Bijlage 7 ENSIA - Rapportage over informatieveiligheid

Informatieveiligheid

1. Inleiding/aanleiding:

a) VNG resolute "Informatieveiligheid, randvoorwaarde voor de professionele gemeente"
Met de VNG resolute "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, IT-audit, 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 Ridderkerk 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 in de BIO, 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 burgemeester en wethouders van de gemeente Ridderkerk draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor en 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 Ridderkerk 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 Ridderkerk.
- Het voldoen aan wet- en regelgeving.
- Het beheersen van risico's.

Het informatiebeveiligingsbeleid van de gemeente Ridderkerk 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 Ridderkerk 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.

4. Beheersmaatregelen IB
Hieronder wordt een overzicht gegeven van de belangrijkste beheersmaatregelen die bijdragen aan het realiseren van de IB-doelstellingen van de gemeente Ridderkerk:
a) Het creëren van bewustzijn binnen de organisatie door regelmatig op intranet te communiceren over informatieveiligheid;
b) In 2021 hebben de CISO en Privacy Officer meerdere verwerkingsovereenkomsten beoordeeld/opgesteld, inclusief het voeren van de gesprekken met leveranciers en externe partijen hierover;
c) 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 in 2021 verder geïmplementeerd binnen de gemeente Ridderkerk;
b) Het beoordelen en afhandelen van datalekmeldingen en informatiebeveiligingsincidenten (inclusief de vertrouwelijke cyberdreigingen overeenkomstig het Traffic Light Protocol (TLP4) afkomstig van de informatiebeveiligingsdienst voor gemeenten" (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, Social Domein, informatiemanagement) over het jaar 2021 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.
We ervaren binnen de gemeente Ridderkerk een toename van het aantal cybercrime dreigingen/aanvallen. 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.

7. Doorkijk prioriteiten voor 2021 informatieveiligheid

Hieronder wordt een overzicht gegeven van de belangrijkste IB-doelstelling voor 2022. Voor informatieveiligheid zijn deze prioriteiten:

- Maken van een Informatiebeveiligingsplan 2022 met een jaarplanning 2022;
- Maken van een Bewustwordingsprogramma 2022-2023 met jaarplanning 2022;
- P&C-cyclus voor informatieveiligheid is ingericht voor alle afdelingen;
- Technische maatregelen groeien mee met het cyberdreigingsbeeld;
- De verdere implementatie van de BIO en de bijbehorende verplichte overheidsmaatregelen;
- De uitvoering van de ENSIA-cyclus voor de verantwoording over het jaar 2022;
- Enz.