Rapportage informatieveiligheid horizontale verantwoording ENSIA 2020

Onderwerp: Horizontale verantwoording ENSIA over 2020 gemeente Albrandswaard

Domein/afdeling:
Coördinator ENSIA / CISO

Portefeuillehouder college van B&W:
M. Goedknegt

Naam opsteller:
R. Gillesen

1. Inleiding/aanleiding:

a) VNG resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente"

Met de VNG resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. De BIG is de kern van de verantwoording over informatieveiligheid aan de gemeenteraad. De horizontale verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het college van burgemeester en wethouders en een passage over informatieveiligheid in het jaarverslag.

Van BIG naar BIO

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek.

b) Verantwoordingsverplichting ENSIA

Om aan te tonen dat de gemeente Albrandswaard werkt in overeenstemming met de geldende wet- en regelgeving, interne regels en gedragscodes worden gemeenten sinds 2017 jaarlijks onderworpen aan de ENSIA (Eenduidige Normatiek Single Information) audit. Deze ENSIA audit bestaat uit een zelfevaluatie over de mate waarin de gemeente voldoet aan de afspraken uit de BIO, een horizontale verantwoording aan de gemeenteraad en een verticale verantwoording aan de landelijke toezichthouders zoals LOGIUS (DigiD) en het ministerie (inspectie) van Sociale Zaken en Werkgelegenheid (Suwinet).

2. IB-beleid, doelstellingen en afspraken

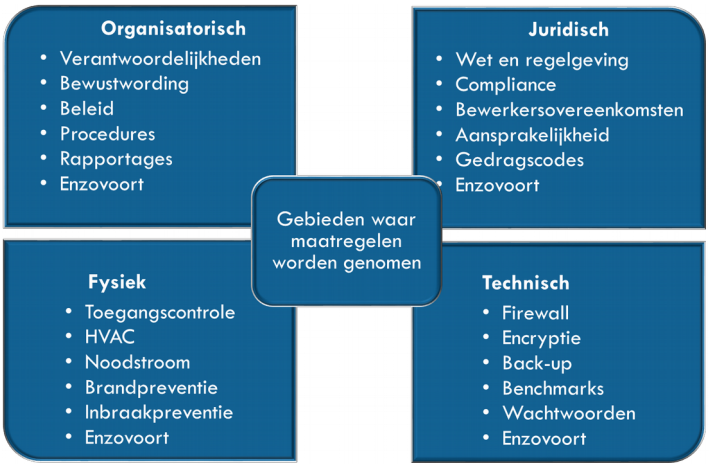
Gemeenten beschikken over uiterst gevoelige informatie van burgers en hebben zowel de wettelijke als morele plicht om daar zorgvuldig mee om te gaan. Het college van burgemeesters en wethouders van de gemeente Albrandswaard draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid en privacybescherming. 100%-veilig bestaat niet. Risico's worden doelbewust en proactief geaccepteerd en beheerst. Het college van burgemeester en wethouders van de gemeente Albrandswaard stelt, op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders zoals de BIO, de kaders ten aanzien van informatieveiligheid en privacybescherming voor de gemeente vast. De belangrijkste gemeentelijke informatiebeveiligingsdoelstellingen zijn:

- Het zorgvuldig omgaan met informatie en deze gegevens beschermen tegen onrechtmatige toegang en/of misbruik en/of manipulatie;
- Het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van deze (persoons)gegevens en de continuïteit van de dienstverlening van de gemeente Albrandswaard.
- Het voldoen aan wet- en regelgeving;
- Het beheersen van risico's.

Het informatiebeveiligingsbeleid van de gemeente Albrandswaard bevat de kaders voor het treffen en onderhouden van een samenhangend pakket van maatregelen teneinde de betrouwbaarheid (beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid) van de informatievoorziening te waarborgen. Het informatiebeveiligingsbeleid van de gemeente Albrandswaard is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).

3. Algemeen beeld en resultaten afgelopen periode

Informatieveiligheid reikt veel verder dan het implementeren van technische informatiebeveiligingsmaatregelen. Het is namelijk een groot misverstand om te denken dat informatieveiligheid iets technisch is. Hieronder wordt schematisch op hoofdlijnen weergegeven binnen welke domeinen door de gemeente Albrandswaard informatiebeveiligingsmaatregelen worden getroffen en onderhouden.



4. Beheersmaatregelen IB

Hieronder wordt een overzicht gegeven van de belangrijkste beheersmaatregelen die bijdragen aan het realiseren van de IB-doelstellingen van de gemeente Albrandswaard:

a) Het creëren van bewustzijn binnen de organisatie door regelmatig op intranet te communiceren over informatieveiligheid;
b) In 2020 werd op 9 risicovolle gegevensverwerkingen[1] een Data Protection Impact Analyse[2] (DPIA) inclusief een dataclassificatie[3] uitgevoerd;
c) In 2020 hebben de CISO en Privacy Officer 19 verwerkingsovereenkomsten beoordeeld/opgesteld, inclusief het voeren van de gesprekken met leveranciers en externe partijen hierover;
d) Het adviseren bij en het opstellen van het pakket van eisen rondom informatieveiligheid en privacybescherming bij inkoop trajecten.

5. Realisatie doelstellingen IB-beleid (effectiviteit beheersmaatregelen en risico's)

Hieronder wordt een overzicht gegeven van de belangrijkste IB-doelstellingen die zijn gerealiseerd:

a) De Baseline Informatiebeveiliging Overheid (BIO) is per 1 januari 2020 de opvolger Baseline Informatiebeveiliging Gemeenten (BIG). De BIO is vanaf dat moment van het verplichte normenkader voor de informatieveiligheid binnen gemeenten. In 2020 werd het op de BIG

1 Dit zijn gegevenswerkingen die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan beïnvloeden. Denk hierbij aan de verwerking van bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands gezondheid, ras, godsdienst, strafrechtelijk verleden of seksuele leven medische en/of strafrechtelijke gegevens.

2 Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna beveiligingsmaatregelen te kunnen nemen om de risico's te verkleinen.

3 Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan wordt mede bepaald welke beveiligingseisen gelden en welke beveiligingsmaatregelen moeten worden genomen.

gebaseerde informatiebeveiligingsbeleid van de gemeente Albrandswaard herzien en conform de BIO vernieuwd en vastgesteld door het college van burgemeesters en wethouders;

b) Het beoordelen en afhandelen van datalekmeldingen en informatiebeveiligingsincidenten (inclusief de vertrouwelijke cyberdreigingen overeenkomstig het Traffic Light Protocol (TLP[4]) afkomstig van de informatiebeveiligingsdienst voor gemeenten[5] (IBD));
c) Het adviseren van het (lijn)management/proceseigenaren over de implementatie van informatiebeveiligings- en privacybeschermende beheersmaatregelen voor hun verantwoordelijkheidsgebieden;
d) De CISO heeft samen met de domeindeskundige medewerkers van de verschillende afdelingen (ICT, HRM, Backoffice, Sociaal Domein, informatiemanagement) over het jaar 2020 de zelfevaluatie ENSIA uitgevoerd.

6. Incidenten(afhandeling)

Cybercriminaliteit heeft de laatste jaren een grote vlucht genomen en geen enkele overheidsorganisatie ontkomt aan pogingen van onbevoegden om informatie buit te maken of om de bedrijfsvoering te verstoren. Cybercriminaliteit is inmiddels “BIG business” en een serieus verdienmodel voor criminelen. Daarmee is een permanente wedloop ontstaan tussen het implementeren en in stand houden van informatiebeveiligingsmaatregelen en de innovatie in het hacken van organisaties. Op hoofdlijnen onderkennen we de volgende typen cyberdreigingen:

1: Extern en ongericht, bijvoorbeeld grootschalige phishing- en ransomwarecampagnes;
2: Intern en onbedoeld, bijvoorbeeld fouten van medewerkers met incidenten als gevolg;
3: Extern en gericht, bijvoorbeeld doelgerichte pogingen om geld of informatie buit te maken;
4: Intern en gericht, bijvoorbeeld fraude en ondermijnende activiteiten van eigen medewerkers.

Ook gemeenten worden hiervan het slachtoffer en staan bloot aan deze cyberdreigingen. Onlangs nog werd door een externe cyberaanval het computersysteem van de gemeente Hof van Twente[6] plat gelegd en als gevolg daarvan viel de complete dienstverlening van deze gemeente (langdurig) stil. Ook de gemeente Albrandswaard heeft het afgelopen jaar (2020) te maken gehad met diverse cyberdreigingen, waaronder phishingmails[7] en ransomware[8] dreigingen, enzovoorts. We ervaren binnen de gemeente Albrandswaard een toename van het aantal cybercrime dreigingen/aanvallen. Zie tevens bijlage 2 met het dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten 2021/2022. Helaas betreft het voorkomen van onrechtmatige toegang (door cyberaanvallen/hacking/fraude/ondermijnende activiteiten) tot onze gegevens en het treffen van passende beveiligingsmaatregelen een bewegend doel, waardoor we nooit “klaar” zijn. De dreigingen, kwetsbaarheden en technische mogelijkheden veranderen namelijk constant. Om dergelijke incidenten gecoördineerd af te handelen hebben we intern een Computer Emergency Response Team[9] (CERT) samengesteld onder aansturing van de CISO.

---

4 Het Traffic Light Protocol (TLP) is ontworpen om het uitwisselen van informatie op een veilige manier te laten verlopen. TLP zorgt voor een simpel en intuïtief schema om aan te duiden hoe gevoelig bepaalde informatie is en hoe deze gedeeld kan worden binnen de gemeenschap.

- WHITE / Wit – Informatie die vrij verspreid mag worden, voor zover de verspreiding niet strijdig is met de wet zoals bijvoorbeeld de wet op het auteursrecht;
- GREEN / Groen – Informatie voor een gemeenschap, maar niet te verspreiden op het internet;
- AMBER / Oranje – Informatie voor een organisatie, eventueel beperkt tot bepaalde personen van de organisatie. De informatie mag binnen de organisatie worden verspreid op een ‘need-to-know’ basis.
- RED / Rood – Informatie uitsluitend bestemd voor de rechtstreeks geadresseerden.

5 De Informatiebeveiligingsdienst voor gemeenten is een initiatief van alle Nederlandse gemeenten en actief sinds 1 januari 2013. De IBD is de sectorale CERT / CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team) voor alle Nederlandse gemeenten en ondersteunt bij incidenten op het gebied van informatiebeveiliging.

6 Nieuwsbericht | Gemeente Hof van Twente

7 Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze bijvoorbeeld te lokken naar een valse website om ze daar, nietsvermoedend, te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien.

8 Bij ransomware (gijzelsoftware) worden je bestanden versleuteld, en de manier om ze weer te ontsleutelen is meestal om het gevraagde losgeld (in bitcoins) te betalen;

9 Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt een CERT zich ook op preventie en preparatie.

7. Doorkijk prioriteiten voor 2021 informatieveiligheid

Hieronder wordt een overzicht gegeven van de belangrijkste IB-doelstelling voor 2021. Voor informatieveiligheid zijn deze prioriteiten:

- De verdere implementatie van de BIO en de bijbehorende verplichte overheidsmaatregelen;
- De uitvoering van de ENSIA cyclus voor de verantwoording over het jaar 2021;
- Het op- en laten vaststellen van het volgende onderliggend beleid:
    1: Cryptografiebeleid;
    2: Logging beleid;
    3: Wachtwoordbeleid;
    4: Clear screen clean desk Beleid.
    5:

Naast deze prioritering zal een groot deel van de beschikbare capaciteit worden besteed aan “reguliere” werkzaamheden zoals:

- Het afhandelen van cybercrime dreigingen (IBD tlp meldingen, phishingmails en ransomware) en datalekken (zoals vermiste telefoons enzovoorts);
- Het treffen en onderhouden van preventieve en correctieve beveiligingsmaatregelen, waaronder het installeren van beveiligingspatches op het moment dat deze naar aanleiding van een kwetsbaarheid door de leverancier beschikbaar worden gesteld;
- Het adviseren van het college van burgemeester en wethouders van de gemeente Albrandswaard, de BAR-directie, de managers en medewerkers binnen de afdelingen;
- Het opstellen, evalueren en/of onderhouden van verwerkersovereenkomsten, beleid, procedures en beveiligingsmaatregelen;
- Bewustzijn creëren, oftewel het “scherp” houden van medewerkers op het gebied van informatieveiligheid en privacybescherming.
- Enzovoort.

8. Bijlage(n)

1. De collegeverklaring ENSIA.
2. Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022.