en de implementatie daarvan. Controles uitvoeren en loggen.
- USB-poorten afsluiten.

6.5.3. Firewall

Constatering
- Er is een dubbele Sonic firewall geïmplementeerd. In principe wordt deze automatisch geupdate, maar er vindt geen structurele controle plaats op het succesvol verloop van de update.

Risico
- De actualiteit van de firewall kan ongemerkt achterlopen.

Mogelijke verbetermaatregelen
- Vastleggen en verbeteren van het proces en de implementatie daarvan. Controles uitvoeren en loggen.

6.6. Incident-, probleem- & verandermanagement ICT

Constatering
- Er zijn geen procedures voor incident-, probleem- en verandermanagement in de OTAP-omgeving (OTAP = Ontwikkel, Test, Acceptatie, Productie).
- Beveiligingsincidenten krijgen geen structurele aandacht en de acceptatie van wijzigingen in de informatie-infrastructuur (hardware, software, processen) vinden niet volgens een vast test- en acceptatieprotocol plaats. Ook voor het verwijderen van oude hardware is er geen protocol.

Risico's
- Problemen worden niet opgelost, verbanden tussen problemen blijven onzichtbaar en ondeugdelijke componenten in de informatie-infrastructuur kunnen worden geïmplementeerd of goede componenten kunnen ondeugdelijk worden geïmplementeerd.
- Onderling strijdige wijzigingen kunnen worden aangebracht.

Mogelijke verbetermaatregelen
- Implementeren ITIL procedures voor incident, problem & change management in het verlengde van lopende Topdesk-implementatie, alsmede de implementatie van de bijbehorende beheerorganisatie.
- Opstellen van acceptatieprotocollen voor software, hardware en diensten (inclusief het toetsen van contracten).
- Opstellen van verwijderingprotocollen voor oude hardware, met name van opslag media.

6.7. Continuïteitsmanagement

6.7.1. Back-up & restore

Constateringen
- Dagelijks vindt zowel voor de Windows-omgeving als de AS400-omgeving (door Buren) een back-up plaats van alle mutaties. Wekelijks vindt een volledige back-up plaats. De tapes van de Windows back-up worden Kesteren bewaard en die van Buren worden extern bewaard
- De opslag van Windows back-up tapes in Kesteren is niet waterdicht, zie ook bij Fysieke Beveiliging. Bovendien worden ze niet planmatig getest op bruikbaarheid.

Risico

- Er bestaat een risico dat bestanden in de Windows-omgeving niet adequaat hersteld kunnen worden, ontvreemd worden of gemanipuleerd worden. Daar zich hier ook de back-up van het DMS onder bevindt is dit een ernstige tekortkoming.

Mogelijke verbetermaatregelen
- Planmatig testen van Windows-back-up tapes.
- Verbeteren van de opslag.

6.7.2. Uitwijk

Constateringen
- Er is een gedocumenteerd uitwijkplan voor de AS400 (CiVision, GBA). Hoe actueel dit plan is, is vanaf het document niet vast te stellen. Bewijzen van een uitwijktest in 2011 zijn er wel en de resultaten zijn goed. Let wel dat gemeente Buren hier de regie over voert.
- Uitwijk van de KA-omgeving is volgens de ICT coördinator wel geregeld en getest te samen met de AS400-uitwijk, maar hiervan is geen gedocumenteerd bewijs.
- De dataverbinding met de buitenwereld is niet dubbel uitgevoerd, maar er is een goed contract met de provider dat voorziet in reparatie binnen 24 uur. De praktijk heeft aangetoond dat dit werkt.

Risico
- De Windows-uitwijk is niet auditeerbaar door het gebrek aan documentatie en staat hiermee een mogelijke goedkeurende verklaring voor een substitutiebesluit in de weg, immers Decos maakt deel uit van de Windows-omgeving. Gebrek aan documentatie maakt de uitwijk exercitie lastig herhaalbaar en verbeterbaar.

Mogelijke verbetermaatregelen
- Documenteren van een uitwijkplan voor de Windows-omgeving.

6.7.3. Noodstroomvoorziening

Constatering
- Nieuwe noodstroomvoorziening in Opheusden is opgeleverd en werkt naar wens.

Risico
- Geen

Mogelijke verbermaatregelen
- Testprocedures vastleggen en tests plannen, uitvoeren en documenteren.

7. Verbeterprojecten

7.1. Verkrijgen van het basisniveau van beveiliging

De onderstaande stappen moeten worden doorlopen om 'ín control' te komen van de informatie-beveiliging. Pas als dit is gebeurd, is het zinvol om op te gaan voor een substitutiebesluit.

Stap 1: Ontwikkel Informatiebeveiligingsbeleidsplan en beveiligingsorganisatie

Definiëren integraal beveiligingsbeleid in een Informatiebeveiligingsbeleidsplan. Dit moet in ieder geval bevatten:

1. Doelstelling, principes en reikwijdte
2. Intentieverklaring van management ter ondersteuning van de doelstelling en de principes
3. Toelichting op punt 1 met verwijzing naar:
    - wettelijk verplichtingen (o.a. refereren aan GBA, BAG, RODIN, art 213a, etc.)
    - eisen beveiligingstraining
      - het voorkomen / onderkennen van kwaadaardige software en computercriminaliteit
    - continuïteitsmanagement
    - consequenties van het niet naleven van het beveiligingsbeleid (zie risico impact analyse)
4. Beschrijving van verantwoordelijkheden / beveiligingsorganisatie / beheer-, beoordelings en verbetercyclus (globale beschrijving met details in een te ontwikkelen beveiligingshandboek)
5. Verwijzing naar beleidsondersteunende documentatie

Stap 2: Ontwikkel Informatiebeveiligingshandboek

Dit handboek is in feite het kwaliteitssysteem voor beveiliging en bevat de (proces)beschrijving van de verschillende controle en beheer maatregelen. De ontwikkeling van het handboek gaat samen met de implementatie van de daarin beschreven maatregelen, die onderwerp zijn van het op te zetten Verbeterplan Informatiebeveiliging.
Het geeft inzicht in hoe de manier waarop het beveiligingsbeleid en de onderliggende normen vertaald zijn in concrete maatregelen. Tijdens toekomstige audits zou het moeten volstaan om te toetsen of de inhoud van dit boek voldoet aan de gestelde normen van de diverse auditerende instanties en of er bewijs van is dat dit boek wordt nageleefd.

Het handboek voor GBA zou als voorbeeld kunnen dienen, maar het is verstandiger om de hoofdstukindeling van de Code voor Informatiebeveiliging hierbij aan te houden te beginnen met het managementproces.
Detail beschrijvingen van processen kunnen het best in bijlagen worden opgenomen om de leesbaarheid en beheersbaarheid van dit document te vergroten. Bestaande documenten zoals het uitwijkplan AS400 kunnen dan eenvoudig onderdeel van het handboek worden.

Stap 3: Opstellen Verbeterplan Informatiebeveiliging

Het Verbeterplan geeft aan welke verbeteringen voor de informatiebeveiliging men heeft onderkend en onder handen gaat nemen (inclusief plandatums en prioriteiten).

De oplossingen voor de in dit onderzoek gevonden hiaten moeten worden geprioriteerd en ingepland. De hoogste prioriteit hebben in dit kader alle zaken die samen het Basis Beveiligingsniveau vormen:

- Opstellen fysieke beveiligingsplan Opheusden
- Evalueren uitwijkprocedure AS400
- Evalueren en beschrijven uitwijkprocedure KA/Windows omgeving
- Idem back-up & restore procedures KA/Windows omgeving
- Idem autorisatieproces voor netwerk, applicaties en gegevens
- Idem antivirus updateprocedures
- Idem firewall updateprocedures

Onder evalueren wordt ook verstaan evalueren van leverancierscontracten voor ondersteunende diensten.

7.2. Continue verbetering

De overige in het Verbeterplan op te nemen projecten zijn onderdeel van de reguliere continue verbetering en kunnen na het aanvragen van substitutiebesluit plaatsvinden. Deze projecten zijn:

Reactief en proactief incident management
Log opzetten voor melding beveiligingsincidenten en zwakke punten in de beveiliging almede het organiseren van de actieve opvolging daarvan incl. de managementrapportage, terugkoppeling aan de melder, het implementeren van de verbetermaatregel en het nemen van eventuele disciplinaire maatregelen.

Awareness training
Organiseren regelmatige awareness campagnes en trainingen op het thema informatiebeveiliging. Eventueel een awarenesstoets afnemen

Verbeteren profielen en autorisatieprocedure
Opstellen informatieprofielen voor medewerkers of medewerkergroepen. Deze profielen moeten aangeven wie welke applicaties mag gebruiken en wie welke informatie mag toevoegen, inzien, muteren of verwijderen. Autorisatie van medewerkers via P&O laten lopen op basis van profiel.

Verbeteren screeningsprocedure voor medewerkers met directe of indirecte toegang tot informatie
Aanvragen VOG en checken referenties en voor de functie relevante diploma's of certificaten tot standaard maken voor alle nieuw aan te nemen medewerkers en externen.

Alle medewerkers en externen die dat nog niet gedaan hebben, moeten alsnog een geheim-houdingsverklaring tekenen.

Opzetten verandermanagement voor applicaties en technische infrastructuur
Definiëren van test en acceptatieprotocollen voor wijzigingen in de informatie infrastructuur. Opzetten van een verandermanagement organisatie die o.a. tot doel heeft om elkaar beïnvloedende wijzigingen te coördineren..