Ter info

(AB)

Afdeling:	Beh.door:	Port.houder:
Team: Bedrijfsbureau	Bos, M.G.	DB,

Agendapunt 7f
van de vergadering van het Algemeen Bestuur
van 18 december 2015.

Memo Informatiebeveiliging

Inleiding

Met de toegenomen digitalisering van onze samenleving vormen cybercrime en andere inbreuken op de informatieveiligheid steeds grotere bedreigingen voor burgers, bedrijven en publieke organisaties. Een reeks kleine en grote incidenten in het recente verleden hebben de wereld en Nederland bewust gemaakt van de grote gevolgen die dergelijke incidenten kunnen hebben. Ook wordt steeds duidelijker dat geen enkel individu of organisatie zich in deze tijd immuun kan wanen voor incidenten op het gebied van de veiligheid van informatie.

De waterschappen hebben op 22 maart 2013 in de Ledenvergadering van de Unie van Waterschappen ingestemd met het voorstel om zelfregulering voor de waterschappen te realiseren. Daarbij is voorgesteld om een nulmeting uit te voeren, een visie op zelfregulering uit te werken en een programmaplan op te stellen voor de realisatie van de zelfregulering omstreeks begin 2015.

Er zijn afspraken gemaakt om een baseline informatiebeveiliging waterschappen (BIWA) en een gezamenlijk kwaliteitsniveau van de beveiliging van fysieke objecten en digitale informatie voor de waterschappen te realiseren. De baseline bestaat uit twee delen en is gebaseerd en afgestemd op de baselines van de gemeenten (BIG) en het Rijk (BIR). Het eerste deel is een strategisch kader en het tweede deel een tactisch kader. De baseline bevat maatregelen die algemeen voorkomende informatiebeveiligings-risico's bij de waterschappen afdekken. Het bevat een aantal minimale beveiligingsniveaus waaraan een waterschap zou moeten willen voldoen. Voor risico's die niet door de baseline zijn afgedekt dient het management van het waterschap aanvullende maatregelen vast te stellen.

Hefpunt is als uitvoeringsorganisatie voor drie waterschappen werkzaam op het terrein van belastingheffing en –invordering. Zij conformeert zich aan het hiervoor geschetste beleid van de waterschappen en ziet de BIWA als het normenkader voor de informatiebeveiliging. Voor ICT voorzieningen wordt daarbij gebruik gemaakt van de diensten van de waterschappen.

Wat wordt verstaan onder informatiebeveiliging

Informatiebeveiliging is het managen van de risico's die samenhangen met informatieverwerking en het gebruik van ICT-systemen door het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van die informatie en systemen. Hieronder wordt verstaan:

- Beschikbaarheid: de mate waarin gegevens of functionaliteit beschikbaar zijn wanneer ze nodig zijn: er voor zorgen dat systemen en informatie, die cruciaal zijn voor de uitvoering van dagelijkse werkzaamheden of ten tijde van een crisissituatie, beschikbaar zijn.
- Integriteit: de mate waarin men kan vertrouwen op de juistheid van gegevens en men zeker weet dat gegevens en systemen niet gemanipuleerd zijn door kwaadwillenden.
- Vertrouwelijkheid: de mate waarin toegang tot gegevens beperkt is tot degenen die bevoegd zijn deze ook in te zien (bijvoorbeeld bij privacygevoelige informatie of vertrouwelijke gegevens over de organisatie).

Het managen van de risico's rondom informatieveiligheid vraagt om maatregelen in:

- Fysieke toegangsbeveiliging (maatregelen om ongewenste toegang tot kantoren en apparatuur te voorkomen).

- Personele en organisatorische/procedurele sfeer (bijvoorbeeld regels omtrent bevoegdheden voor toegang tot systemen) en bewustwording bij bestuur en medewerkers.
- ICT technische beveiliging (bijvoorbeeld beveiliging van het netwerk, het afdwingen van complexe wachtwoorden).

Ofwel mens-, organisatorisch- of technische gerichte maatregelen.

Informatieveiligheid gaat zowel over de beveiliging van kantoorautomatisering (met gegevens van Hefpunt, bestuurlijke informatie en persoonsgegevens) als de basisregistraties en de kernregistraties voor heffen en invorderen. Het heeft betrekking op alle informatie die onder verantwoordelijkheid van Hefpunt valt. Ondanks dat de zorg primair bij Hefpunt ligt, zijn ook de moederorganisaties mede verantwoordelijk voor veiligheid van de gegevens bij Hefpunt. Belangrijke uitgangspunten zijn:

- Informatieveiligheid is gericht op het beveiligen en beschermen van die zaken die echt beveiligd moeten worden, niet minder maar ook niet meer. Beveiliging is geen doel op zich.
- Informatieveiligheid leidt niet tot onnodige bureaucratie en een ‘papieren vinkjescultuur’. Het belangrijkste is dat het niveau van veiligheid aantoonbaar wordt verhoogd.
- Informatieveiligheid is niet enkel een ICT-aangelegenheid, maar een integraal onderdeel van de bedrijfsvoering.

Informatiebeveiligingsbeleid bij Hefpunt

Hefpunt neemt een groot deel van haar ICT-diensten af van NZV. Dit is een belangrijke overweging geweest in het besluit om Hefpunt te laten meeliften in het project Informatiebeveiliging bij NZV.

De algemene uitgangspunten en principes hierbij voor Hefpunt zijn:

1. De focus ligt op het borgen van beschikbaarheid en de kwaliteit van informatie.
2. IB is een organisatie brede aangelegenheid en betreft zowel digitale als analoge informatie en kennis bij de medewerkers.

a. De manager is verantwoordelijk voor het op orde hebben van de informatiebeveiliging in zijn/haar proces.
b. De bedrijfsprocessen bepalen welke eisen er ten aanzien van de informatie en gegevens nagestreefd dienen te worden.
c. Hefpunt deelt de gegevens. Deze gegevens zijn kwalitatief goed en het delen is adequaat geregeld.

d. Alle gegevens en informatie is vrij beschikbaar zonder tussenkomst van medewerkers, mits dit vanuit vertrouwelijkheid toegestaan is.
e. In elk project of informatieplan wordt stil gestaan bij informatiebeveiliging. Daarbij is speciale aandacht voor de beschikbaarheid- en integriteitsborging van informatie.
f. Hefpunt conformeert zich aan door de waterschappen geaccordeerde Baseline Informatiebeveiliging Waterschappen (BIWA). Hiermee voldoet Hefpunt automatisch aan de ISO-27001 en 27002 standaarden. Hefpunt hanteert de BIWA alsof het een “pas toe of leg uit” standaard is.

Plan van aanpak

De eerste twee stappen zijn inmiddels uitgevoerd te weten een nulmeting analyse t.o.v. de BIWA (GAP-analyse) en een risico-inventarisatie (A&K-analyse, afhankelijkheid en kwetsbaarheid). Dit heeft geleid tot een plan van aanpak waarin de uitkomsten van de GAP-analyse zijn vastgelegd en waarbij maatregelen worden voorgesteld om te voldoen aan de gestelde eisen. In de risico-inventarisatie zijn de meest kritische informatiesystemen in beeld gebracht als het gaat om informatiebeveiliging. De te nemen maatregelen hiervoor zullen nog nader moeten worden uitgewerkt.

Maatregelen GAP-analyse

De maatregelen uit de GAP-analyse zijn gerubriceerd naar hoog (binnen één jaar), midden (binnen twee jaar) en laag (voorlopig niet, alleen als er tijd is). Om aansluiting te houden met de BIWA, zijn de maatregelen specifiek gemaakt en gekoppeld aan de eisen uit de BIWA. Per maatregel is aangegeven wie actiehouder is en wanneer een maatregel moet zijn uitgevoerd.

A&K analyse

Een A&K analyse brengt de afhankelijkheid en kwetsbaarheid van de belangrijkste informatiesystemen in beeld. In totaal zijn alle 30 informatiesystemen van Hefpunt beoordeeld. Naast beschikbaarheid, integriteit en vertrouwelijkheid (BIV) is tevens gescoord op imago/politiek. Per onderdeel is gescoord tussen 1 en 4. In totaal hebben 7 systemen een score van 11 of meer punten. Deze systemen zijn voor IB als meest kritisch aangemerkt.

Scope en afbakening

Naast enkele generieke zaken wordt bij de uitvoering van het maatregelenpakket vooralsnog gekeken naar de meest kritische informatiesystemen (zie hiervoor). Omdat informatievoorziening continu in beweging is, zal jaarlijks doch minimaal tweejaarlijks de risico-inventarisatie herhaald worden.

Planning

De planning is er op gericht om uiterlijk eind 2017 te voldoen aan de gestelde eisen uit de BIWA.

Financiën

De insteek is het project zoveel als mogelijk met eigen capaciteit en de ondersteuning van NZV te draaien. Mocht er toch gebruik worden gemaakt van externe ondersteuning dan zal dat zeer beperkt zijn en vooraf worden overlegd.

Communicatie

Het MT en DB van Hefpunt zal op basis van een halfjaarlijkse voortgangsrapportage worden geïnformeerd.