Bijlage 3 Beveiliging en privacy

Met de recente incidenten bij verschillende (overheids)organisaties in het achterhoofd staat het thema informatiebeveiliging en privacy hoog op de (bestuurlijke) agenda, zowel landelijk als in Staphorst.

Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) trad in 2020 in werking en dwingt gemeenten te voldoen aan normen met betrekking tot informatiebeveiliging met als doel de digitale weerbaarheid te vergroten.
Hoewel de Rekenkamer in haar onderzoek naar informatiebeveiliging in 2018 nog heeft geconcludeerd dat de basis in Staphorst vrijwel op orde was, gaan de eisen van de BIO verder dan de eisen die in 2018 werden gesteld. Om te voldoen aan de nieuwe eisen is binnen Staphorst een actieprogramma opgestart.

In het verlengde hiervan is eind 2020 het strategisch informatiebeveiligingsbeleid gemeente Staphorst 2020-2023 door het college vastgesteld. Dit beleid is conform de BIO opgesteld.

Eén van de onderdelen van het strategisch informatiebeveiligingsbeleid was de bespreking en vaststelling van de 10 voor Staphorst leidende bestuurlijke principes voor informatiebeveiliging:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

In aansluiting op het strategische informatiebeveiligingsbeleid is, op basis van een risicoafweging, onder regie van de CISO een Informatiebeveiligingsplan opgesteld. In zowel het informatiebeveiligingsplan als in het voorliggende document zijn acties opgenomen die de bovenstaande 10 bestuurlijke principes onderschrijven dan wel daar invulling/uitvoering aan geven.

Daarnaast is bij de GAP-analyse op het informatiebeveiligingsbeleid gebleken dat een aantal ICT-voorzieningen en -processen nog ingericht en/of aangescherpt moeten worden. Ook deze zijn In het beveiligingsplan opgenomen. In dit plan staan de activiteiten die uitgevoerd moeten worden, inclusief doorlooptijd en benodigde capaciteit en middelen.

VNG-agenda Digitale Veiligheid 2020-2024

In aanvulling op de BIO, welke met name in gaat op het thema digitale weerbaarheid, en aansluitend bij de 10 vastgestelde bestuurlijke principes volgt Staphorst ook de VNG-agenda Digitale Veiligheid 2020-2024. Hierin staan de volgende actielijnen:

- Bewustzijn (van risico's en spelregels omtrent gebruik van informatie(systemen).
- Weerbaarheid van de gemeentelijke organisatie en haar informatiesystemen.
- Digitale brandoefening.

Ook deze agenda leidt tot acties, te vertalen in projecten, zie ook de paragraaf over het informatiebeveiligingsplan en projecten.

IBD- en VNG-berichten en richtlijnen

Naast de BIO en de agenda Digitale Veiligheid 2020-2024 is er een voortdurende stroom van actuele informatie van de VNG en met name de IBD (Informatiebeveiligingsdienst), mede op basis van aanwijzingen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), onderdeel cybersecurity. Deze berichtgeving bevat informatie over dreigingen en incidenten alsmede informatie op basis waarvan acties om incidenten te voorkomen dienen te worden uitgevoerd.

Deze informatiestroom die met name de laatste twee jaar sterk is toegenomen eist de nodige aandacht en vooral ook personele inzet en budget om de benodigde acties uit te voeren. De belangrijkste (dwingende) richtlijnen op het gebied van beveiligingsmaatregelen, de speerpunten, zijn:

- 2-Factor authenticatie: Veel beveiligingsincidenten ontstaan doordat inloggegevens gelekt worden. Een effectief middel om schade te voorkomen en te beperken is het toepassen van 2-factor authenticatie. Deze wordt al gebruikt in Staphorst (bv werkplek.staphorst.nl) maar kan en moet nog breder ingezet worden. Zeer recent heeft ook de IBD aangedrongen om dit op korte termijn toe te passen op minimaal de ontsluiting van Webmail, alle beheerdersaccounts en bedrijfskritische en privacygevoelige cloud-toepassingen. Dit onderdeel is met prioriteit in 2021 opgepakt en in uitvoering, zal voor enkele applicaties doorlopen in 2022.

- Om geavanceerde dreigingen, zowel vanuit binnen als buiten de organisatie, te kunnen adresseren is het essentieel om over de juiste hulpmiddelen en processen te beschikken, waarmee dreigingen en aanvallen in een zeer vroeg stadium gedetecteerd kunnen worden. Op basis van deze vroegtijdige detectie kan er actie ondernomen worden om de aanval zo snel mogelijk te stoppen of in een aantal gevallen zelfs te voorkomen. Het inrichten van een Security Information & Event Management (SIEM) proces met de bijbehorende tooling en organisatie kan ervoor zorgen dat de gevolgen van aanvallen worden verminderd of in sommige gevallen worden voorkomen. De daarbij behorende uitvoerende processen van SIEM (o.a. 24/7 bewaking en signalering) worden in een Security Operations Center (SOC) belegd.

  Omdat dit complexe en specifieke materie is, heeft de VNG zowel de SIEM als SOC-dienstverlening voor alle Nederlandse gemeenten aanbesteed en gegund aan één partij. Gemeenten kunnen instappen op het moment dat zij dat zelf willen. De implementatie van SIEM/SOC Staphorst eerste fase staat gepland voor 2023-2024. De overige fasen in de jaren daarna.

De IBD- en VNG-richtlijnen leiden tot meer acties dan deze twee. Gedurende het jaar zullen wij de richtlijnen vertalen in projecten en zo mogelijk opnemen in het jaarlijks projectenoverzicht van het informatiebeveiligingsplan, zie ook onderstaande paragraaf informatiebeveiligingsplan en projecten.

Omdat een aantal van de richtlijnen een ad-hoc karakter heeft en soms op korte termijn uitgevoerd dienen te worden is het noodzakelijk structureel budget te reserveren om snel te kunnen reageren.

Het informatiebeveiligingsplan en projecten

Het huidige informatiebeveiligingsplan bevat alle BIO gerelateerde acties uit de GAP-analyse. In een update zal dit zijn uitgebreid met de acties die voortvloeien uit de VNG-agenda Digitale Veiligheid 2020-2024. Tevens wordt een jaarkalender opgesteld waarin ook de jaarlijkse acties voor het privacy domein zijn opgenomen. Daarmee wordt invulling gegeven aan de plan-do-check-act (PDCA) cyclus zoals vastgesteld in het strategisch beveiligingsbeleid en zo efficiënt mogelijk ingezet op informatiebeveiliging en privacy.

Privacywetgeving

Waar informatiebeveiliging zich richt op alle informatie, processen en handelingen van de gemeente, richt de zorg voor privacy zich specifiek richt op de omgang met (bijzondere) persoonsgegevens van burgers en medewerkers.

De privacywetgeving, (uitvoeringswet) Algemene verordening gegevensbescherming (AVG) schrijft voor hoe de gemeente Staphorst rechtmatig dient om te gaan met persoonsgegevens. Hoewel informatiebeveiliging niet expliciet in deze wet is beschreven leidt de wet tot de nodige informatiebeveiligingsmaatregelen: zonder informatiebeveiliging kan op geen enkele wijze privacy worden gegarandeerd.

Naast eisen aan bescherming kent de wet ook rechten toe aan burgers om bijvoorbeeld een overzicht van de bij de gemeente in beheer zijnde persoonsgegevens op te vragen. Ook worden vanuit privacywetgeving eisen gesteld aan verplichte meldingen bij datalekken, jaarlijkse rapportages en de verplichting een onafhankelijke toezichthoudende functionaris gegevensbescherming (FG) aan te stellen of in te huren.

Sinds de komst van de AVG in 2018 is de jurisprudentie op gang gekomen en komt de Autoriteit Persoonsgegevens (AP), de landelijke toezichthouder, regelmatig met aanbevelingen en richtlijnen. Recent bijvoorbeeld inzake het gebruik van pasjes bij afvalcontainers en aanbevelingen voor gemeenten die met slimme sensoren en meetapparatuur data in de openbare ruimte verzamelen ten behoeve van smartcity-toepassingen waarbij persoonsgegevens van de burgers verwerkt worden

Daar waar de AVG extra eisen stelt aan de informatiebeveiliging, staat deze wetgeving (afscherming van persoonsgegevens en zeer korte bewaartermijnen) juist weer op gespannen voet met de Archiefwet en Wob/Woo (langdurig bewaren en openbaar, tenzij). Deze tegenstrijdigheden creëren dilemma's als het gaat om rechtmatig handelen op het vlak van informatievoorziening, welke door de gemeente met behulp van de VNG-richtlijnen worden genavigeerd.

Privacy uitvoeringsprogramma

Afgelopen jaar wisten steeds meer medewerkers de privacy- en beveiligingsfunctionarissen te vinden. Vooral het thuiswerken leidde tot meer vragen. Het is goed te constateren dat het informatieveiligheid en privacy bewustzijn van de medewerkers toeneemt. In de komende periode worden meer verschillende campagnes en acties binnen de gemeente Staphorst gestart om medewerkers regelmatig aan het belang en de spelregels te herinneren.

De invoering van nieuwe wetgeving zoals de Wet hergebruik van overheidsinformatie (Who), de modernisering van de Archiefwet, de Wet digitale overheid (inclusief Generieke Digitale Infrastructuur, GDI) en de Wet Open Overheid (Woo) zal leiden tot beveiligings- en privacyvraag-stukken en maatregelen.

Op kortere termijn wordt de in Staphorst in het kader van informatiebeveiliging en privacy gestarte dataclassificatie nader uitgewerkt. Dit is noodzakelijk om risico's beter te kunnen inschatten en waar nodig specifieke aanvullende maatregelen op het vlak van informatie-beveiliging en privacy te treffen. Voorts zal er in het verlengde van de Regeling periodieke audit politiegegevens (waar de Staphorster BOA mee te maken heeft) een auditcyclus ingericht worden.

De terugkerende awareness campagnes, acties en audits ten behoeve van het privacy domein worden meegenomen in de jaarkalender zoals in de paragraaf over beveiliging wordt aangeduid om met het beperkte aantal beschikbare medewerkers acties en verplichtingen zo goed mogelijk te monitoren en na te leven.