Informatieveiligheid 2016 – 2017

Eerste voortgangsrapportage

John Visbeen
Provincie Utrecht
Januari 2017
Doc.nr. 81A4C216

Inhoud

1.0 Inleiding

De **beschikbaarheid integriteit en vertrouwelijkheid** in informatie betreffen de kwaliteit van informatievoorziening. Het is belangrijk dat informatie niet in verkeerde handen valt door bijvoorbeeld externe dreigingen, zoals hacking, ddos aanvallen, of door interne menselijke fouten. Verder is van belang dat de gegevens juist, accuraat en beschikbaar zijn op het moment dat dit nodig is. Daarom hebben de provincies gezamenlijk afspraken gemaakt over informatieveiligheid en dit vastgelegd in het "**Convenant interprovinciale** regulering informatieveiligheid" uit 2014 (hierna: convenant).

Op 9 december 2014 hebben Gedeputeerde Staten van de provinciale Utrecht ingestemd met dit convenant en is gestart met het project Informatieveiligheid. Op basis van het convenant heeft herijking van het Beleid informatieveiligheid plaatsgevonden. In 2015 en 2016 is eigen onderzoek gedaan en heeft een onderzoek van de Randstedelijke Rekenkamer plaatsgevonden. Als rode draad door de bevindingen en aanbevelingen door beide onderzoeken loopt dat:

- het besef van urgentie op het gebied informatieveiligheid verbeterd moet worden in de organisatie.
- Door middel van rapportages meer inzicht moet worden geboden in de status van de informatieveiligheid maatregelen en borging in P&C cyclus.

Als uitwerking van het beleidsplan en om de aanbevelingen uit eigen onderzoek en het onderzoek van de Rekenkamer op te volgen, is het Plan van Aanpak Informatieveiligheid 2016-2017 opgesteld. Hierin worden de belangrijkste activiteiten benoemd die noodzakelijk zijn om informatieveiligheid meer planmatig in te richten, het besef van urgentie voor informatieveiligheid te verhogen en om aan het basisniveau van informatieveiligheid te voldoen.

In dit document wordt als eerste de voortgang besproken aan de hand van de vier kernthema's uit het Convenant. Deze kernthema's zijn:

1. Sturing & verantwoordelijkheid:
2. Beleid & normenkader:
3. Verantwoording & toezicht:
4. Bewustwording

Vervolgens wordt in dit verslag een overzicht gegeven van de activiteiten zoals deze zijn benoemd in het Plan van Aanpak Informatieveiligheid 2016-2017 .

Plan-do-check-act:
Juni 2016 is het beleidsplan en plan van aanpak vastgesteld voor de jaren 2016 en 2017 We zijn nu in de "Do" fase. Gedurende het jaar 2017 zullen ook meer audit activiteiten ondernomen worden, waaronder een onderzoek van een onafhankelijke derde, om te "checken" waar we staan. Deze informatie levert input voor het Jaarplan Informatieveiligheid 2018.

2.0 Samenvatting

Door het vaststellen van het Convenant Informatieveiligheid, het oppakken van bevindingen van eigen onderzoek en het onderzoek van de Rekenkamer is door bestuur en management het belang van het treffen van maatregelen om de beschikbaarheid en integriteit van informatie te borgen onderkend en is opdracht gegeven tot het herijken van informatieveiligheidsbeleid en het opstellen van een Plan van Aanpak. De activiteiten in het plan van aanpak zijn er op gericht om doelstellingen uit het Convenant te realiseren waaronder het implementeren van de Interprovinciale standaard voor informatieveiligheid (IBI).

Ten opzichte van juni 2016 is op de vier kernthema's uit het convenant: sturing & verantwoordelijkheid, beleid & normenkader, verantwoording & toezicht en bewustwording vooruitgang geboekt. Het portefeuillehouderschap is stevig verankerd, de IBI is uitgangspunt voor ons beleidskader, het awareness programma voor medewerkers is nagenoeg gereed en de periodieke en onafhankelijke toets staat gepland voor 2017. Uit het activiteiten overzicht blijkt dat alle activiteiten gestart zijn volgens planning. De risico/GAP analyse op basis van de toolbox-systematiek die per proces worden uitgevoerd, kunnen daarbij worden gezien als een vorm van tussentijdse interne audit.

Toch is het noodzakelijk informatieveiligheid nog steviger te verankeren binnen de provincie om te voorkomen dat de verantwoordelijk gedragen blijft door enkelingen. Om toe te groeien van ad-hoc naar "de fase 2/3 (beschreven/uitgevoerd)[1] uit het procesvolwassenheidsmodel voor informatieveiligheid wordt gehanteerd is het noodzakelijk dat de proceseigenaren nog beter toegerust worden om hun verantwoordelijkheid te kunnen nemen. Er hebben zich een aantal beveiligingsincidenten voorgedaan waarop actie is genomen Verdere implementatie door de proceseigenaren, bijvoorbeeld door het opstellen/aanpassen van procedures/instructies en door het uitvoeren van instructies is noodzakelijk om verder toe te groeien naar het niveau van "beschreven/uitgevoerd" uit genoemd model. Een deel van de activiteiten in deze rapportageperiode heeft zich gericht op treffen van voorbereidingen voor nadere bewustwording en instructie voor CMT, directie en teamleiders. Omdat risk-based werken een belangrijk uitgangspunt is bij het nemen van besluiten, zal aan de implementatie van dit proces en de rol van de proceseigenaar/teamleider hierin ruim aandacht worden besteed.

Om proceseigenaren/teamleiders goed te kunnen faciliteren en om de rapportagelasten te vereenvoudigen is het belangrijk om de toolbox informatieveiligheid goed te gebruiken. Om te bepalen wat het juiste (detail)niveau is van het gebruik van dit instrument en daarmee draagvlak voor het gebruik te creëren, wordt nader overleg en besluitvorming met de proceseigenaren/teamleiders georganiseerd. De provincie Utrecht anticipeert hiermee op de Baseline Informatieveiligheid Overheden die momenteel wordt ontwikkeld en waarvan de verwachting is dat zij grote delen van de IBI en toolbox systematiek zullen overnemen.

Innovaties met betrekking tot technische maatregelen worden betrokken in het project Verbetering Infrastructuur Provincie Utrecht. Dit betreft de onder meer de kavels netwerk/ICT infra, printers, connectiviteit en lap-tops. Diverse activiteiten die zijn genoemd in het Plan van Aanpak worden onder dit project gebracht (bv. Mobile Device Management, anti ramsomware-protection). Daarmee kan een juiste afweging gemaakt worden tussen technische investeringen en het beschermingsniveau dat gerealiseerd kan worden.

Samen met bewustwording van medewerkers blijft het doel van de technische maatregelen om informatieveilig tijd- en plaats onafhankelijk te kunnen werken.

[1] Deze fasen zijn vergelijkbaar met de termen "herhaalbaar/gedefinieerd") uit het volwassenheidsmodel zoals Audit Connect in haar audit (2015/2016) heeft gebruikt,

3.0 Stand van zaken Convenant

Hierna wordt de stand van zaken beschreven op de vier kernthema's. Als eerste volgt de afspraak uit het convenant, vervolgens de stand van zaken zoals beschreven in het Plan van Aanpak Informatieveiligheid van juni 2016, daarna de huidige stand van zaken en ten slotte kijken we kijken we vooruit naar de activiteiten in 2017.

3.1 Sturing & verantwoordelijkheid:

3.1.1. portefeuille informatieveiligheid

Uit convenant:
Informatieveiligheid wordt een onderdeel van de portefeuille van een lid van gedeputeerde staten.

Stand van zaken juni 2016:
Informatieveiligheid als onderdeel van de portefeuille lid Gedeputeerde Staten en als verantwoordelijkheid management wordt geactiveerd naar aanleiding van vaststellen beleid en Plan van Aanpak,

Stand van zaken januari 2017:
In Provinciale Staten van augustus 2016 is het onderzoek van de Rekenkamer besproken en heeft de Portefeuillehouder opdracht gegeven aan de ambtelijke organisatie om uitvoering te geven aan het Plan van Aanpak. Middels deze rapportage is de portefeuillehouder op de hoogte gebracht van de voortgang. Awareness binnen het college van GS heeft er aan bijgedragen dat de commissaris van de Koning een bijeenkomst voor burgemeesters heeft georganiseerd rond het thema informatieveiligheid waarbij de digi-commissaris Bas Eenhoorn een presentatie heeft verzorgd. De commissaris van de Koning heeft tevens een publicatie verzorgd in Ibestuur.

Vervolg activiteiten:
In Juni 2017 volgt een tweede voortgangsrapportage. Om het bewustzijn van de collegeleden verder te vergroten zal een simulatieoefening rond Cybercrime worden georganiseerd. Medewerkers van de provincie zijn in gesprek met VNG Utrecht over een ambtelijk vervolg op de bijeenkomst van burgemeesters en commissaris van de Koning over informatieveiligheid.

3.1.2. Risicoanalyse en –afweging

Uit convenant:
Elke provincie implementeert passende (beheers)maatregelen, gebaseerd op risicoanalyse en afweging.

Stand van zaken juni 2016
De eerste risicoanalyses zijn begin dit jaar gedaan. Begonnen is met het financiële deel van het project PRESTO. De uitvoering van de beheersmaatregelen die uit de risicoanalyse voortkomen is deels uitgevoerd. Er is dus een "gat", een GAP, tussen de gewenste situatie en de feitelijke situatie. De voorbereiding van de GAP analyse is voltooid. Zodra de GAP analyse voltooid is kan er gewerkt worden aan risicoafweging en eventueel risicoacceptatie van dit deel van PRESTO. Ook voor het facilitaire deel van PRESTO is een risicoanalyse uitgevoerd. Twee andere risicoanalyses staan in de planning.

Stand van zaken 1 januari 2017
Naast de risicoanalyse rond het project PRESTO en voor het facilitair deel hebben risicoanalyses plaats gevonden voor de volgende processen: Personeelsadministratie, Assets wegen, GIS informatie. Voor de processen BIBOP, DIV, Inkoop, BEM, Personeelszaken, CCO, IBT en Subsidies was reeds een risico-analyse uitgevoerd.
Ten behoeve van de risico-analyse wordt gewerkt met een toolbox die speciaal voor provincies is ontwikkeld. In deze toolbox zijn de maatregelen opgenomen die voortvloeien uit de Interprovinciale Baseline Informatieveiligheid (IBI), die een uitwerking is van de ISO27001 en ISO27002. Het resultaat van de gevolgde risicoanalysemethodiek is een overzicht van de maatregelen om de gesignaleerde risico's te mitigeren. Deze beheersmaatregelen moeten door de proceseigenaren uitgevoerd worden OF door de proceseigenaren wordt gevraagd om het risico te accepteren, wast vervolgens door een management besluit wordt bekrachtigd. .

In de tweede helft van 2016 hebben de voorbereidingen voor awareness/kennis sessies voor CMT, directie en teamleiders plaatsgevonden.

Vervolgactiviteiten 2017.
Om informatieveiligheid binnen de gehele organisatie tot een gedragen en gestructureerd proces te maken wordt in 2017 verder geïnvesteerd in bewustwording en training. Voor het CMT en directie worden, samen met het management van de provincie Flevoland Informatie-awareness sessies georganiseerd, waar ook informatieveiligheid onderdeel vanuit maakt. In een vervolgbijeenkomst zal nader worden ingezoomd op risico's en impact en het onderwerp risicoacceptatie. Doel hiervan is richting te geven aan de afweging tussen (financiële) inspanningen versus het risico dat je gemotiveerd kan/wilt dragen. Voor de teamleiders is het van belang om verantwoordelijkheid te nemen voor de passende maatregelen die voortvloeien uit de analyse uit de toolbox en hier periodiek over te rapporteren. Tot op heden wordt alleen door één specialist gewerkt met de toolbox. Om de toolbox tot een werkend instrument te maken voor de gehele organisatie is het noodzakelijk nader kennis op te bouwen over informatieveiligheid en specifiek de werking van de toolbox. Het kennistraject voor de teamleiders start in februari met de 'serious game' Alcatraz om als eerste de kennis-behoefte van de teamleiders en voor hun team nader in beeld te brengen.

3.2 Beleid & normenkader:

3.2.1. Interprovinciale Baseline Informatieveiligheid

Uit convenant:
De provincies hanteren de Interprovinciale baseline informatieveiligheid (IBI) en gebruiken dit als uitgangspunt bij het beleidskader informatieveiligheid.

Stand van zaken juni 2016:
Het beleid informatieveiligheid en het plan van aanpak in formatieveiligheid 2016-2017 vloeit voort uit interprovinciale baseline informatieveiligheid (IBI) versie 2. Dit is de meest courante versie. Deze baseline is gebaseerd op risicoanalyses, die door de provincies Utrecht en Noord Brabant intern zijn uitgevoerd. Op 20 mei 2016 is deze baseline vastgesteld in het SIO.

Stand van zaken 1 januari 2017:
Momenteel wordt gewerkt aan de Baseline Informatieveiligheid voor Overheden (BIO). Ontwikkelingen worden door de gezamenlijke provincies gevolgd door het CIBO. Vanuit het projectteam die met de BIO aan de slag is, is interesse getoond voor de aanpak en tooling die is gekozen door de provincies Noord-Brabant en Utrecht.

Vervolgactiviteiten 2017:
Ontwikkelingen met betrekking tot de BIO en de eventuele consequenties voor provincies worden gevolgd door het CIBO en het Strategisch Informatie Overleg van de gezamenlijke provincies.

3.2.2. Implementatie standaard beveiligingsniveau

Uit convenant:
De provincies implementeren de generieke maatregelen van de IBI als standaard beveiligingsniveau en zorgen voor organisatorische inbedding.

Stand van zaken juni 2016:
Maatregelen beschermen "assets" (het te beveiligen belang). Op dit moment is er echter geen compleet inzicht van de "assets". Een belangrijk aspect bij de "assets" zijn in de huidige tijd de persoonsgegevens. Er is een redelijk overzicht van collecties van persoonsgegevens in de bedrijfsvoering. Collecties persoonsgegevens in het primair proces worden nader i beeld gebracht.
De provincie beschikt wel over het juiste gereedschap (3A Toolkit informatieveiligheid) om dit inzicht te krijgen. Er is echter onvoldoende menskracht beschikbaar voor de administratie van de maatregelen. Nadere bekendmaking en voorlichting over de mogelijkheden van dit instrument bij proces- en applicatie eigenaren is noodzakelijk.
Vanuit interprovinciaal overleg, SIO, ligt er sinds kort voor elke provincie wel een opdracht voor het uitvoeren van een eerste GAP analyse voor 1 januari 2017 en een opdracht voor een onderzoek naar de (personele) capaciteit die nodig is om deze GAP te sluiten.

Stand van zaken 1 januari 2017:
In de tweede helft van 2016 is aan de hand van de toolbox gewerkt aan de gapanalyse voor de meest cruciale processen. Deze keuze is gemaakt omdat het instrument tijdsintensief is gebleken. Tevens is het inzicht ontstaan dat de proceseigenaren/teams/afdelingen zelf een grotere rol moeten krijgen in het gebruik van dit instrument. Daarvoor is het noodzakelijk om op teamleidersniveau te bepalen tot op welk detailniveau de toolbox gebruikt gaat worden. Daarbij kan onderscheid gemaakt worden naar meer of minder risicovolle projecten.
Binnen de afdeling UFL heeft een eerste privacy-scan plaatsgevonden een verplichting die voort vloeit uit de Wet op de persoonsgegevens. Deze wet wordt vervangen door Europese regelgeving op het gebied van privacy.

Vervolg activiteiten 2017:
In 2017 zal de GAP afgerond worden om daarmee in beeld te brengen welke maatregelen door de proceseigenaren genomen moeten worden en hoeveel tijd en capaciteit dit gaat kosten. Begin februari start nadere bekendmaking en voorlichting over de mogelijkheden van de toolbox ter ondersteuning van de werkzaamheden van de proceseigenaren. Tevens worden de proceseigenaren op de hoogte gebracht van verplichtingen die voortvloeien uit privacy regelgeving en wordt hen gevraagd een privacy-scan op te leveren voor hun domein.

3.3. Verantwoording & toezicht:

Uit convenant:
Iedere provincie laat periodiek een onafhankelijke toets uitvoeren op het beveiligingsniveau en de implementatie-status van het informatieveiligheidsbeleid, waar mogelijk als onderdeel van een bestaande accountantscontrole. De bevindingen worden in de vorm van een control- of auditrapport aan het bestuur en aan het management gerapporteerd.

Stand van zaken juni 2016:
Om het niveau van informatieveiligheid in de organisatie goed te regelen is het nodig om de basale informatieveiligheidsprocessen te implementeren. Deze processen hebben te maken met de GAP analyse, risicoanalyse, risicoacceptatie, rapporteren aan het management, omgaan beveiligingsincidenten etc..
Er zijn twee toetsen uitgevoerd. Het mystery-guest onderzoek van FOX-IT, waarbij niet alleen gekeken is naar het I-bewustzijn van medewerkers, maar ook onderzocht is waar aangrijpingspunten voor kwaadwillenden bestaan om door te dringen in de technische systemen van de provincie. Dit onderzoek heeft 13 aandachtspunten opgeleverd. Van deze aandachtspunten zijn er 10 opgelost. De overblijven de aandachtspunten zijn aanpassing wachtwoordbeleid (langere wachtwoorden), het verbeteren van de toegang tot het gebouw, de segmentatie van het netwerk. Dit laatste komt neer op het plaatsen van virtuele schotten in het netwerk. Deze techniek beperkt de gevolgen van aanvallen op het netwerk.
In oktober en november 2015 is door AuditConnect in opdracht van CCO een assessment op het gebied van informatieveiligheid bij de Provincie Utrecht (PU) uitgevoerd om enerzijds vast te stellen wat het huidige volwassenheidsniveau van informatieveiligheid bij proceseigenaren en direct betrokkenen is en anderzijds het gewenste volwassenheidsniveau (ambitie) in kaart te brengen. De conclusie van dit onderzoek is het besef aan urgentie op het gebied informatieveiligheid in de organisatie verbeterd moet worden. Bij het onderzoek van de Randstedelijke Rekenkamer is ook gekeken naar de implementatiestatus van het beleid. Dit onderzoek was in juni 2016 in een finale fase van afronding.

Stand van zaken 1 januari 2017:
De audit door onafhankelijke derde staat gepland voor Q3 2017 (zie hierna).

Vervolgactiviteiten 2017:
In 2017 zal opnieuw een mystery-guest onderzoek worden uitgevoerd en voor het vierde kwartaal van 2017 staat de tweede audit zoals gedaan door AuditConnect gepland. CCO zal daartoe opdracht verstrekken en er zal volgens dezelfde systematiek een analyse worden gemaakt naar het volwassenheidsniveau op het gebied van informatie-veiligheid. Daarmee wordt het mogelijk een vergelijking te maken ten opzicht van de eerste audit. Cruciaal daarin is hoe het lukt om proceseigenaren toe te rusten om hun verantwoordelijkheid te nemen voor informatieveiligheid om daarmee vanuit de ad-hoc fase (fase 1) te groeien naar de fase beschreven/uitgevoerd. herhaalbaar/gedefinieerd (fase 2 en 3).

3.4 Bewustwording

Uit convenant:
Iedere provincie voert periodiek een bewustwordingsprogramma uit met als doel alle medewerkers te informeren over de noodzaak van informatieveiligheid.

Stand van zaken 2016
Technische maatregelen alleen zijn niet afdoende en hebben soms grote financiële impact. Houding en gedrag van medewerkers zijn daarom belangrijke componenten van informatieveiligheid. We hebben deelgenomen aan de landelijke campagne Alert Online en geregeld worden medewerkers via Atrium geïnformeerd over de werkwijze. Bij de hoeveelheid van informatie is de vraag of informatie via Atrium ook bij medewerkers voldoende beklijfd. Daarom moet ook naar andere vormen gezocht zoals online trainingen. Daarvoor kijken we ook naar ander provincies.

Het eerder genoemde mystery-guest onderzoek van FOX-IT bevat veel onderdelen die specifiek gericht zijn op I-bewustwording. Voorbeeld: Er is een phishing mailactie uitgevoerd, waarbij gekeken is of medewerker bereid zijn om op een link te klikken van een emailbericht dat niet afkomstig van de provincie. Dit was het geval bij 30% van de aanwezige medewerkers. Hackers hebben slechts een werkstation nodig om binnen te komen en vandaar het netwerk te besmetten, verkennen of misbruiken. Dit is ook gebleken bij een ander deel van het mystery-guest onderzoek.
Een belangrijke bron van infectie zijn ransomware en de phishing e-mailberichten. Het effect van de besmetting is dat de bestanden op de harde schuif op de laptop en bestanden op de netwerkopslagruimte versleuteld worden. Voor de medewerker heeft dit grote gevolgen. Herstel van deze infectie is slechts in enkele gevallen mogelijk. Standaardprocedure is daarom dat de laptop opnieuw wordt ingericht waarbij alle opgeslagen bestanden verloren gaan. De getroffen medewerker heeft meestal 1-2 dagen nawerk om zijn oude situatie te herstellen. Vanuit het ICT team moet er nog meer gedaan worden. Uitgezocht moet worden of er bestanden op netwerk zijn aangetast. Het herstellen van aangetaste bestanden gebeurd met de back-up bestanden. Back-up bestanden zijn per definitie nooit actueel. Er is dus een kans dat er gegevens verloren zijn gegaan. Als hierbij persoonsgegevens mogelijk definitief verloren zijn gegaan, moet volgens de Wet Meldplicht Datalekken onderzocht worden of er sprake is van een datalek.

Stand van zaken 1 januari 2017

In 2016 zijn de volgende presentaties gegeven:
- Inrichtingsoverleg over informatieveiligheid
- UFL over privacy en informatieveiligheid
- OR over informatieveiligheid
- Juristenoverleg over datalekken
- Kabinet CvdK over informatieveiligheid
- MT bedrijfsvoering over informatieveiligheid
- Team TKP over informatieveiligheid

Om de werking van ons informatieveiligheidsbeleid onder medewerkers te toetsen is in december 2016 een phishing-mail-actie uitgevoerd. Bij de vorige acties heeft 70% van de medewerkers niet gereageerd op de ‘foute’ bijlage in de mail, door bijvoorbeeld de mail direct te verwijderen. Bij deze actie heeft 93% van de medewerkers niet op de mail hebben gereageerd. Wel is een zorgelijk punt dat toch ook een beperkt aantal medewerkers verleid kon worden hun inloggegevens af te geven. Dat alertheid significant groeit blijkt niet alleen uit de vermindering van het aantal medewerkers dat onbekende bestanden heeft geopend, maar ook om dat er binnen de organisatie een ‘early-warning-syteem is ontstaan, waarin medewerkers elkaar informeren over ransomware aanvallen. Ook het gebruik van verdachtemail@provincie-utrecht neemt toe. Daarbij komt dat ook het treffen van fysieke maatregelen heeft bijgedragen aan het sterk verminderen van ransomware aanvallen.
In de tweede helft van 2016 is een trainee aangetrokken die zich specifiek bezig houdt met het ontwikkelen van een programma voor de medewerkers. Daartoe is ook bij andere (overheids)organisaties gekeken welke acties het meeste effect hebben bij medewerkers. Het programma is in december 2016 opgesteld en wordt voor nader besluitvorming aan het management aangeboden, waarna de uitvoering van het programma in 2017 kan starten.

Vervolgactiviteiten 2017
In vervolg op de phishingmail actie wordt voor de gehele organisatie een lunch bijeenkomst georganiseerd waarin de resultaten bekend worden gemaakt, maar waarin ook een demo door een “ethisch-hacker” zal worden verzorgd. Dit is één van de eerste activiteiten die plaatsvindt in het kader van het awareness programma dat voor medewerkers in 2017 zal worden uitgevoerd.

4.0 Technische maatregelen

Het aanpassen van de technische maatregelen aan nieuwe dreigingen is een noodzakelijk onderdeel van informatiebeveiliging. Ten tijde van de verhuizing (project I move) is gekozen voor een bepaalde set aan technische beveiligingseisen. De standaard die is gekozen paste bij het werkplekbeleid Anders Werken. Medewerkers kregen, binnen kaders, ruimte om hun werkstation naar eigen inzicht in te richten.

Technische maatregelen om informatie te beveiligen ontwikkelen zich voortdurend. Momenteel worden de kavels rond de ICT infra (o.m. netwerk, laptops, connectiviteit, printers) opnieuw aanbesteed om daarmee de basis op orde te houden. Daarbij wordt ook gekeken met welke eisen vanuit de IBI rekening gehouden moet worden. Omdat in het I domein continu innovatie plaatsvindt, zal vanuit informatieveiligheid gezien steeds een afweging gemaakt moeten worden tussen enerzijds de vrijheid die een gebruiker heeft (om bv. zelf software te kunnen installeren) en anderzijds het inperken van de rechten van gebruikers indien het dreigingsbeeld dit noodzakelijk maakt. Dit vraagt om een goed samenspel tussen kaderstellers en de technisch experts. Afgesproken is dat deze afweging, met kennis uit de staande organisatie binnen het project VIPU (Verbetering Infrastructuur Provincie Utrecht) plaats vind. In het activiteiten overzicht (hoofdstuk 5) wordt dit bij de activiteiten die het aangaat vermeld.

5.0 Informatieveiligheidsincidenten 2016

Informatieveiligheidsincidenten zijn volgens het beleid Informatieveiligheid van de provincie: “Incidenten met betrekking tot de informatieveiligheid zijn onverwachte gebeurtenissen die een bedreiging vormen of kunnen vormen voor de integriteit, vertrouwelijkheid of de beschikbaarheid van de informatievoorziening. (paragraaf 6.1, op pagina 8).” Als het om ICT incidenten gaat worden deze net zo afgehandeld als gewone incidenten, maar wel apart geregistreerd. Het proces wordt nog wel verder gestructureerd en door middel van real life cases zullen rollen worden geoefend net zoals bij het proces rond de Wet datalekken is gebeurd. Incidenten worden altijd onder de aandacht gebracht van de proceseigenaar. Incidenten waar persoonsgegevens bij betrokken zijn, worden behandeld in het Intern Meldpunt Datalekken. Deze incidenten worden hieronder gerapporteerd. De IV incidenten worden periodiek geëvalueerd. Deze analyse richt zich op de effectiviteit van de genomen informatieveiligheidsmaatregelen, de noodzaak van aanvullende/ nieuwe maatregelen en de effectiviteit van de gedragscodes.

Overzicht van informatieveiligheidssncidenten 2016	
Beveiligingsincident	**Opvolging**
27 ransomware incidenten op laptops	Een aanpassing in de mailomgeving (ironport) heeft het aantal ransomware incidenten fors gereduceerd.
2 andere serieuze malware besmettingen	Besmetting van laptops verwijderd
1 VPN incident	Als standaard incident afgehandeld
1 werkwijze met remote toegang geven aan leveranciers	Dit incident is door Intern Meldpunt Datalek onderzocht. Bevindingen zijn gerapporteerd aan verantwoordelijke proceseigenaar.
1 Melding van toegang tot provinciale verdieping door niet geautoriseerden	Vanuit management zijn medewerkers er op geattendeerd dat niet geautoriseerden niet op de verdiepingen mogen komen
1 Melding misbruik persoonlijk account	Gesprek met betrokkene
1 Melding van post-it blaadje met wachtwoord onder een toetsenbord	Blaadje is verwijderd Proceseigenaar geïnformeerd.
1 Melding van het niet afsluiten van computerschermen in openbare ruimtes en/of onbeheerd achterlaten van computers in openbare ruimtes.	Betrokkene zijn aangesproken
Melding van de mogelijkheid voor onbevoegden om mail namens medewerker of bestuurder te versturen (fake mail).	Dit blijkt onderdeel te zijn van een complexer vraagstuk dat projectmatig is opgepakt

Meldingen bij Interne Meldpunt Datalekken
Met ingang van 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. De meldplicht datalekken is een aanpassing op de Wet bescherming persoonsgegevens (Wbp) en behelst onder meer het onverwijld in kennis stellen van/melden van een datalek bij de Autoriteit persoonsgegevens (AP). Bedrijven, overheden en

andere organisaties tot wie de meldplicht datalekken zich richt moeten zelf een beredeneerde afweging maken of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt.

De beoordeling en eventueel de melding van een datalek is belegd binnen het team Advisering (ADV) van de afdeling Managementondersteuning (MAO). Voor de beoordeling en melding van een datalek is het interne Meldpunt Datalekken (hierna: het Meldpunt) ingericht. Dit Meldpunt wordt (parttime) bemenst door vier medewerkers (twee medewerkers vanuit de Information Security Officer (hierna: ISO)-rol en twee juridische adviseurs). Naar procesvolwassenheid geredeneerd kunne we stellen dat hier de fase van “uitgevoerd” is bereikt.

Het Meldpunt heeft dit jaar 17 meldingen ontvangen van mogelijke datalekken. Geen van deze meldingen waren zo ernstig dat deze bij de Autoriteit Persoonsgegevens moest worden gemeld. In de meeste gevallen ging het om meldingen waarbij persoonsgegevens zichtbaar waren voor andere collega’s. Dit is doorgaans het gevolg van onjuiste of onvolledige autorisatieniveaus binnen de provinciale systemen (uitgangspunt moet zijn need-to-know) en onbekendheid/onwetendheid van medewerkers. Daarnaast blijkt er nog onduidelijkheid te bestaan over de vele verschillende verwerkingen van persoonsgegevens binnen de organisatie in relatie tot het wettelijke kader.

Het komende jaar zal dus tijd en energie worden gestoken in het vergroten van de awareness en kennis bij bestuur, management en medewerkers, alsmede het inventariseren van de verschillende verwerkingen van persoonsgegevens binnen de organisatie, om te voorkomen dat datalekken onopgemerkt blijven of niet gemeld worden.

Implementatie Algemene Verordening Gegevensbescherming (AVG)
Op 17 mei 2016 is de “Algemene Verordening Gegevensbescherming” (hierna: de AVG) in werking getreden, waarin spelregels staan over de bescherming van persoonsgegevens. De verordening versterkt de rechten op gegevensbescherming en biedt natuurlijke personen meer controle over hun persoonsgegevens. De verordening werkt rechtstreeks in de hele Europese Unie waardoor de Wet bescherming persoonsgegevens zal komen te vervallen. Onder het nieuwe systeem kunnen Europese privacy-toezichthouders als de AP boetes van maximaal twintig miljoen euro of 4 procent van de wereldwijde omzet van een bedrijf uitdelen.

Uiterlijk 25 mei 2018 moet de provincie aan de verordening voldoen. Dat lijkt nog ver weg, maar er moeten nog een flink aantal stappen worden gezet om aan de verordening te voldoen. Tijdig beginnen is dus essentieel!

6.0 Voortgang Activiteiten Plan van Aanpak 2016-2017

In dit hoofdstuk wordt gerapporteerd over de activiteiten uit het Plan van Aanpak.

Legenda prioriteit :

	Legenda bij Planning Q3 en Q4		Legenda bij Status
		Gepland voor 2017	
	O	Gestart	Gestart = in besluitvorming of begonnen met uitvoering
	V	Afgerond	

Categorie	Activiteit	2016 Q3	2016 Q4	Status 1 januari 2017
B1 Verbeteren, aanpassen van beleid en nieuw beleid	Strategisch beleid informatieveiligheid			-gesprekken zijn gevoerd om dit samen met de provincie Flevoland op te pakken als vervolg op gezamenlijk I- awareness traject
	Operationeel beleid beheer software mobiele apparaten (MDM)		**O**	-Memo met operationeel beleid is opgesteld. Dit memo wordt verder afgehandeld door de projectleider van kavel 8 van het programma VIPU.
	Operationele richtlijnen over gebruik van provinciale informatie op privé apparaten.	**O**		- Centraal staat de bescherming van provinciale informatie. Door de stuurgroep VIPU is gevraagd te onderzoeken of het vigerende BYOD beleid hierop aangepast moet worden. Deze opdracht is belegd bij de afdeling MAO.
	Besluitvorming nieuw (operationeel) wachtwoordbeleid		**O**	-In concept klaar en wordt ingebracht in het ICT overleg
	Operationeel beleid voor laten uitvoeren van technisch beheer van (bedrijf)applicaties door externe partijen		**V**	Richtlijnen zijn vanuit Intern Meldpunt Datalekken opgesteld en toegezonden aan verantwoordelijk teamleiders (31 okt . 2016).
	Operationeel beleid over privé gebruik van provinciale middelen	**O**		Uitgangspunt is dat beveiligingsniveau van de provincie ook beveiligingsniveau is dat gegarandeerd kan worden voor privé-informatie op bv. smartphones. Medewerkers moeten zich daarvan bewust zijn en daarover zal gecommuniceerd moeten worden. -Actie: Er dient korte memo opgesteld te worden en dit wordt meegenomen in het awareness-

				programma. In het managementcontract voor 2017 is informatieveiligheid opgenomen. Speciale aandacht is er voor deelname van medewerkers aan het ibewustzijnsprogramma
B12 Randvoorwaarde informatieveiligheid	Personele inzet afstemmen met het ambitieniveau en de achterstanden in IV.	**O**		-Voorbereiding met oog op voorjaarsnota zijn besproken met afdeling financiën.
	Abonnement 3A Toolkit	**V**		
	Strippenkaart expertise (risico-analyses)	**V**		
B2 Verwerken bevindingen eerder onderzoek	Uitwerken bevindingen eerder onderzoek naar actiepunten: Randstedelijke Rekenkamer en het onderzoek AuditConnect	**V**		Reeds verwekt in beleidsplan en Plan van Aanpak.
	Besluitvorming over restpunten uit mystery guest onderzoek FOX-IT	**O**		Tourniquets: De beveiliging van onze gebouwen is opnieuw aanbesteed. Bedrijf dat voor ons aan de slag gaat heeft veel ervaring in beveiligen van openbare gebouwen waaronder politie. Begin januari 2017 heeft een gesprek plaatsgevonden om vanuit hun visie en ervaring m.b.t. gastvrijheid vs. veiligheid over de toegang van de hoofdingang te spreken. .Het bedrijf heeft aangegeven dat bij vergelijkbare organisaties goede resultaten geboekt worden door in te spelen op het gedrag van bezoekers. -Deze lijn wordt ook gevolgd door de provincies Noord Brabant en Friesland
				Segmentering netwerk wordt opnieuw bekeken bij aanbesteding van het netwerk (VIPU)
B3 Activiteiten verbeteren I-bewustzijn van medewerkers	Jaarlijks mystery guest onderzoek zoals in 2015 is uitgevoerd. Niet in 2016 omdat door Rekenkamer soortgelijk onderzoek is uitgevoerd.			
	Selectieve actie	**V**		Maandag 12 december 2016 is er in

	in het kader van het I-bewustzijn van de medewerkers in 2016			opdracht van de provincie door FOX-IT een phishingmail simulatie uitgevoerd. 93% van de medewerkers heeft niet gereageerd op het mailbericht.
	Gebruik digitale leeromgeving informatieveiligheid van de Provincie Noord Brabant. (onderzoek)	**V**		Gesprekken hebben plaatsgevonden. Voorbereidingen gaan de voor een week van de veiligheid in 2017 zijn gaande.
	Voorlichten proceseigenaren, applicatie-eigenaren en gegevens-eigenaren over hun rol in informatie-veiligheid	**O**	**O**	Presentaties dit jaar gegeven: - Inrichtingsoverleg over informatieveiligheid - UFL over privacy en informatieveiligheid - OR over informatieveiligheid - Juristenoverleg over datalekken - Kabinet CvdK over informatieveiligheid - MT bedrijfsvoering over informatieveiligheid - Team TKP over informatieveiligheid Wordt voor alle proceseigenaren vervolgd in 2017.
	Inrichten operationeel overleg Informatieveiligheid o.l.v. CISO	**V**		Overleg is opgezet en inwerking
	Opstellen activiteiten-kalender met gerichte actie om I-bewustzijn te verhogen + verslaglegging van de activiteiten.	**V**	**V**	Hiervoor is een trainee aangetrokken. Als eerste wordt gekeken welke acties bij ander organisaties succesvol zijn gebleken. Hoe zorg je ervoor dat er een cyclisch proces van leren op gang wordt gebracht . Op basis van deze bevindingen is een activiteiten kalender opgesteld. Definitieve besluitvorming over de activiteiten dient nog plaats te vinden. Deze activiteiten worden het meest zichtbaar naar de medewerkers en leden van GS en PS. De activiteiten worden uitgevoerd in 2017.
B4 Activiteiten om informatieveiligheid goed te laten functioneren	Inbedden fundamentele processen informatieveiligheid in organisatie	**O**	**O**	Opdrachtformulering proces beveiligingsincidenten is opgesteld. Evenals voor de inrichting van het proces Wet datalekken zal dit worden uitbesteed.
	Beleggen rollen uit beleid informatieveilig	O	O	De rollen CIO, ISO en security officers ICT en facilitair zijn belegd. -Actie: Brede communicatie naar

	heid			de organisatie is nodig.
	Inventariseren van de assets			Hangt samen met B5
	Toetsing of de standaard informatieveiligheid maatregel set voldoende is of dat er extra maatregelen nodig zijn voor een asset	**O**		Voorbereiding getroffen voor een scan van de provinciale website aan de hand van de beveiligingsrichtlijnen van het National Cyber Security Centrum
	Inventariseren van de maatregelen voor de assets.	**O**		Hangt samen met B5. Aan de hand van eerdere risico analyse wordt het eigenaarschap van maatregelen belegd bij proceseigenaren c.q. applicatie en gegevenseigenaren
	Planmatige aanpak voor dichten van de GAP			Hier is ook gezocht naar een bestendige rapportagevorm die gebruikt kan gaan worden die aansluit bij de toolkit informatieveiligheid die al gebruikt wordt. In deze rapportage vorm kan getoetst worden aan procesvolwassenheidniveau die thans gangbaar is op het onderwerp informatieveiligheid en waarin het proces van continu verbeteren is geïncorporeerd. Wat we anders gaan doen is dat dit instrument niet door enkelingen maar breed in de organisatie gebruikt gaat worden. In 2017 zullen de proceseigenaren hierin betrokken worden.
B5 Risicoanalyses	Uitvoeren van Risicoanalyses	**O**	**O**	Risico analyse die dit jaar gedaan zijn: - PRESTO financieel- voltooid - PRESTO facilitair-voltooid - Personeelsadministratie – wordt voltooid - Assets wegen – wordt voltooid - GIS informatie – wordt voltooid
	Uitvoeren van GAPanalyses n.a.v. een risicoanalyse		**O**	Hangt samen met B5 Voorbereiding voor een GAP analyse a.d.h.v. de interprovinciale baseline informatieveiligheid zijn nu gaande
B6 Rapportage aan interpovinciaal overleg SIO	Overzicht uitvoering status maatregelen informatieveiligheid			
B7 Toetsen (onderdeel van PDCA cyclus)	Interne audits			De ‘officiele’ audit door onafhankelijke derde en op dezelfde manier als in 2015 (vergelijkbaarheid resultaten) staat gepland voor Q3 2017; wel is

				steeds meer duidelijk dat de risicoanalyses voor de verschillende processen (financieel, facilitair) op basis van de Toolkit gezien kunnen worden als een vorm van een interne audit.
	Pentesten (in wisselwerking met B 3.1)		**V**	In 2016 is gekozen voor phishing mail simulatie die op 12 december werd uitgevoerd. Hierbij is onderzocht of medewerkers te verleiden zijn om op een link in een emailbericht te klikken en vervolgens hun logincodes achter te laten. 93% van de medewerkers heeft dit niet gedaan. Bij de meting van 2015 was dit 70%. Vergelijkbare organisaties hebben in 2016 een score van 80-85%
B8 Beveiliging van provinciale websites	Analyse beveiligingsmaatregelen websites			
B9.1 Verbeteren technische beveiliging werkstations	Aanpassen configuratie van de IronPort (soort van email gateway) als preventiemaatregel voor ransomware.	**V**		Aanpassingen Ironport zijn uitgevoerd. Dit heeft een groot effect gehad. Het aantal ransomware aanvallen zijn gedaald tot minder dan gem. 2 per maand.
	Ransomware preventie	**O**		Ransomware. Gezien voorstaande actie (9.1.1.) en effect wordt gekozen voor risico-acceptatie en volgt op korte termijn geen investeringsactie, maar wordt aanbesteding anti ransom software in het project VIPU meegenomen tegelijk met ander maatregelen m.b.t. end-point security. Maatregelen end point security ihkv project VIPU worden zichtbaar in Q2 2017.
	Rechtenbeheer op laptops	**O**		Overgedragen naar programma VIPU i.v.m. nieuwe werkstations die waarschijnlijk in eerste kwartaal 2017 komen.
B9.2 Verbeteren beheer en bescherming mobiele apparaten (smartphones en tablets)	Herinstallatie software voor beheer van mobiele apparaten (MDM), die provinciale informatie bevatten	**O**		Wordt opgepakt vanuit het programma VIPU, die een aanbesteding gaat doen naar virus/malware/ ransomware protectie; daarbij wordt gekeken naar meest recente technieken om bij beveiliging onderscheid te maken tussen bedrijfsgegevens en prive gegevens.
	Verbeteren informatieveiligheid mobiele apparaten, die provinciale informatie bevatten	**O**		Wordt opgepakt vanuit het programma VIPU, die een aanbesteding gaat doen naar virus/malware/ ransomware protectie

B9.3 Overige technische verbeteringen	SIEM	**O**		Dit wordt opgepakt in het programma VIPU
	SOC	**O**		Dit wordt opgepakt in het programma VIPU
	Installatie nieuwe internet protocollen, conform interprovinciale afspraken	**O**		De leverancier KPN heeft hierover een presentatie gegeven. Vervolgstappen worden genomen. Binnen begroting is hiervoor een bedrag van 15.000 euro vrijgemaakt.
B10 Documentum en Postverwerking	Postkamer hanteert aparte procedures bij het verwerken van post met gevoelige persoonsgegeve ns	**O**		Het betreffende team heeft voorstellen gedaan voor verbetering. Deze zijn neergelegd bij het Intern Meldpunt Datalekken voor een standpunt.
	Documentum voldoet aan de IV eisen om personeelsdossi ers, van vertrokken medewerkers te importeren.			Er is een protocol opgesteld om de personeelsdossier op een veilige manier van ADP (de leverancier van het personeel systeem) over te brengen naar het digitaal archiefsysteem van de provincie en hierin op te slaan. De uitvoering gaat binnen enkele weken van start.
	Review van de samenstelling van de logbestanden van Documentum			
B11 Wegen	-Status maatregelen Informatieveilig -heid (BIR-RWS) van de verkeerregel- installaties (VRI's) op nemen in de 3A Toolbox	**O**		De eerste stappen zijn gezet. De maatregelen van de BIR-RWS zijn opgenomen in de 3A Toolbox. Vervolgstappen worden gepland. De eerste stap is een risicoanalyse van de verkeerscentrale van de PU.
	Verwerken bevindingen eerder onderzoek naar informatieveilig heid van VRI’s en verkeercentrale	**O**		De eerste stappen zijn gezet. De maatregelen van de BIR-RWS zijn opgenomen in de 3A Toolbox. Vervolgstappen worden gepland. De eerste stap is een risicoanalyse van de verkeerscentrale van de PU.