Rapportage vervolgonderzoek informatieveiligheid mens, organisatie en techniek

Gemeente Assen

Rapport rekenkamercommissie gemeente Assen
versie 1.0

Groningen, 7 december 2017

insitesecurity

Inhoudsopgave

1 Managementsamenvatting

1.1 Inleiding

Door de toenemende afhankelijkheid van ICT, is de beveiliging van de gegevens in de systemen van de gemeente Assen ook steeds belangrijker geworden. Zo worden de gegevens van burgers niet meer met de hand geschreven op papieren documenten en in kasten gearchiveerd. Gegevens van burgers worden door de digitalisering nu digitaal bewaard. Bovendien werken gemeenten en burgers steeds meer samen omdat de digitalisering die nieuwe mogelijkheden ondersteund. Met de digitalisering heeft de gemeente ook een extra verantwoordelijkheid gekregen om zorgvuldig om te gaan met de gegevens van haar burgers. En dat betreft niet alleen de veiligheid (security) maar ook de privacy. Want de gegevens van burgers mogen niet rondslingeren en in verkeerde handen komen. Bovendien is de wettelijk druk daaromtrent ook fors toegenomen. Denk aan de verplichte melding van datalekken aan de Autoriteit Persoonsgegevens en ook aan de recente verhoging van de boetecategorie die de Autoriteit Persoonsgegevens kan opleggen (820.00 euro). Daarnaast wordt met de inwerkingtreding van de Europese Algemene Verordening Gegevensbescherming in mei 2018 de druk op de gemeenten en andere publieke organisaties nog groter. Van de gemeenten zal nog meer worden verwacht om de security en privacy van haar burgers aantoonbaar te borgen.

Door de decentralisatie van het sociale domein naar de gemeenten zijn er ook allerlei informatiesystemen toegevoegd. Het betreft veelal complexe systemen die veel persoonsgegevens bevatten en bovendien worden gebruikt door vele betrokkenen.
Tegelijkertijd verandert de wereld om ons heen snel. Ontwikkelingen zoals ‘cloud’ maar ook nieuwe dreigingen zoals ‘phishing’ vragen om een meer proactieve benadering van informatieveiligheid. En tot slot willen de burgers ook steeds meer zekerheid over het niveau van informatieveiligheid van de gemeente Assen en kunnen zij vragen naar de door de gemeente Assen getroffen beveiligingsmaatregelen.

In 2015 is in opdracht van de Rekenkamercommissie Assen door Insite Security een nulmeting informatieveiligheid uitgevoerd. De resultaten gaven aanleiding voor gemeente Assen tot het nemen van verschillende technische en organisatorische maatregelen. Ook is aandacht besteed aan het verhogen van het niveau van beveiligingsbewustzijn van de medewerkers van gemeente Assen. Er is bijvoorbeeld een e-learning phishing aangeboden om de medewerkers het onderscheid te leren tussen legitieme e-mail en phishing e-mail.

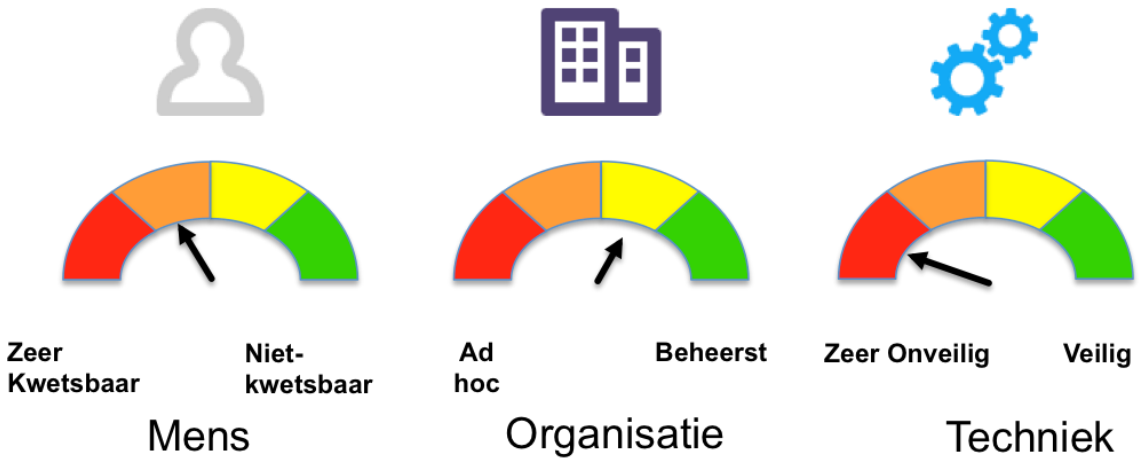
In het vervolgonderzoek 2017 heeft de Rekenkamercommissie, ten opzichte van de in 2015 uitgevoerde nulmeting laten vaststellen:

- Of het niveau van informatieveiligheid al dan niet is verbeterd;
- Welke resterende, nog niet verholpen, risico’s er zijn geconstateerd;
- Welke eventuele nieuw geconstateerde risico’s er zijn geconstateerd;
- Welke eventuele aanvullende beveiligingsrisico’s zich voordoen door de (ICT) samenwerking met derde partijen.

Evenals de nulmeting in 2015 heeft het onderzoek zich gericht op de verschillende aspecten die raken aan informatieveiligheid, oftewel menselijk gedrag, de organisatie (IT Governance en beheersing) en de inrichting en werking van de techniek.

1.2 Resultaten vervolgonderzoek informatieveiligheid

Insite Security heeft een vervolgonderzoek informatieveiligheid uitgevoerd in opdracht van de rekenkamercommissie gemeente Assen. Dit vervolgonderzoek betreft de perspectieven mens, organisatie en techniek. Te samen geven deze perspectieven een beeld van het volwassenheidsniveau omtrent informatieveiligheid zoals onderstaand is gevisualiseerd voor de perspectieven mens en organisatie en techniek. De uit de technische vervolgonderzoek afkomstige hiaten zijn gelijk opgepakt en verbeterd waarna het continue proces van verbetering in gang is gezet.



Aspect Mens

De resultaten van het vervolgonderzoek op het aspect mens laten zien dat de medewerkers nog steeds kwetsbaar zijn voor mensgerichte aanvallen. Ten opzichte van het eerste rekenkameronderzoek (2015) zien we qua resultaten wel enige verbetering. Door 232 (23%) medewerkers is de phishingmail niet herkend en hebben 123 (12%) medewerkers gebruikersnaam en wachtwoord afgegeven. Het percentage medewerkers dat de phishing mail weet te herkennen is gelijk gebleven. Het percentage dat gebruikersnaam en wachtwoord afgeeft is gelukkig sterk gedaald, maar het aantal blijft nog steeds een hoog risico. Het gemeentehuis is door een ‘mystery visitor’ nog steeds relatief makkelijk binnen te dringen door mee te lopen met een medewerker van de gemeente Assen. Dit kon ook gedaan worden na plaatsing van de nieuwe interne toegangsdeuren. Vervolgens kan er ongestoord gezocht worden naar vertrouwelijke informatie op bureaus en in kasten of misbruik te maken van niet gelockte schermen.
Bij de Screenlock actie zijn 10 onbeheerde niet gelockte schermen gemanipuleerd en ‘vastgezet’. Twee medewerkers (20%) hebben dit incident gemeld bij de eigen helpdesk. Eén medewerker heeft dit in eerste instantie gemeld bij de fictieve helpdesk. De medewerkers geven aan dat het locken van het scherm bij kortdurende afwezigheid niet echt nodig te vinden. Ook het voorval melden als incident vindt men niet echt noodzakelijk.
De uitdaging blijft dus ook liggen in het verbeteren van de aspecten kennis, houding en gedrag van informatieveiligheid bij de medewerkers van de gemeente Assen.

Aspect Organisatie

Uit het organisatorische vervolgonderzoek komt naar voren dat de gemeente Assen zich bewust is van het aspect informatieveiligheid en het toenemende belang voor haar organisatie onderkent. Gemeente Assen is zich zeker bewust van het belang van informatieveiligheid en heeft in 2016 een actieplan gemaakt waarin acties ter verbetering van informatieveiligheid zijn opgenomen. De aanbevelingen uit het vorige onderzoek zijn zichtbaar aangepakt en verbeterd.

1. Houdt risicoanalyses op de meest kritische projecten, klanten en informatiesystemen.
   Er worden risicoanalyses uitgevoerd, aandachtspunt is het zorg dragen voor een gestandaardiseerde manier van uitvoeren zodat ze herhaalbaar worden en de resultaten eenduidig vergeleken kunnen worden.
2. Zorg dat incidenten als security incident kunnen worden aangemerkt en zorg dat er (extra) maatregelen worden genomen in voorkomende gevallen.
   Beveiligingsincidenten worden specifiek vastgelegd en opgevolgd.
3. Classificeer de gegevens die worden gebruikt en richt op basis daarvan de rollen met bijbehorende rechten in gebruikmakend van het 'Principle of least privilege'.
   Gegevens worden geclassificeerd, het classificeren en opschrijven van beleid wordt als complex ervaren en moet nog eenduidig vastgelegd worden
4. Zorg dat de verantwoordelijke eigenaren van gegevens/ informatiesystemen/ applicaties periodiek de uitstaande autorisaties controleren en waar nodig laten bijstellen.
   Er is een periodieke controle voor autorisaties ingericht.

Naast de bovenstaande zaken zijn er voor de verschillend processen zoals wijzigingsbeheer, incidentbeheer, continuïteit, fysieke beveiliging en wachtwoordbeleid structurele verbeteringen doorgevoerd. Er zijn tevens en aantal verbeteringen wel onderkend die nog uitgevoerd gaan worden. Het niveau van informatiebeveiliging qua organisatie is nadrukkelijk verbeterd ten opzichte van het vorige onderzoek.

Aspect Techniek

Er zijn meerdere kwetsbaarheden aangetroffen met een kritisch en hoog risico.
Binnen de gegeven tijd is men erin geslaagd om de beveiliging van het interne netwerk te doorbreken. Het onderzoek is opgedeeld in een her-test, een regressie-test en een beoordeling van de beveiliging van vijf kritische systemen o.a. in het sociaal domein en de systemen voor informatie-uitwisseling met ketenpartners.

Om het technische vervolgonderzoek efficiënt uit te voeren is als onderzoeksopzet besloten om de onderzoekers rechtstreeks toegang te verlenen tot het netwerk (middels een lijst van IP-adres ranges) en ook de beschikking te geven over een werkplek met toegang tot het interne netwerk van de gemeente Assen. Deze bewuste keuze is ingegeven vanuit de gedachte dat binnendringen in het interne netwerk van de gemeente Assen louter een kwestie van tijd is omdat hackers met voldoende middelen en tijd op afstand het interne netwerk op verschillende manieren kunnen bereiken (bijvoorbeeld door het plaatsen van kwaadaardige software om zo werkstations of servers te compromitteren of door middel van kwaadaardige hardware zoals een raspberry pi, etc.). Er is van uitgegaan dat de mogelijkheid tot verkrijgen tot toegang tot het gemeentelijke netwerk een gegeven feit is en niet aangetoond hoeft te worden.

De beveiliging van het externe netwerk is beperkt getest tijdens het onderzoek.
Het resultaat als gevolg van misbruik van aangetroffen kwetsbaarheden op het interne netwerk wordt geïllustreerd aan de hand van de volgende situaties.

- Het is mogelijk om aanwezige functionaliteit van het besturingssysteem te misbruiken om zodoende verdere toegang en rechten te verschaffen tot het getroffen doelsysteem en overige systemen in het netwerk.

- Omdat medewerkers bestanden op onvoldoende afgeschermde locaties hadden geplaatst, is het mogelijk gedeelde mappen van verschillende afdelingen binnen de gemeente Assen te bereiken. Daardoor kon vertrouwelijke documenten met onder andere wachtwoorden, financiële informatie, persoonlijke informatie en gegevens van burgers worden ingezien. Het gaat hier om voornamen, achternamen, adresgegevens en BSN-nummers.
- Als gevolg van een gebrek aan authenticatie bleek het mogelijk om de e-mail servers van de gemeente Assen te instrueren op een manier waarbij impersonatie van een willekeurig e-mail adres (binnen het gemeente Assen domein) tot stand komt. Een kwaadwillende zou zich kunnen voordoen als een willekeurige gebruiker met een @assen.nl e-mail adres.

Conclusies

Op basis van de vraagstelling van de rekenkamer constateren we het volgende:

- Naar aanleiding van het in 2015 gehouden rekenkameronderzoek heeft gemeente Assen verschillende initiatieven ondernomen op het menselijke, organisatorische en technische vlak om het niveau van informatiebeveiliging te verhogen. Er zijn hierin duidelijke stappen genomen.
- Op het organisatorische vlak zien we een manier van werken, waarbij verbeteringen op een gestructureerde en gecontroleerde manier worden doorgevoerd op basis van de PDCA-cyclus. Voor de nieuwe striktere privacywetgeving (AVG, mei 2018) dienen nog een aantal maatregelen genomen te worden.
- Het in 2016 ingezette bewustwordingsprogramma voor medewerkers is nog onvoldoende verankerd in de kennis, houding en gedrag van de medewerkers. De medewerkers blijven kwetsbaar voor mensgerichte aanvallen ondanks het afgenomen aantal medewerkers dat gebruikersnaam en wachtwoord verstrekt na een phishing praktijktest. Het niet/minder herkennen en melden van incidenten is/blijft tevens een aandachtspunt.
- Op het technische vlak zijn er diverse beheersmaatregelen genomen zoals verbeterd patchmanagement en zijn de aanbevelingen uit het voorgaande rekenkameronderzoek gestructureerd opgevolgd. Echter gezien de aangetroffen kwetsbaarheden wordt het netwerk als zeer onveilig beoordeeld. Inmiddels zijn er op dit onderdeel op basis van de kwetsbaarheden al een aantal maatregelen genomen.
- In het kader van de ICT-samenwerking met derde partijen zijn er diverse maatregelen genomen om risico's tegen te gaan. Hierbij is het beheer van autorisaties om onbevoegde inzage van gegevens geregeld. Aandachtspunt hierbij is nog wel het wijzigings- en incidentbeheer. De scope van het onderzoek op het menselijke vlak richtte zich niet op de derde partijen. De scope van het technisch onderzoek is met name gericht op 'fact-finding' en niet gericht op Design Review. Op basis hiervan worden geen uitspraken gedaan over de onderliggende IT-architectuur met de samenwerkende partners. Dit zou meegenomen kunnen worden in een vervolgonderzoek.

Verbetermogelijkheden

Op basis van het vervolgonderzoek op de aspecten mens, organisatie en techniek en op basis van haar kennis van en ervaring met informatieveiligheid bij andere organisaties geeft de rekenkamercommissie in samenspraak met Insite Security onderstaand een opsomming van de verbetermogelijkheden en een mogelijke prioritering. De mogelijke verbeterdoelstellingen op basis van het vervolgonderzoek voor de gemeente Assen zijn, in volgorde van prioriteit:

- Starten en onderhouden van een op maat gemaakt bewustwordingsprogramma voor de komende drie jaren (zoals e-learning phishing, communicatie, workshops etc.). Het programma zou minder vrijblijvend kunnen worden aangeboden in samenspraak met het lijnmanagement;
- Verder doorvoeren van de adviezen uit het technische rapport zoals het configuratiemanagement en hardening van het netwerk en haar doelsystemen.
- Implementeren van 'baseline hardening' beleid. Dit sluit niet alleen mogelijke veiligheidsrisico's uit, maar vermindert tevens de de complexiteit van nieuw in productie genomen doelsystemen en maakt dit de betreffender doelsystemen beheersbaarder voor de IT-afdeling.
- Invoeren en uitvoeren van vaste werkwijze van risicoanalyses vanuit het informatieveiligheidsperspectief (zoals BIA);
- Scherp de verantwoordelijkheden binnen de procedure voor het melden van datalekken aan, specifiek voor de afweging voor bepalen of een incident een datalek is.
- Maak resources vrij voor het uitvoeren van de benodigde maatregelen voor de invoering van de AVG en de BIG.
- Herevalueren van de fysieke toegangsbeveiliging in combinatie met de minder alerte houding van de medewerkers

In dit rapport worden verbeteradviezen gegeven op basis van het onderzoek in opdracht van de rekenkamercommissie.

2 Inleiding

2.1 Opdrachtomschrijving en reikwijdte

De rekenkamercommissie doet onderzoek naar de uitvoering van het gemeentelijk beleid. Hierbij wordt gekeken of de uitvoering efficiënt en volgens de regels heeft plaatsgevonden en of het doel bereikt is. In het kader van haar rol wil de rekenkamercommissie de informatieveiligheid toetsen op de onderdelen mens, organisatie en techniek.

De rekenkamercommissie van de gemeente Assen heeft Insite Security gevraagd een vervolgonderzoek informatieveiligheid uit te voeren op de aspecten organisatie, mens en techniek.

In 2015 is in opdracht van de Rekenkamercommissie Assen door Insite Security een nulmeting informatieveiligheid uitgevoerd. De resultaten gaven aanleiding voor gemeente Assen tot het nemen van verschillende technische en organisatorische maatregelen. Ook is aandacht besteed aan het verhogen van het niveau van beveiligingsbewustzijn van de medewerkers van gemeente Assen. Er is bijvoorbeeld een e-learning phishing aangeboden om de medewerkers het onderscheid te leren tussen legitieme e-mail en phishing e-mail.

In het vervolgonderzoek 2017 wil de Rekenkamercommissie, ten opzichte van de in 2016 uitgevoerde nulmeting laten vaststellen:

- Of het niveau van informatieveiligheid al dan niet is verbeterd;
- Welke resterende, nog niet verholpen, risico's er zijn geconstateerd;
- Welke eventuele nieuw geconstateerde risico's er zijn geconstateerd;
- Welke eventuele aanvullende beveiligingsrisico's zich voordoen door de (ICT) samenwerking met derde partijen.

Evenals de nulmeting in 2015 zal het onderzoek zich moeten richten op de verschillende aspecten die raken aan informatieveiligheid, oftewel menselijk gedrag, de organisatie (IT Governance en beheersing) en de inrichting en werking van de techniek.

De opdracht 'Vervolgonderzoek Informatieveiligheid' betrof de gehele gemeente Assen. De ondersteuning van Insite Security bestond uit het in kaart brengen van de huidige situatie (vervolgonderzoek) voor de aspecten Mens, Organisatie en Techniek.

In dit rapport worden de resultaten van de vervolgonderzoek weergegeven en de adviezen die daaruit voortvloeien.

Het vervolgonderzoek is uitgevoerd in de periode juni – oktober 2017.

2.2 Aanpak

Het doel van het vervolgonderzoek was het bepalen in hoeverre de gemeente Assen voldoet aan de geselecteerde (generieke) maatregelen op de aspecten Organisatie, Mens en Techniek. Het vervolgonderzoek is uitgevoerd aan de hand van een technische scan, het bestuderen van bestaande documentatie, eigen waarneming (bijv. het controleren van bepaalde systeeminstellingen), het houden van een aantal interviews aan de hand van gestructureerde vragenlijsten en een aantal praktijktesten (mystery visit, phishingmail en screenlock-actie).

Op basis van de vervolgonderzoek wordt een globaal advies gegeven omtrent de te treffen of te verbeteren beveiligingsmaatregelen.

2.3 Leeswijzer

Dit rapport is als volgt ingedeeld. Hoofdstuk 1 bevat de management samenvatting. In hoofdstuk 3 worden de uitkomsten van het vervolgonderzoek gepresenteerd. De bijlagen bevatten de gedetailleerde bevindingen van de vervolgonderzoek en de door ons geraadpleegde bronnen en referenties.

3 Uitkomsten vervolgonderzoek

3.1 Inleiding

Dit hoofdstuk beschrijft de bevindingen en aanbevelingen van dit vervolgonderzoek en bevat het mensgerichte onderdeel (praktijktesten van gedrag) en het organisatorische onderdeel (analyse interne beheersing). De bevindingen en aanbevelingen van het technische onderdeel van deze vervolgonderzoek (penetratietest en kwetsbaarhedenscan) zijn opgenomen in een aparte rapportage die aan de rekenkamercommissie ter beschikking is gesteld.

3.2 Aspect Mens

Aanpak

Het aspect mens is getoetst aan de hand van enkele praktijktesten, die zijn beoordeeld en op niveau zijn ingedeeld aan de hand van de onderstaande classificering.

Niveau 1 **Zeer kwetsbaar**

Bovengemiddeld veel (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Niveau 2 **Kwetsbaar**

Gemiddelde hoeveelheid (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Niveau 3 **Minder kwetsbaar**

Minder dan gemiddelde hoeveelheid (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Niveau 4 **Niet kwetsbaar**

Weinig tot geen (gevoelige) informatie aangetroffen/verkregen/afgegeven in de praktijktesten van gedrag.

Resultaten

De praktijktesten phishing test, mystery guest bezoek en de screenlock-actie zijn in juni-oktober 2017 uitgevoerd. Onderstaand worden de resultaten beschreven. Conclusie: de menselijke factor in informatieveiligheid is nog steeds een risico voor de informatieveiligheid van de gemeente Assen. De medewerkers zijn/blijven kwetsbaar voor dergelijke aanvallen.

Phishing e-mail

Bevindingen:

- Er zijn 999 e-mails (maillijst acitve directory van de gemeente Assen) verstuurd. In 2015 betrof het 946 e-mails.
- In totaal is er 232x (23%) op de phishing-link geklikt. (In 2015: was het percentage vergelijkbaar: 26%).
- 12% (123 unieke gebruikers) van het totale aantal mailadressen (999) heeft data (gebruikersnaam en wachtwoord) gepost. (In 2015: 245 unieke gebruikers: 26%). De cijfers van het laatste onderzoek kunnen enigszins geflatteerd zijn omdat het aantal geregistreerde medewerkers 717 bedraagt en het bestand van de aangeleverde mailadressen echter 999 groot is. Ook blijkt dat er in de maillijst uit de active directory veel mailadressen niet gekoppeld zijn aan afdelingen. Ook bij het vorige onderzoek was dit al naar voren gekomen.
- Er zijn 11 meldingen (in 2015: waren er 61 meldingen) gerelateerd aan de phishing e-mail geweest bij de servicedesk. De servicedesk was op de hoogte van de test en heeft niet ingegrepen.
- Conclusie: het aantal geposte credentials (gebruikersnaam en wachtwoord) is sterk afgenomen van 245 naar 123 medewerkers. Dit lijkt een mooi resultaat echter voor de cybercrimineel zijn een paar verkregen gebruikersnamen en wachtwoorden voldoende om het systeem binnen te dringen. Het percentage medewerkers dat de phish niet kan onderscheiden van een legitieme mail blijft nagenoeg gelijk.
- Naar aanleiding van de resultaten van het rekenkameronderzoek is er in 2016 aan alle medewerkers een e-learning phishing op vrijwillige basis aangeboden. Minder dan de helft (41%) heeft de e-learning ook daadwerkelijk gevolgd. Gezien de resultaten zou het zinvol om de e-learning opnieuw en minder vrijblijvende aan te bieden in samenspraak met het lijnmanagement.

Screenlock-actie

In oktober zijn er 10 niet gelockte schermen ‘geprepareerd’ door een interne medewerker. Het systeem geeft aan dat het een fatale fout heeft ondergaan. Op het beeldscherm verschijnt de melding dat de fout kan worden verholpen door contact op te nemen met ‘Centic Helpdesk’. Op deze manier werden drie gedragsregels getest:

-bij het verlaten van de werkplek dien je je schermen te locken
-een incident dient te worden gemeld bij de servicedesk
-je wachtwoord is persoonlijk en geef je nooit af

Bevindingen:

Door twee medewerkers (20%) is er van het voorval een incident gemeld bij de servicedesk. Eén medewerker nam contact op met de fictieve servicedesk. Er zijn geen gelukkig geen wachtwoorden afgegeven aan de fictieve servicedesk.
Medewerkers geven te kennen alleen bij langere afwezigheid het scherm te locken en niet bijvoorbeeld bij toiletbezoek. Ook blijkt dat dergelijke incidenten niet standaard bij de servicedesk worden gemeld. De medewerkers die het betrof, zijn na afloop bevraagd op de reden van hun (niet) handelen. Hieruit komt het beeld naar voren van een houding dat men het locken van schermen bij kortdurende afwezigheid niet echt noodzakelijk vindt. Ook geeft men aan het melden van dergelijke voorvallen bij de servicedesk niet echt nodig te vinden. In 2015 is de screenlock-actie niet uitgevoerd.
Conclusie: besteed extra aandacht aan de gedragsregels en informeer medewerkers over nut en noodzaak van informatieveiligheid en de kritische rol van de medewerker hierin.

Mystery guest

Een medewerker van Insite Security heeft in september en oktober het stadhuis van de gemeente Assen geobserveerd en is er onder kantooruren gezocht naar vertrouwelijke informatie. Hierbij is geprobeerd zonder afspraak of identificering het pand binnen te dringen. Eenmaal binnen is geprobeerd vertrouwelijke informatie te verzamelen door onder andere te zoeken naar fysieke documenten bij printers, werkplekken en archieven.

Bevindingen:

- De mystery guest kon meerdere keren eenvoudig het pand binnengaan door mee te lopen met een medewerker in bezit van een pas (het zogeheten 'tailgating') via de hoofdingang. Recent zijn er nieuwe deuren geplaatst. Ook kon nu relatief eenvoudig meegelopen worden met medewerkers met een toegangspas. De mystery guest wordt niet aangesproken bij de balie maar kan gewoon doorlopen. Ook in 2015 kon de mystery guest gewoon doorlopen en op zoek gaan naar gevoelige informatie.
- De medewerkers van de gemeente Assen vertrouwen over het algemeen op de goede bedoelingen van bezoekers. Onze medewerker is niet aangesproken en kon enige uren ongestoord door het stadhuis lopen;. Blijkbaar is het lastig voor de medewerkers om 'onbekenden' aan te spreken. Een oorzaak kan zijn dat er (te) veel 'onbekenden' in het stadhuis rondlopen.
- Er zijn diverse documenten met vertrouwelijke informatie op bureaus en in kasten onbeheerd aangetroffen;
- Er zijn meerdere onbeheerde niet gelockte schermen aangetroffen, maar deze schermen waren minder goed toegankelijk omdat er collega's in de buurt aanwezig waren;
- Op de 'doorloop' (gang) zijn meerdere niet gelockte schermen aangetroffen, deze waren eenvoudig te 'misbruiken';
- In de kantine kon eenvoudig worden meegeluisterd met overleggen die daar plaats vonden
- Vertrouwelijk materiaal kan worden aangeboden in speciaal hiervoor bestemde afgesloten grijze bakken. Deze bakken waren afgesloten.
- Bij de printers zijn geen vertrouwelijke documenten aangetroffen. Men maakt gebruik van een vorm van secure printen;

Conclusies en aanbevelingen vervolgonderzoek mens

De menselijke factor in informatieveiligheid blijft nog steeds een risico voor de informatieveiligheid van de gemeente Assen. Er zijn zowel 'online' als 'offline' pogingen gedaan om waardevolle informatie buit te maken. De medewerkers zijn kwetsbaar voor dergelijke aanvallen.

Verhoog het kennisniveau en het risicobesef van de medewerkers door het verzorgen van een op maat gemaakt bewustwordingsprogramma de komende jaren. In het programma worden onderdelen opgenomen als frequente praktijktesten phishing, e-learningprogramma's, workshops en communicatie uitingen. In dergelijke programma's zou extra aandacht besteed kunnen worden aan de rol van de leidinggevende en bijvoorbeeld de gedragsregels: lock je scherm bij het verlaten van je werkplek (clear screen), het melden van incidenten bij de servicedesk en spreek onbekenden aan in het gebouw. Tevens zou de effectiviteit van de huidige fysieke toegangsbeveiliging in combinatie met de minder alerte houding van de medewerkers opnieuw geëvalueerd kunnen worden.

3.3 Aspect Organisatie

Aanpak

Het organisatorische vervolgonderzoek is uitgevoerd aan de hand van gestructureerde vragenlijsten, het bestuderen van bestaande documentatie en het houden van een aantal interviews, zie de bijlage voor lijst van geïnterviewde personen.

De elementen uit de ISO27002 zijn gescoord conform de Cobit versie 4.1. normering (zie de bijlage), met dien verstande dat de status 0 (niet existent) en de status 5 (geoptimaliseerd) buiten beschouwing zijn gelaten omdat deze niet relevant zijn in de onderzoeksopzet. De onderstaande normering is gehanteerd.

Niveau 1 **Ad Hoc**, initieel

Dit normelement krijgt geen/weinig aandacht of er zijn uitsluitend plannen om met dit normelement aan de slag te gaan.

Niveau 2 **Beperkt**

Dit normelement is beperkt gedefinieerd en geïmplementeerd in de organisatie. De controle op doeltreffendheid heeft nog niet plaatsgevonden.

Niveau 3 **Gedefinieerd** en gecontroleerd

Dit normelement is geïmplementeerd op alle, voor informatieveiligheid, meest kritieke plaatsen en de doeltreffendheid is ten minste één keer door de organisatie gecontroleerd.

Niveau 4 **Beheerst** en Meetbaar

Dit normelement is breed geïmplementeerd en de doeltreffendheid wordt structureel en periodiek door de organisatie gecontroleerd.

Resultaten

Adhoc Beheerst **Gedefinieerd** en gecontroleerd

De resultaten van het vervolgonderzoek laten zien dat de gemeente Assen al een groot aantal organisatorische en ook (deels) technische beheersmaatregelen heeft getroffen die (periodiek) gecontroleerd worden van waaruit verbetering worden benoemd en doorgevoerd.

Sterke punten zijn:

- De gemeente Assen werkt vanuit een actieplan gestructureerd aan het verbeteren van informatiebeveiliging.
- Een groot aantal beheersmaatregelen zijn geïmplementeerd en worden in een PDCA-cyclus verbeterd, zoals maatregelen voor de continuïteit, wijzigingsbeheer, fysieke beveiliging, incidentbeheer etc.
- De gemeente Assen heeft recent het 'Mobile Device Management' geïmplementeerd. Daardoor lopen de mobiele apparaten, zoals de iPads en telefoons, geen technisch risico. Voorwaarde is uiteraard dat medewerkers tijdig een melding afgeven van verlies e.d.
- De gemeente Assen heeft een Functionaris Gegevensbescherming aangesteld en beschikt over een werkende procedure voor het melden van datalekken.
- Er wordt periodiek op autorisaties gecontroleerd.
- Er is voor de continuïteit een glasvezel ring aangelegd tussen Assen, Gieten en Tynaarlo

Tegelijkertijd zijn er nog zaken die aandacht behoeven. In onderstaande paragrafen worden adviezen gegeven. Voor deze adviezen is het van belang dat een afweging plaatsvindt tussen de informatieveiligheidsrisico's die de gemeente Assen loopt en de inspanning in tijd en geld die moet worden geleverd om het advies op te volgen. De organisatorische vervolgmeting is ingegaan op

- Beveiligingsbeleid;
- Logische toegangsbeveiliging (autorisaties);
- Wijzigingsbeheer;
- Incidentbeheer;
- Contract- en servicemanagement;
- Beveiliging van (web)applicaties;
- Continuïteit.
- Compliance (naleving wet- en regelgeving). De mate waarin gemeente Assen is voorbereid op de invoering van de Algemene Verordening Persoonsgegevens;
- De beveiligingsmaatregelen rondom mobile device management;
- De beveiligingsmaatregelen die gemeente Assen heeft getroffen in het Sociaal Domein;
- De maatregelen die gemeente Assen heeft getroffen om de informatie-uitwisseling met ketenpartners te beveiligen.

Beveiligingsbeleid

Beperkt

De gemeente Assen heeft vastgesteld informatieveiligheidsbeleid en heeft in 2016 een actieplan opgesteld voor het verbeteren van informatiebeveiliging. Er is een CISO en daarnaast is een Functionaris Gegevensbescherming aangesteld. Er is een procedure voor het melden dan datalekken ingericht waarbij de afweging bij de leidinggevende ligt. Het uitvoeren van risicoanalyse wordt wel gedaan maar nog niet volgens een formeel vastgesteld format. Een belangrijk issue blijft de beschikbare tijd van de CISO. Door de beperkt beschikbare tijd heeft de CISO onvoldoende slagkracht om de jaarplannen in de organisaties (STAAN) voldoende tot uitvoering te laten brengen. Hierbij is de organisatie van de technische beheerprocessen op orde maar is het belangrijkste aandachtspunt de borging van de BIG-maatregelen in de lijn.

Advies:

- *Zorg dat afweging of een gemeld incident een datalek is, belegd wordt bij de Functionaris Gegevensbescherming.*
- *Invoeren en uitvoeren van vaste werkwijze van risicoanalyses vanuit het informatieveiligheidsperspectief (zoals BIA);*
- *Zorg voor aandacht en tijd voor de projectmatige borging van de BIG-maatregelen in de lijn.*

Logische toegangsbeveiliging

Gedefinieerd en gecontroleerd

Logische toegangsbeveiliging betreft niet alleen de toegang tot applicaties, maar ook tot mappen en bestanden op het filesysteem (home-dir en afdelingsmappen) en in de diverse mailboxen.

Het aanvragen en wijzigen van autorisaties verloopt via de servicedesk waarbij de eigenaar van een applicatie verantwoordelijk is voor de toestemming. Er worden periodieke controles op de uitgegeven autorisaties gedaan, waarbij specifiek aandacht is voor niet gebruikte autorisaties.

Het in- en uitdienst proces van medewerkers is vastgelegd, tussentijdse mutaties in dienstverband en bijbehorende wijzigingen in autorisaties is nog niet formeel vastgelegd. Het wachtwoordbeleid voor de gemeente Assen is aangescherpt en geïmplementeerd.

Advies:

- *Leg het wijzigen van rechten bij mutaties in dienstverband vast in een procedure en implementeer deze*

Wijzigingsbeheer

Gedefinieerd en gecontroleerd

Het proces wijzigingenbeheer is op orde. Wijzigingen worden op een gestructureerde wijze ingediend, beoordeeld en geaccordeerd. Hierbij hebben verschillende disciplines als changemanager, informatiemanagement, accountmanagement en inhoudelijke experts een rol. In het proces is continu aandacht voor mogelijke verbeteringen die doorgevoerd kunnen worden. Voorbeelden hiervan zijn de aandacht voor de klant tevredenheid en het borgen van wijzigingen in de productdienst catalogus (PDC).

Advies:

- *Standaardiseer de uitvoer van testen en het vastleggen van testresultaten bij wijzigingen.*
- *Zorg voor een formelere vastlegging van de testresultaten door de klant.*
- *Blijf aandacht houden voor het registreren van wijzigingen in de CMDB.*

Incidentbeheer

Gedefinieerd en gecontroleerd

Het incidentbeheer is op orde en verbeterd. Voor het melden van beveiligingsincidenten is een specifieke procedure en is een goede samenwerking tussen de CISO en de incidentmanager. Er is een type beveiligingsincident aangemaakt waarbij voor specifieke gebeurtenissen een procedure is gemaakt, bijvoorbeeld voor het verlies van een telefoon. Opvallende zaken worden door de servicedesk gemeld en het melden van beveiligingsincidenten is normaal. Er worden ad-hoc analyses op incidenten uitgevoerd, dit is nog niet structureel ingepland. Bij de applicatie eigenaren is de bewustwording rondom informatiebeveiliging verbeterd waar het doorvoeren van verbeteringen beter verloopt. Een aandachtspuntspint is dat de techniek vaak nog leidend is in de keuze voor niveau van beveiliging terwijl dit in de lijn behoort te liggen.

Advies:

- *Voor periodieke analyses van incidenten in om het voorkomen en herhalen van incidenten nog verder te verbeteren.*

Contract en servicemanagement

Gedefinieerd en gecontroleerd

Het maken van afspraken met externe klanten die gebruik maken van faciliteiten van de gemeente Assen over de dienstverlening en de service hierop wordt gedaan binnen het service level management proces en wordt uitgevoerd door de accountmanager. Afspraken over het niveau van serviceverlening en de kosten worden vastgelegd in een Dienstverleningsovereenkomst (DVO). Een voorbeeld hiervan is het Werkplein Drentsche AA (WPDA). De WPDA maakt gebruik van door gemeente Assen beheerde werkplekken en huurt kantoorruimte van gemeente Assen. Voor deze dienst zijn de afspraken vastgelegd en deze worden gemonitord in het service level management proces. Voor informatiebeveiliging heet de WPDA een eigen Security Officer die rechtstreeks contact onderhoud met de CISO van gemeente Assen.

Het afsluiten van contracten voor applicaties die geleverd worden aan de gemeente Assen is belegd bij de applicatie eigenaar. De eigenaar is verantwoordelijk voor de controle en naleving van de contractafspraken met de leverancier. Voordat deze afspraken tot stand komen is een proces ingeregeld dat borgt dat dit tot een goed einde wordt gebracht. Een aanvraag voor een nieuwe applicatie wordt gedaan bij de servicedesk. Vervolgens wordt er een intake gedaan op de functionele vraag en wordt in het Change Management Overleg de intake besproken. Na de intake wordt een business case gemaakt dat voorzien van een advies naar het SIO gaat waarna bij een akkoord een aanbesteding of uitvraag volgt. In deze uitvraag worden de eisen van de contracteigenaar meegenomen en worden ook de eisen vanuit informatiebeveiliging meegenomen.

De accountmanager en informatiemanager(s) zijn bezig met een rondje langs de applicatie eigenaar om de taken en verantwoordelijkheden die bij deze rol horen duidelijk te maken.

Beveiliging van (web) applicaties

Beperkt

Er is een overzicht van het applicatielandschap, deze is bekend bij de IBD. Op basis van deze lijst worden bekende kwetsbaarheden door de IBD gerapporteerd aan de gemeente. Daarnaast wordt interne maandelijks een kwetsbaarhedenscan uitgevoerd. De resultaten van de scan worden elke 2 weken in een sessie met

systeembeheerders besproken. Er wordt niet gestructureerd op applicaties een test gedaan op de beveiliging van de applicaties.

Advies:

- *Voer periodiek beveiligingstesten uit op applicaties met hoog risico.*

Continuiteit

Gedefinieerd en gecontroleerd

De gemeente Assen heeft (ruim) voldoende beheersmaatregelen geïmplementeerd om de continuïteit van de ICT-voorzieningen te borgen. Er wordt gebruik gemaakt van moderne virtuele servers, waarmee de continuïteit van de servervoorzieningen in grote mate is geborgd. De noodstroomvoorzieningen zijn op orde. Hetzelfde geldt voor de (gescheiden) back-up- en restorevoorzieningen. De bewustwording van de noodzaak voor maatregelen ten behoeve van continuïteit is bij de eigenaren van applicaties en/of processen aanwezig waardoor ICT nu volgend is. Ze zijn zich bewust van de risico's en dreigingen die hun proces verstoren De toetsing en controle hiervan heeft echter nog niet plaatsgevonden.

Voor de uitwijk naar andere gemeenten is een glasvezel ring aangelegd tussen Assen, Gieten en Tynaarlo. Voor het zaaksysteem wordt voor de continuïteit toegang via Tynaarlo ingericht.

Er wordt jaarlijks een test gedaan waarbij alles van de stroom af gaat en er opnieuw opgestart wordt. Van deze test wordt een rapportage gemaakt die geëvalueerd wordt en van waaruit eventuele verbeteringen worden doorgevoerd. Een voorbeeld hiervan is dat het nu helder is welke afdeling als preferente groepen op het noodaggregaat worden aangesloten zodat ze door kunnen werken bij een stroomuitval.

Voor de continuïteit zijn dus de technische maatregelen aanwezig. De volgende stap is het maken van een gemeente breed plan voor de bedrijfscontinuïteit.

Een onderkend risico voor de continuïteit is het ontbreken van beschikbaarheidsdiensten. De ondersteuning is nu geboden tijdens kantoortijden en avondopenstellingen.

Advies:

- *Maak een gemeente breed bedrijfscontinuïteitsplan.*
- *Maak op basis van het geplande onderzoek naar ondersteuning buiten kantoortijden bewust de afweging over het risico voor de continuïteit van de dienstverlening.*

Compliance (naleving wet- en regelgeving)

Beperkt

De gemeente Assen registreert diverse persoonsgegevens. Aan de registratie van deze persoonsgegevens stelt de nieuwe privacywetgeving strikte eisen, want vanaf 1 januari 2016 is de Wbp[1] aangepast en is het wettelijk verplicht datalekken te melden. Met ingang van mei 2018 zal tevens nieuwe Europese privacy-verordening van kracht worden, de Algemene Verordening Gegevensbescherming (AVG). Deze wet stelt, onder andere, dat een organisatie die persoonsgegevens verwerkt voor deze registraties een Privacy Impact Assessment (PIA) dient uit te voeren en een register aanlegt van persoonsgegevens. De gemeente Assen heeft (nog) geen PIA's uitgevoerd en beschikt nog niet over een register. Organisaties hebben tot mei 2018 de tijd hun processen aan

[1] Wet Bescherming Persoonsgegevens.

te passen aan de nieuwe wet. Vanaf dat moment zal de Autoriteit Persoonsgegevens de Europese verordening gaan handhaven.

De gemeente Assen heeft een Functionaris Gegevensbescherming aangesteld die verantwoordelijk is voor de implementatie van de benodigde maatregelen voor de invoering van de AVG. Gemeente Assen beschikt reeds over een werkende procedure voor het melden van datalekken. Aandachtspunt hierbij is bij wie de afweging is belegd of een incident een datalek betreft.

Advies:

- *Scherp de verantwoordelijkheden binnen de procedure voor het melden van datalekken aan, specifiek voor de afweging voor bepalen of een incident een datalek is.*
- *Maak resources vrij voor het uitvoeren van de benodigde maatregelen voor de invoering van de AVG.*

Mobile Device management

 Gedefinieerd en gecontroleerd

Recent is de mobiele telefonie voor gemeente Assen aanbesteed. Binnen deze aanbesteding zijn expliciet de eisen opgenomen voor de aansluiting op de bestaande Mobile Device Management (MDM) oplossing die gebruikt wordt binnen gemeente Assen. De toestellen die zijn aangeschaft zijn zogenaamde corporate toestellen waarmee de controle over de configuratie geregeld is en dus de eisen ten aan zien van beveiliging afgedwongen worden. Voorbeeld hiervan is het kunnen afdwingen van het vergrendelen van het toestel door het verplichten van een pincode. Voor ontvangst van het toestel heeft de medewerker gelegitimeerd en is de ontvangst vastgelegd waarbij meteen het akkoord voor de werkkostenregeling is geregeld. De uitgegeven toestellen worden in de administratie opgenomen waarmee bij incidenten als verlies of diefstal bij melding meteen de benodigde acties, zoals het van afstand wissen, kunnen worden uitgevoerd.

Voor het privé gebruik van de toestellen is nog geen Bring Your Own Device (BYOD) beleid gemaakt. Tablets die uitgegeven worden ook beheerd binnen de MDM-portal. Binnen gemeente Assen worden leenlaptops uitgegeven, deze laptop worden niet op het netwerk aangesloten. De laptops bieden de mogelijkheid om mobiel te werken waarbij altijd met two-factor authenticatie ingelogd moet worden.

Advies:

- *Voer naast de technische maatregelen ook gedragsregels in omtrent privé gebruik.*

Sociaal Domein

 Gedefinieerd en gecontroleerd

Binnen het sociaal domein is privacy een primair aandachtspunt bij de uitvoering van de processen. Het uitwisselen van gegevens gaat via het landelijk berichtenverkeer of bij uitwisseling met niet aangesloten partijen via cryptshare. Er is geen voorlichting over datalekken geweest, maar het is wel bekend bij wie een datalek gemeld moet worden. Er is via de Functionaris Gegevensbescherming aandacht voor datalekken en er zijn in overleg met de Functionaris Gegevensbescherming bewerkersovereenkomsten afgesloten. De procedure voor autorisatie op basis van rollen is vastgelegd met daarin specifiek aandacht voor functiescheiding. Er is een periodieke controle ingericht waarbij 1x per half jaar gecontroleerd wordt op de uitgegeven autorisaties. In de gebruikte applicatie is voor de eventuele benodigde audit-trails logging op mutaties van gegevens ingeregeld.

Advies:

- *Zorg voor een extra voorlichting op het gebied van datalekken*

Informatie-uitwisseling met ketenpartners

 Gedefinieerd en gecontroleerd

De samenwerking Drentsche Aa is in praktische zin per 1-11-2015 gestart. De medewerkers waarvoor dit geldt doen dezelfde werkzaamheden, voor hun oude gemeente, als voor 2015. Ze werken nu nog met dezelfde toegangsrechten binnen dezelfde applicaties als voor 1-11-2015. Deze medewerkers die nu gedetacheerd zijn in de “ontvangende” gemeente komen in het eerste kwartaal van 2018 in dienst bij de betreffende gemeente. Op dit moment loopt het proces om sluitende afspraken over het inloggen en gebruiken van applicaties door medewerkers van een samenwerkingsgemeente bij de andere gemeenten vast te leggen.

De gemeente Assen heeft een aantal applicaties in beheer die gebruikt worden door de gemeente Tynaarlo en de gemeente Aa & Hunze. De gemeente Tynaarlo maakt gebruikt van de applicaties Beaufort en YouForce.
De gemeente AA & Hunze maakt gebuikt van het financiële pakket Coda en het zaaksysteem van de gemeente Assen.

Voor deze applicaties gelden dat ze in beheer zijn bij Assen en de maatregelen rondom autorisaties gelden die ook binnen de gemeente Assen van toepassing zijn. Dit betekent dat de aanvraag en controle van autorisaties geborgd is en hiermee maatregelen tegen onbevoegde inzage zijn ingeregeld.

Een aandachtspunt bij de samenwerking is de afstemming rondom wijzigings- en incidentbeheer van de samenwerkende partijen.

Advies:

- *Maak heldere afspraken over het wijzigings- en incidentbeheer rondom de gezamenlijke voorzieningen*

3.4 Aspect Techniek

Aanpak

De rekenkamercommissie van de gemeente Assen heeft besloten de beveiliging van het interne en externe netwerk te laten toetsen. Onderdeel hiervan was een toets in hoeverre de kwetsbaarheden uit het vorige onderzoek zijn verholpen (her-test), een test om vast te stellen dat er geen nieuwe kwetsbaarheden zijn ontstaan (regressie-test) en een beoordeling van de beveiliging van maximaal vijf kritische systemen, o.a. in het Sociaal Domein. In de uitvoering is meegenomen; de penetratietest (hierna pentest) op het interne, externe en draadloze netwerk van de gemeente Assen. Onderzocht is of het mogelijk is op enigerlei wijze toegang te krijgen is vanaf binnen en buitenaf tot de systemen en gegevens. Met andere woorden hoeveel moeite kost het om de beveiliging te doorbreken en wat kun je zien als dit gelukt is.

Daarnaast wordt een risicoaanduiding gegeven en wordt een mogelijke oplossing gegeven die de kwetsbaarheid wegneemt. In een gegeven hoeveelheid tijd —time-box— zijn zoveel mogelijk zwakke plekken in kaart gebracht. Zo is er onderzocht of bijvoorbeeld netwerk segmentatie aanwezig is. Zijn er kritische kwetsbaarheden aanwezig? Wat kan een kwaadwillende gebruiker misbruiken om toegang te krijgen tot gevoelige informatie?

De onderstaande indeling is gehanteerd om de uitkomsten van de kwetsbaarheden scan te waarderen.

Niveau 1 **Zeer onveilig**

Eén of meerdere bevindingen met een hoog risico zijn aangetroffen.

Niveau 2 **Onveilig**

Eén of meerdere bevindingen met een gemiddeld risico zijn aangetroffen en geen hoog risico.

Niveau 3 **Veilig**

Eén of meerdere bevindingen met een laag risico zijn aangetroffen en geen gemiddeld en/of hoog risico

Niveau 4 **Zeer veilig**

Geen bevindingen met enig risico zijn aangetroffen.

Resultaten

Op basis van de bevindingen van het onderzoek wordt de beveiliging van het interne en externe netwerk van de gemeente Assen beoordeeld als ‘**zeer onveilig**’ op het moment van het vervolgonderzoek.

Zeer Onveilig

Er zijn meerdere kwetsbaarheden aangetroffen met een kritisch en hoog risico. Binnen de gegeven tijd is ITsec erin geslaagd om de beveiliging van het interne netwerk te doorbreken. Het onderzoek van ITsec is opgedeeld in een her-test, een regressie-test en een beoordeling van de beveiliging van vijf kritische systemen o.a. in het sociaal domein en de systemen voor informatie-uitwisseling met ketenpartners.

Ten opzichte van het voorgaande onderzoek zijn de volgende verbeteringen geconstateerd:

- Het patch management is aanzienlijk verbeterd. Verouderde software is minder grootschalig aanwezig dan voorheen waardoor het moeilijker wordt misbruik te maken van kwetsbaarheden in aanwezige besturingssystemen, software en web-applicaties.
- Werkstations zijn beter beveiligd ten opzichte van het vorige onderzoek.
- Algeheel worden aanbevelingen die voortkomen uit voorgaande onderzoeken structureel opgevolgd.

De beveiliging van het externe netwerk is beperkt getest tijdens het onderzoek.
Het resultaat als gevolg van misbruik van aangetroffen kwetsbaarheden op het interne netwerk wordt geïllustreerd aan de hand van de volgende situaties.

- Het is mogelijk om aanwezige functionaliteit van het besturingssysteem te misbruiken om zodoende verdere toegang en rechten te verschaffen tot het getroffen doelsysteem en overige systemen in het netwerk.
- Omdat medewerkers bestanden op onvoldoende afgeschermde locaties hadden geplaatst, is het mogelijk gedeelde mappen van verschillende afdelingen binnen de gemeente Assen te bereiken. Daardoor kon vertrouwelijke documenten met onder andere wachtwoorden, financiële informatie, persoonlijke informatie en gegevens van burgers worden ingezien. Het gaat hier om voornamen, achternamen, adresgegevens en BSN-nummers.
- Als gevolg van een gebrek aan authenticatie bleek het mogelijk om de e-mail servers van de gemeente Assen te instrueren op een manier waarbij impersonatie van een willekeurig e-mail adres (binnen het gemeente Assen domein) tot stand komt. Een kwaadwillende zou zich kunnen voordoen als een willekeurige gebruiker met een @assen.nl e-mail adres.

Er zijn op korte termijn verbeteringen noodzakelijk om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te kunnen garanderen. Hierbij moet er rekening worden gehouden met bijvoorbeeld het configuratiemanagement en hardening van het netwerk en haar doelsystemen.
Een geïmplementeerd ‘baseline hardening’ beleid gebaseerd op het advies zoals beschreven in het technisch rapport sluit niet alleen mogelijke veiligheidsrisico’s uit. Tevens vermindert dit de complexiteit van nieuw in productie genomen doelsystemen en maakt dit de betreffender doelsystemen beheersbaarder voor de IT-afdeling.

Gezien de vertrouwelijkheid van de informatie wordt voor de verdere technische rapportage verwezen naar het separaat opgeleverde technisch rapport.

4 Bijlagen

Bronnen en afkortingen

De volgende personen waren betrokken bij de vervolgonderzoek:

Onderwerp	Namen
Beveiligingsbeleid;	Arnoud Bijvoet
Fysieke toegangsbeveiliging	Ingeborg ter Veen
Wijzigingsbeheer	Richard Krist
Incidentbeheer	Niels Boorsma
Contract- en servicemanagement	Jan Bosma
Beveiliging van (web)applicaties Logische toegangsbeveiliging (autorisaties)	Patrick Fekkes
Continuïteit.	Ans Timmerman
Compliance (naleving wet- en regelgeving).	Arnoud Bijvoet
Mobile device management;	Cor Hardebil
Meldplicht datalekken	Jelmar de Vries
De beveiligingsmaatregelen voor het Sociaal Domein	Rob Kah Johnny Samallo Erik Jan Vens
SLA met ketenpartners	Jan Bosma
Contract en servicemanagement	Richard Krist Jan Bosma Ans Timmerman
Informatie-uitwisseling met ketenpartners	Robert Arntzenuis Patrick Fekkes

Verklaring van veel gebruikte afkortingen:

Afkorting	Verklaring
AP	Autoriteit Persoonsgegevenvs
AVG	Algemene Verordening Persoonsgegevens
BIA	Business Impact Assessment
CMDB	Configuation Management Data Base
FG	Functionaris Gegevensbescherming
ISMS	Information Security Management System
PIA	Privacy Impact Assessment
SaaS	Software as a Service
WBP	Wet Bescherming Persoonsgegevens

Cobit Framework versie 4.1. Maturity Model

APPENDIX III—MATURITY MODEL FOR INTERNAL CONTROL

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organised occasionally.
5 Optimised	An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes, and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organisation benchmarks to external good practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Voor meer informatie zie: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx

Onderzoeksbureau:

Het onderzoek is uitgevoerd door de consultants van Insite Securtiy en Itsec (onderdeel Insite Groep):

Naam	Onderdeel
drs. Lourens W. Dijkstra MMC CISM	Onderdeel mens en projectleiding
Dennie Oosterbaan	Onderdeel organisatie
Pieter Compaan (ITsec)	Onderdeel techniek