Jaarverslag Informatiebeveiliging 2019 Hollands Kroon

Auteurs:
Tarik Fakir: Chief information security officer
Ronald Zwaan: Controller (Ensia coördinator)

Inhoudsopgave

1 Inleiding

Onder informatieveiligheid wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Belangrijke aspecten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en kritische (organisatorische) informatie en maatregelen.

Dit jaarverslag is een verantwoording over de kwaliteit van de informatiebeveiliging over 2019. Met het jaarverslag legt het college verantwoording af aan de gemeenteraad en aan het Rijk en haar toezichthouders. Het jaarverslag is tot stand gekomen door zelfevaluaties waarin de kwaliteit van de informatiebeveiliging is beoordeeld aan de hand van de normen van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG geeft richtlijnen voor een beheersing van de informatiebeveiliging door het inrichten en uitvoeren van een set van organisatorische en technische beheersmaatregelen.

Dit jaarverslag is vormvrij. Wij hebben ervoor gekozen de informatiebeveiliging in 2019 op hoofdlijnen te beschrijven aan de hand van een toetsing in hoeverre de normen van de BIG zijn gerealiseerd en nageleefd. Deze verantwoording is een meting van de kwaliteit van de informatiebeveiliging in 2019. In dit jaarverslag en volgende jaarverslagen wordt de kwaliteit ten opzichte van het voorgaande jaar vergeleken en toegelicht. Dat geeft inzicht in de inspanningen die de organisatie doet om de informatiebeveiliging te vergroten en op een hoger niveau te brengen.

2 Managementsamenvatting

Dit verslag geeft de uitkomsten weer van de gemeente brede (horizontaal) uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2019. Deze zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG)[1]. Wij rapporteren op één moment in het jaar over de status van onze informatieveiligheid. De methodiek heet ENSIA en staat voor Eenduidig Normatiek Single Information Audit.

Vanuit deze horizontale (gemeente brede) zelfevaluatie is eveneens de verantwoording aan de stelselhouders/toezichthouders afgeleid, de zogenaamde verticale verantwoording. Zo zijn de verantwoordingen (Uittreksels) over de Basisregistratie Personen (BRP) en de Paspoortuitvoeringsregeling (PUN) op 14 februari 2020 toegestuurd naar de Rijksdienst voor Identiteitsgegevens, de Autoriteit Persoonsgegevens en het Ministerie van BZK.

De verantwoordingen over de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT) en de Basisregistratie Ondergrond zijn tijdig vóór 1 mei 2020 opgeleverd aan het Ministerie van I&W[2]. De verantwoordingen voor Suwinet en DigiD zijn eveneens tijdig vóór 1 juni 2020 aan de stelselhouders (ministerie van SZW en Logius) verantwoord door middel van een Collegeverklaring Informatiebeveiliging op basis van de bevindingen uit onze zelfevaluatie. Deze zelfevaluatie is getoetst door een externe IT-auditor. De IT-auditor heeft de Collegeverklaring op juistheid beoordeeld en heeft de uitkomsten van zijn onderzoek vermeld in een Assurancerapport. Met beide documenten voldoen wij aan de verantwoordingsplicht voor Suwinet en DigiD.

Algemeen beeld en resultaten afgelopen periode

[1] Gemeenten hebben met aanname van de resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente” in november 2013 deze Baseline Informatieveiligheid Nederlandse Gemeenten (BIG) als hét gemeentelijk basisnormenkader voor informatieveiligheid omarmd.

[2] De BAG, BGT en BRO kennen elk in ENSIA ook een domein specifieke vragenlijst en een specifieke rapportage. Deze is separaat voorgelegd aan het College ter vaststelling en aangeboden aan het Ministerie van I&W.

De conclusie is dat de organisatie in 2019, evenals in 2018, overall adequate beheersmaatregelen heeft getroffen op het terrein van informatiebeveiliging. De organisatie handelt en werkt pragmatisch. Op onderdelen ontbreekt echter nog wel vastgesteld beleid, processen (procesbeschrijvingen, vastgestelde richtlijnen en werkinstructies) en proceseigenaarschap. Over de implementatie en borging van de informatieveiligheid is in Mei 2020 gerapporteerd aan het college.

Hieronder is een overzicht opgenomen van de deelgebieden van de BIG en hoe wij deze beoordelen. In het jaarverslag kunt u teruglezen hoe tot deze beoordeling is gekomen en welke verbeteracties er zijn doorgevoerd en nog noodzakelijk zijn.

	jaarverslag ENSIA 2019	
3.1	Implementatie tactische baseline	X O
3.2	Samenwerkingsverbanden	n.v.t.
3.3	Beveiligingsbeleid	OX
3.4	Organisatie van de informatiebeveiliging	X O
3.5	Beheer bedrijfsmiddelen	X O
3.6	Personele beveiliging	XO
3.7	Fysieke beveiliging / beveiliging omgeving	OX
3.8	Beheer communicatie	X O
3.9	Toegangsbeveiliging	OX
3.10	Verwerven / ontw. en onderh. info.systemen	X O
3.11	Beheer informatiebeveiligingsincidenten	X O
3.12	Bedrijfscontinuiteitsbeheer	X O
3.13	Naleving	X O
	Legenda	
	X= 2018	
	O= 2019	

In 2018 en 2019 zijn een aantal maatregelen genomen om de informatiebeveiliging naar een hoger niveau te tillen. Hierbij moet opgemerkt worden dat een 100% beveiliging niet kan worden gegarandeerd. Organisatorische en technische maatregelen (Hard controls) zijn niet waterdicht en hebben hun prijs. Op basis van een risicoanalyse is een noodzakelijk pakket maatregelen en middelen gerealiseerd. Risico's van datalekken en hacken blijven altijd aanwezig, maar de organisatie tracht deze risico's tot een minimum te beperken.

Gedrag, veiligheidsbewustzijn en risicobewustzijn (Soft controls) van medewerkers hebben grote invloed op de informatieveiligheid. Uit de praktijk is gebleken dat veel van de veiligheidsincidenten zijn veroorzaakt door de menselijke factor. Onzorgvuldig handelen en onbewuste fouten vinden nu eenmaal plaats in een omgeving waar gewerkt wordt. Om dit zoveel mogelijk te beperken zijn en worden er bewustwordingsdagen georganiseerd en worden de medewerkers via interne communicatiekanalen op de hoogte gehouden over verschillende informatiebeveiligings-onderwerpen en actuele fraude-, phishing- hackrisico's. Daarnaast is het ISMS een essentieel onderdeel voor de PDCA (plan, do, check, act) cyclus. Mede hierdoor worden de normen waaraan voldaan moet worden op de agenda gezet en is men zich dus hiervan bewust.

In 2019 is Hollands Kroon niet geconfronteerd met sancties van de Autoriteit Persoonsgegevens (boetes), Logius (afsluiten Digi-D) en BKWI (afsluiten Suwinet).

Er zijn In 2019 maatregelen getroffen van technische en organisatorische aard. Hierbij is het verbeterplan dat in 2018 is opgesteld, tegen het licht gehouden. Hieruit zijn een aantal verbeteringen doorgevoerd zoals het uitwerken en implementeren van het ISMS. Dit systeem helpt ons om te sturen op de beveiliging van onze IT-onderdelen, processen en gewenst gedrag van medewerkers. Met behulp van een plan, do, check, act (pdca) cyclus worden dreigingen van buitenaf en behoeften van binnenuit gecoördineerd. Hierbij wordt gestuurd op normen in het kader van wet en regelgeving en op ons organisatiebeleid en strategie.

Verder zijn er een aantal trajecten gestart die onderdeel uitmaken van onze security roadmap. Deze roadmap is

een plan van aanpak opgezet in een chronologisch bepaalde volgorde dat bestaat uit onder meer: het opzetten en onderhouden van onze digitale identiteiten, het veilig uitwisselen van gegevens voor medewerkers, ketenpartners en inwoners en het verhogen van de digitale weerbaarheid en beveiliging van de infrastructuur door aansluiting op het landelijke GGI-Veilig[3]. Ook zijn bewustwording dagen georganiseerd waarbij medewerkers geattendeerd worden op de gevaren van phishing en hacken door middel van workshops en trainingen.

In deze verantwoording informeren wij u over de BIO-norm die de BIG-norm heeft vervangen in 2020. BIO staat voor Baseline Informatiebeveiliging Overheid. De BIO verschilt in een aantal opzichten van de BIG. Er zijn in de BIO ten opzichte van de BIG ongeveer 200 maatregelen geschrapt om meer ruimte te bieden voor de relevante maatregelen die voor ons als gemeente ertoe doen. Dit nieuwe normenkader is meer gemeente specifiek en staat in het teken van risicobeheersing. De BIO beoogt het college meer te positioneren in een rol waarbij risico-gebaseerd gestuurd wordt. In 2019 is gestart met een aantal voorbereidingen voor de implementatie van de BIO. Hierbij zijn maatregelen geprioriteerd en zijn deze toebedeeld aan verschillende (proces) eigenaren die verantwoordelijk zijn voor het uitvoeren hiervan.

De CISO ziet vanuit een coördinerende rol toe op een juiste en tijdige uitvoering van de veiligheidsmaatregelen. Het jaarverslag over 2020 wordt dan ook opgesteld volgens het BIO-normenkader. Vergelijking met het jaarverslag over 2019 is niet mogelijk, omdat de normenkaders verschillen.

Verder informeren wij u ook over de afwezigheid van onze functionaris gegevens bescherming (hierna FG). Vanaf oktober 2019 is de FG van Hollands Kroon langdurig ziek geweest. Taken en verantwoordelijkheden die gepaard gaan met deze rol zijn toebedeeld waar mogelijk. Hierbij is rekening gehouden met bepaalde richtlijnen, zoals rolvermenging. De organisatie houdt zich sinds februari 2020 bezig met een nieuwe invulling van de FG rol. Dit is projectmatig opgepakt en zal naar verwachting in september 2020 opgeleverd gaan worden.

3 Verantwoording volgens indeling van de BIG

[3] GGI-Veilig is een initiatief van de VNG en helpt gemeenten hun digitale weerbaarheid te verhogen en hun ICT-infrastructuur veiliger te maken. GGI-Veilig bestaat uit een portfolio van producten en diensten voor operationele informatiebeveiliging. Via GGI-Veilig nemen gemeenten onder meer actieve netwerk monitoring af voor het bewaken van dataverkeer op het eigen bedrijfsnetwerk. Ook worden beveiligingsproducten voor de gemeentelijke ICT-infrastructuur afgenomen (zoals bijvoorbeeld firewalls, anti-DDOS, end-point protection). Tot slot kunnen beveiligingsexpertise diensten worden afgenomen.

3.1 Implementatie van de Tactische Baseline (Hoofdstuk 3 van de BIG)

De gemeentelijke organisatie beschikt over een vastgesteld Informatiebeveiligingsbeleid. Wat ontbreekt is een jaarplan met concrete actiepunten. Het jaarplan op basis van de BIG wordt niet meer opgesteld. In plaats daarvan wordt gewerkt aan een jaarplan op basis van de BIO. Deze wordt in juli 2020 gepresenteerd aan het bestuur zodat een duidelijk beeld ontstaat in hoe ver de gemeente is in de uitvoering van de BIO-normen. Deze wordt jaarlijks geactualiseerd en geeft aan welke beveiligingsmaatregelen moeten worden uitgevoerd. Het ISMS wordt hiervoor ingezet en bewaakt en monitort de te nemen maatregelen. Deze maatregelen worden dan toegewezen aan verantwoordelijke proceseigenaren (entiteiten) binnen onze organisatie. De CISO (Security Officer) bewaakt, coördineert en ziet toe op de uitvoering van de maatregelen.

Door het inzetten en verder uitwerken van het ISMS is dit onderdeel verbeterd ten opzichte van vorig jaar.

3.2 Samenwerkingsverbanden (Hoofdstuk 4 van de BIG)

Alle gemeentelijke taken in het kader van digitale gegevensuitwisseling worden binnen de IT-infrastructuur van Hollands Kroon uitgevoerd.

Dit onderdeel is dan ook niet van toepassing.

3.3 Beveiligingsbeleid (Hoofdstuk 5 van de BIG)

Over 2019 beschikt de gemeente nog over een op basis van de BIG vastgesteld beleid.
Op dit moment beschikt de gemeente nog niet over een door het college vastgesteld beleid conform de BIO. Het huidige beleid is nog gebaseerd op het BIG-normenkader. Naar verwachting wordt het nieuwe beleid in augustus 2020 formeel vastgesteld. Het nog niet hebben van een vastgesteld actueel beleid gebaseerd op het BIO-normenkader weerhoudt ons er echter niet van om aan de slag te gaan met het invoeren van de BIO.

Ten opzichte van vorig jaar is dit onderdeel ongewijzigd.

3.4 Status van organisatie van de Informatiebeveiliging (Hoofdstuk 6 van de BIG)

De gemeente beschikt in 2019 over een door het college vastgesteld beveiligingsbeleid. Wat ontbreekt is een jaarlijkse rapportage waarin het college wordt geïnformeerd over de kwaliteit (opzet, bestaan en werking van informatiebeveiligingsmaatregelen) van de informatiebeveiliging en de uitvoering van de

beveiligingsmaatregelen en de noodzaak van nog te ontwikkelen en uit te voeren beveiligingsmaatregelen en de naleving daarvan vanuit het implementatieplan BIG. Het aangeschafte Information Security Management Systeem (ISMS) ondersteunt het vervaardigen van een jaarlijkse rapportage en wordt ingezet om in 2020 te rapporteren over de implementatie van de BIO.

Voor de coördinatie van de beveiliging beschikt de gemeente over een CISO (Chief Information Security Officer).

De organisatie beschikt nog niet over een formeel goedkeuringsproces voor nieuwe ICT-voorzieningen. Het goedkeuringsproces waarborgt het onder controle houden van nieuwe IT-voorzieningen. Dat is essentieel voor het stabiel houden van de ICT-omgeving, maar ook om beveiligingsmaatregelen effectief te kunnen implementeren. De geheimhouding met betrekking tot vertrouwelijke informatie is in de organisatie geregeld voor zowel de eigen medewerkers als externe medewerkers. Geheimhouding en verantwoordelijkheden voor gecontracteerde (keten) partners worden vastgelegd in een verwerkersovereenkomst. Een verwerkersovereenkomst geeft inzicht in het identificeren van eventuele risico's die betrekking hebben op deze partners.

De Raad is in 2019 op hoofdlijnen geïnformeerd over de kwaliteit van onze informatiebeveiliging. Het college legt ook over 2019 verantwoording af over de huidige kwaliteit en uitvoering van de beveiligingsmaatregelen volgens de ENSIA-methodiek.

Ten opzichte van vorig jaar is dit onderdeel nauwelijks verbeterd, De aanschaf van het ISMS is voor het grootste gedeelte ingezet om ons voor te bereiden op de BIO. Wel is een duidelijker beeld ontstaan wat betreft het vormgeven van een risicoprofiel op onze huidige en potentiele (keten) partners.

3.5 Beheer van bedrijfsmiddelen (Hoofdstuk 7 van de BIG)

De organisatie heeft voor 80% de bedrijfsmiddelen geïnventariseerd. Dit is grotendeels van toepassing op het onderdeel hardware, software en alle overige digitale voorzieningen. Het inventariseren van onze licenties moet nog plaatsvinden. De ambitie is om in 2020 een 100% inventarisatie te hebben uitgevoerd.

In een database dient een volledig en actueel overzicht te worden opgenomen van bedrijfsmiddelen, informatie, software, hardware en diensten. Daarmee is de organisatie in staat om een juiste inschatting te maken bij grote wijzigingen van informatiesystemen en processen en wordt voldaan aan patchmanagement en het maken van een planning bij vervanging van hard- en software. Bij calamiteiten en cyberaanvallen biedt deze database snel inzicht om de impact te bepalen.

Zelfsturende teams zijn verantwoordelijk voor het gebruik en onderhoud van een deel van de bedrijfsmiddelen (laptop en telefoon). Voor het gebruik daarvan is beleid opgesteld met betrekking tot gedocumenteerde en geïmplementeerde ICT-voorzieningen en het aanvaardbaar gebruik van informatie en bedrijfsmiddelen. Dit beleid geeft aan hoe en met welke ICT-voorzieningen wordt gewerkt en geeft inzicht in de normen over het aanvaardbare gebruik van informatie en bedrijfsmiddelen. Namens de Directie wordt toezicht uitgevoerd op het efficiënt en veilig gebruik van bedrijfsmiddelen.

Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie. De organisatie heeft hiervoor de rubriceringrichtlijnen van de IBD (informatiebeveiliging dienst) ingezet, hiermee wordt onderscheid gemaakt tussen herleidbare en niet herleidbare persoonsgegevens. Met rubricerings- of classificatierichtlijnen kan het beschermingsniveau worden beoordeeld door het analyseren van de vertrouwelijkheid, integriteit en beschikbaarheid en andere eisen voor de informatie. Daarnaast dienen procedures te worden (door)ontwikkeld op basis van uit te voeren dataclassificaties, zodat informatie het juiste niveau van bescherming krijgt. Deze procedures zijn ook bruikbaar voor de labeling en de verwerking van informatie.

Ten opzichte van vorig jaar is dit onderdeel licht verbeterd door de inventarisatie van bedrijfsmiddelen. Een classificatie van data heeft plaatsgevonden op onder meer de onderdelen Digi-D en Suwinet. Verder wordt in het informatiestromen programma de classificatie van data direct meegenomen tijdens het project.

3.6 Personele Beveiliging (Hoofdstuk 8 van de BIG)

Rollen en verantwoordelijkheden van medewerkers, ingehuurd personeel en externe gebruikers met betrekking tot informatiebeveiliging zijn niet expliciet vastgelegd. Informatiebeveiliging is een onderdeel van de totale bedrijfsvoering. De achtergrond van kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers worden niet gescreend in relatie tot de eisen volgend uit de classificatie van informatie waar men toegang toe krijgt. De organisatie maakt geen gebruik van het opvragen van de verklaring omtrent het Gedrag (VOG). In plaats daarvan ondertekent iedere medewerker een integriteitsverklaring en wordt er een eed of belofte afgelegd.

Medewerkers, ingehuurd personeel en externe gebruikers hebben de voorwaarden met betrekking tot hun verantwoordelijkheden ten aanzien van informatiebeveiliging en privacy eisen, niet specifiek ter kennisname gekregen en aanvaard. De organisatie hanteert voor het functioneren en handelen van medewerkers de kernwaarden. Verantwoordelijk zijn voor informatiebeveiliging maakt daar onderdeel van uit. In de organisatie zijn trainingen gegeven om het naleven van beveiligingsmaatregelen te bevorderen en bewust te zijn van beveiligingsrisico’s. Vanuit organisatorisch oogpunt is de verantwoordelijkheid voor informatieveiligheid

onderdeel van elk zelfsturend team. Dat geldt ook voor andere verantwoordelijkheden op het terrein van integrale bedrijfsvoering, zoals P&O taken, financiën (budgetbeheer) en interne controlemaatregelen.

Behalve het hanteren van de kernwaarden houdt de organisatie ook rekening met account – en autorisatiebeheer die worden uitgevoerd overeenkomstig de eisen vanuit wet- en regelgeving. Op enkele uitvoeringstaken van de gemeente, zoals op het gebied van het Sociaal domein en Persoonsinformatie, zijn strengere procedures voorgeschreven. Deze strengere en zwaardere specifieke eisen worden toegepast en uitgevoerd.

Ten opzichte van vorig jaar is dit onderdeel ongewijzigd.

3.7 Fysieke beveiliging en beveiliging van de omgeving (Hoofdstuk 9 van de BIG)

De gemeente heeft gepaste toegangsbeveiligingsmaatregelen genomen voor ruimtes waar zich informatie en ICT-voorzieningen bevinden. De toegang tot de gebouwen en de beveiligde zones is uitsluitend mogelijk voor geautoriseerde personen. Ook zijn (binnen de kantoren/ ruimtes) maatregelen getroffen voor de bescherming van mobiele gegevens- en andere informatie (dragers). Voorbeelden daarvan zijn lockers en kluizen.

De organisatie heeft maatregelen genomen die bescherming bieden tegen schade door geweld van buiten. De gemeente is verzekerd tegen brand, bliksem en explosies. De gemeente heeft maatregelen getroffen en procedures geïmplementeerd voor het werken in en toezien op beveiligde ruimtes.

Publiek toegankelijke ruimtes zijn afgeschermd zodat onbevoegden zich geen vrije toegang kunnen verschaffen tot bedrijfsmiddelen. Apparatuur wordt overeenkomstig de voorschriften geplaatst en gebruikt zodat het risico van schade, storing en onbevoegde toegang verminderd worden. Ook zijn maatregelen getroffen en procedures geïmplementeerd om uitval van apparatuur te voorkomen door stroomuitval of onderbreking van de nutsvoorzieningen.

De doelstelling van de fysieke beveiliging is om gebouwen, terreinen en informatiesystemen te beschermen tegen onbevoegde toegang, schade en/of verstoring van continuïteit. Hier hangen strenge eisen aan die jaarlijks getoetst worden op relevantie, juistheid en werking en geborgd worden bij het proces van in en uitstroom van nieuwe medewerkers.

Er is een richtlijn voor het veilig verwijderen van alle gevoelige (vertrouwelijke) informatie op IT-middelen die worden gerepareerd of niet meer worden gebruikt. Alle apparatuur die opslagmedia bevat, wordt

gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

Ten opzichte van vorig jaar is dit onderdeel ongewijzigd.

3.8 Beheer van Communicatie en bedieningsprocessen (Hoofdstuk 10 van de BIG)

De organisatie beschikt over gedocumenteerde en actuele bedieningsprocedures, die beschikbaar worden gesteld aan alle gebruikers die deze nodig hebben. Ook beschikt de organisatie over een procedure voor het beheerst uitvoeren van wijzigingen op de IT-voorzieningen. Deze is echter niet gedocumenteerd.

Organisatorisch is functiescheiding toegepast. Zo beschikt de organisatie onder meer over afzonderlijke functies, zoals een (concern) controller, een CISO, een Functionaris Gegevensbescherming, systeembeheerders en applicatiebeheerders. Dat draagt bij aan het verlagen van het risico dat onbevoegd of onbedoeld wijzigingen worden aangebracht in informatiesystemen en of dat misbruik van bedrijfsmiddelen plaatsvindt.

Voor de uitbestede IT-diensten zijn naast de afgesproken dienstenniveaus, ook alle relevante beveiligingseisen opgenomen in de contracten met de IT-leveranciers en/of verwerkers. In 2019 is niet getoetst dat de IT-leveranciers en/of verwerkers zich ook houden aan de afgesproken diensten niveaus en informatiebeveiligingseisen. Een aandachtspunt is om met partijen waaraan IT-diensten zijn uitbesteed periodiek overleg te voeren over bestaan en actualiteit van IB-maatregelen rondom beschikbaarheid, bescherming, continuïteit van de IT-voorziening/ -diensten en maatregelen af te spreken waarmee de afgesproken actuele en toekomstig systeembelasting inzichtelijk en op voldoende niveau is.

Daarnaast is als verbeterpunt een formeel gedocumenteerde IT-wijzigingen beheer procedure aan te dragen. Hiermee is bij een beoogde IT-wijziging gemakkelijker een impactanalyse uitvoerbaar. Dit in het belang van de borging van de bedrijfscontinuïteit.

De organisatie heeft een formele testprocedure voor accepteren van nieuwe en gewijzigde systemen.
De organisatie beschikt over (antivirus) maatregelen voor detectie, preventie en herstellen om te beschermen tegen virussen en malware en er bestaan activiteiten om het bewustzijn van de gebruikers te vergroten. Ook heeft de organisatie een actueel back-up beleid en worden back-ups getest en opgeslagen op meerdere locaties voor redundantie.

De organisatie heeft adequate maatregelen genomen om de aanwezige netwerken beter te monitoren en te beveiligen. Daarvoor is een service operations center (SOC) dienst afgenomen waarbij een partij proactief

adviseert bij verdacht netwerkverkeer. Deze partij houdt 24/7 ons netwerkverkeer in de gaten. Hiermee wordt onze weerbaarheid naar een hoger niveau getild.

Er bestaan procedures en maatregelen voor het beheer en de beveiliging van informatie op papier en op (verwijderbare) elektronische gegevensdragers zoals laptops, usb-sticks, externe disks en back-up tapes. Er zijn procedures voor verwijderen/vernietigen van informatie en voor de behandeling en opslag van informatie. Gegevens worden op een veilige en beveiligde manier verwijderd als deze niet langer nodig zijn. Onze systeemdocumentatie is geclassificeerd beveiligd met een wachtwoord die enkel toegankelijk is voor bevoegde entiteiten binnen de organisatie.

Er bestaat beleid en er zijn procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling, zowel binnen als buiten de gemeente. Het heeft betrekking op digitale transport van geclassificeerde informatie. Ook beschikt de organisatie over overeenkomsten voor de beheerste en beveiligde wijze van informatie-uitwisseling met andere partijen. Aandachtspunt is dat de uitwisselingsrichtlijnen nog niet bij alle medewerkers bekend zijn. Hiervoor is de organisatie gedurende 2019 meermaals via interne communicatiekanalen erop gewezen hoe deze er precies uitzien.

De gemeente beschikt over procedures waarmee vertrouwelijke informatie op de kantoorautomatisering omgeving op adequate en afdoende wijze wordt beveiligd. Aandachtspunt is dat de risico's en onderlinge verbanden nog niet in kaart zijn gebracht.

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd in audit-logbestanden. Deze logbestanden worden een overeengekomen periode bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. Met het controleren van logbestanden worden eventuele onbevoegde informatieverwerkingsactiviteiten ontdekt.

Ten opzichte van vorig jaar is dit onderdeel ongewijzigd. Er zijn weliswaar stappen genomen om voor de kritische informatiesystemen een dataclassificatie uit te voeren. Het reactief handelen van de beveiliging van het netwerkverkeer brengt hoge risico's met zich mee. Het is van vitaal belang dat er zicht en grip ontstaat op wat voor dataverkeer er precies de organisatie inkomt en uitgaat. Helemaal als wij kijken naar de wereldwijde groei van malware en ransomware aanvallen.

3.9 Toegangsbeveiliging (Hoofdstuk 11 van de BIG)

Er Is beleid vastgesteld dat richting geeft aan de beheerste logische toegang tot gegevens en informatie. Onderdeel daarvan is een vastgestelde autorisatieprocedure voor het administreren van gebruikers en het toekennen/ intrekken van toegangsrechten voor alle informatie en –systemen en de controle daarop.

Aandachtspunt is dat een procedure voor de vormgeving en het (veilig) uitgeven en opslaan van wachtwoorden en andere authenticatie middelen nog moet worden vastgesteld.

In de praktijk is echter wel sprake van maatregelen met betrekking tot wachtwoorden, zoals uitgifte, geheimhouding, lengte en samenstelling van het aantal karakters en de gebruikersduur van een wachtwoord. De toegangsrechten van gebruikers worden regelmatig beoordeeld in een formeel proces. Deze controles worden echter niet in verslagen vastgelegd. Alle medewerkers worden regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van wachtwoorden. De organisatie hanteert de eisen die zijn opgenomen in hoofdstuk 11.2.3 van de BIG.

Alle medewerkers worden regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van hun mobiele apparatuur, zoals laptops, smartphones en tablets. Er wordt echter wel gebruik gemaakt van geautomatiseerde (technisch afgedwongen) beleidsregels (Engels: policy) ter voorkoming van misbruik. De organisatie beschikt over een clear desk-beleid voor papier, usb-sticks, externe schijven en mobiele devices en een clear screen-beleid voor ICT-voorzieningen.

De organisatie heeft een formele procedure voor het toekennen van toegangsrechten voor het netwerk en netwerkdiensten. Tweefactor authenticatie maakt onderdeel uit van het authentiseren van (externe) gebruikers voor toegang tot het netwerk. De organisatie heeft voldoende maatregelen getroffen voor de toegangsbeheersing van de netwerken.

De toegangsbeveiliging voor besturingssystemen is voldoende ingericht door gebruik van onder meer een inlogprocedure, gebruikersidentificatie en -authenticatie, systeem van wachtwoordenbeheer, vergrendeling na periode van inactiviteit en beperking van verbindingstijd door onderhoud door IT-leveranciers.

De toegangsbeheersing voor toepassingen en informatie is voldoende door toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel te beperken en systemen met risicovolle informatie in een eigen omgeving (netwerksegment) onder te brengen zodat dat 'logisch of fysiek gescheiden' is van de rest van het netwerk.

De toegang van gebruikers in een gemeenschappelijk netwerk (met andere organisaties) is ingericht volgens het geldende toegangsbeleid.

De organisatie beschikt sinds 2018 over een beleid beveiligingsmaatregelen voor de inrichting en gebruik van laptops, tablets en andere mobiele communicatie apparaten. Met deze beveiligingsmaatregelen ontstaat bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

De organisatie heeft beleid voor het werken met informatiesystemen buiten de reguliere kantooromgeving. Wat ontbreekt is welke systemen wel en niet mogen worden geraadpleegd. Daarnaast zijn de telewerkvoorzieningen niet op basis van zero-footprint ingericht. De telewerkvoorziening kan echter wel op afstand gewist worden in het geval van diefstal of verlies.

Het is van belang dat wij als organisatie moeten werken naar een rol gebaseerd toegangsmodel. (Role Based Access Model). Dit houdt in dat rechten en bevoegdheden op basis van je rol binnen de organisatie worden toegekend. Hiermee wordt vervuiling van het netwerk en onbevoegde toegang bestreden en vermeden, en kan dit ingezet worden voor een beter gestroomlijnde in door en uitstroom procedure.

Ten opzichte van vorig jaar is dit onderdeel ongewijzigd. De begin stappen voor het inrichten van een role based access model is in 2019 uitgevoerd in de vorm van een inventarisatie en een advies rapport.
In 2020 wordt bepaald welke koers gevolgd gaat worden om hier verdere invulling aan te geven.

3.10 Verwerving, ontwikkeling en onderhoud van informatiesystemen (Hoofdstuk 12 van de BIG)

Bij het analyseren en specificeren van de eisen voor nieuwe systemen of systeemwijzingen werd in 2018 nog niet expliciet aandacht besteed aan de eisen voor informatiebeveiliging. Vanaf 2019 wordt er bij ieder nieuw systeem of systeemwijziging nagedacht over verschillende relevante technische en wettelijke eisen.
Op basis hiervan kan een risicoanalyse plaats vinden. Daarnaast kunnen de eventueel benodigde maatregelen proactief genomen worden om het veiligheid risico tot een minimum te beperken.

Bij invoer van gegevens in (web-)applicaties vindt validatie plaats op aspecten als juistheid en geschiktheid. Validatie is het controleren van een waarde of een methode aan de hand van normen. Het bij (web)applicaties uitvoeren van de juiste invoercontroles is noodzakelijk om te garanderen dat de integriteit van de ingevoerde gegevens juist is en de organisatie correcte beslissingen neemt. Dat betekent dat processen consequent intern worden gecontroleerd, aangevuld met de verbijzonderde interne controle.

De beheersing van de interne gegevensverwerking wordt versterkt door de aanwezigheid van beleid of richtlijnen voor verwerking-, en uitvoervalidaties bij de ontwikkeling van (web-) applicaties. Uitvoering van validatiecontroles in toepassingen voorkomt dat informatie corrupt raakt door verwerkingsfouten en ontdekt eventuele opzettelijke handelingen.

De organisatie beschikt over processen voor het toepassen en beheren van crypto grafische middelen en maatregelen specifiek voor het beheren van crypto grafische sleutels ter bescherming van informatie.

Voor de beveiliging van systemen en bestanden zijn voldoende beheersingsmaatregelen getroffen, zoals bij het wijzigen van (applicatie-) programmatuur en bescherming van testdata.

Voor de beveiliging bij ontwikkeling en ondersteuningsprocessen zijn voldoende beheersingsmaatregelen getroffen, zoals wijzigingsbeheer en technische controle en beoordeling van toepassingen na wijzigingen in het besturingssysteem. Aandachtspunten zijn bescherming tegen het uitlekken van informatie en controle door de organisatie bij uitbestede ontwikkeling van programmatuur.

De beheersingsmaatregelen van technische kwetsbaarheden zijn voldoende door controles op servers en IT-services, patchmanagement, actie ondernemen bij kwetsbaarheidswaarschuwingen van de Informatie Beveiligings Dienst. De maatregelen worden sterker als periodiek penetratietesten en vulnerability assessments (security scans) worden uitgevoerd.

Ten opzichte van vorig jaar is dit onderdeel licht verbeterd door het uitvoeren van risicoanalyses en het toepassen van maatregelen bij nieuwe systemen of systeemwijzigingen.

3.11 Beheer van informatiebeveiligingsincidenten (Hoofdstuk 13 van de BIG)

De organisatie beschikt over een incident management procedure. Een reactie- en escalatieprocedure en een registratiesysteem zijn onderdelen van de incident management procedure. In de procedure is aandacht voor de afhandeling/reactie van een incident. Als een veiligheidsincident is opgetreden wordt rekening gehouden met het zorgvuldig verzamelen van bewijsmateriaal.

Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten wordt geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren. Via trainingen en interne berichtgeving worden medewerkers hierover geïnformeerd.

Ten opzichte van vorig jaar is dit onderdeel licht verbeterd. Veiligheid incidenten worden meer herkend en dus frequenter gemeld en geregistreerd. Ook worden CISO en FG vaker benaderd voor advies.

3.12 Bedrijfscontinuïteitsbeheer (Hoofdstuk 14 van de BIG)

De gemeentelijke organisatie beschikt over een formeel bedrijfscontinuïteitsplan. Bij calamiteiten die de continuïteit van de processen in gevaar brengen of zorgen dat de werkprocessen stil komen te leggen wordt in de praktijk direct actie ondernomen door middel van een draaiboek. Dit bedrijfscontinuïteitsplan is al eens in de praktijk uitgevoerd. Er is echter nog onvoldoende aandacht besteed aan risico inschattingen waarmee

gebeurtenissen die tot onderbreking van processen kunnen leiden proactief worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging en de financiële gevolgen veroorzaakt door de uitval.

Ten opzichte van vorig jaar is dit onderdeel onveranderd gebleven.

3.13 Naleving (Hoofdstuk 15 van de BIG)

De gemeentelijke organisatie leeft wettelijke voorschriften na met betrekking tot de inrichting en uitvoering van processen/ informatiesystemen en voldoet aan alle voor IB relevante wet- en regelgeving en contractuele afspraken.

Opslag en archivering van registraties/ dossiers worden volgens vastgesteld beleid uitgevoerd.

De bescherming van gegevens en privacy worden bewerkstelligd in overeenstemming met de regels.

Uit de zelfevaluatie blijkt dat informatiesystemen niet of onvoldoende regelmatig worden gecontroleerd op naleving van implementatie van beveiligingsnormen. Penetratieproeven en kwetsbaarheidsbeoordelingen geven een momentopname van een systeem in een bepaalde toestand op een bepaald tijdstip en dekken niet alle delen van het systeem af. Penetratieproeven en kwetsbaarheidsbeoordelingen zijn geen vervanging van een risicobeoordeling.

Dit onderdeel is ten opzichte van vorig jaar onveranderd gebleven.

Bijlagen: (met uitzondering van de bedrijf kritische verantwoordingen Suwinet en DigiD)

- 1a. Uittreksel Reisdocumenten (PUN);
- 1b. Uittreksel BRP;
- 1c. Verantwoording BAG;
- 1d. Verantwoording BGT;
- 1e. Verantwoording BRO.