INFORMATIE
BEVEILIGINGS
DIENST

DE TAKEN EN VERANTWOORDELIJKHEDEN VAN EEN CISO

Informatiebeveiliging binnen de overheid wordt steeds belangrijker, omdat we steeds afhankelijker worden van digitale informatievoorziening die veelal tijd en plaatsonafhankelijk toegankelijk moet zijn. Ook allerlei (nieuwe) wetgeving legt eisen op aan de informatiebeveiliging van gemeenten. Een eerste begin om informatiebeveiliging binnen een gemeente 'te organiseren', is het aanstellen van een Chief Information Security Officer (CISO). Wie kan het complete spectrum aan informatiebeveiliging immers beter overzien en coördineren dan een daarvoor speciaal aangestelde functionaris? Deze factsheet biedt u als (beginnend) CISO handvatten om informatiebeveiliging in de gemeentelijke organisatie (verder) vorm te geven. Welke verantwoordelijkheden heeft u als CISO? Wie zijn uw belangrijkste overlegpartners? Wat zijn de belangrijkste aandachtspunten? Wij hebben de antwoorden op deze vragen overzichtelijk op een rij gezet.

DE CISO EN DE BIG

Doel van uw functie als CISO is om op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) zorg te dragen voor een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente te waarborgen. De CISO is geen onderdeel van ICT en dient vanuit een onafhankelijke positie te kunnen adviseren over informatieveiligheid.

AANDACHTSPUNTEN IN RELATIE TOT VERANTWOORDELIJKHEDEN

Het takenpakket van een CISO is veelomvattend. In het BIG OP-product 'Handreiking IB-functieprofiel Chief Information Security Officer (CISO)' leest u hierover meer informatie.

"EEN CISO ZORGT VOOR VOLDOENDE STEUN EN VERANTWOORDELIJKHEID VANUIT HET MANAGEMENT"

Hieronder een overzicht van een aantal belangrijke aandachtspunten in relatie tot verantwoordelijkheden:

- Wat is het mandaat dat u binnen de gemeente heeft? Als CISO dient u vrij en onafhankelijk te kunnen bewegen, waarbij de belangen van een afdelingshoofd niet mee zouden moeten wegen als het gaat om onafhankelijk advies.
- De CISO heeft een controlerende en adviserende rol voor informatiebeveiligingsmaatregelen. Een lijnmanager is verantwoordelijk voor het proces en voor onderliggende informatiesystemen. Tevens is de lijnmanager verantwoordelijk voor de afweging om iets wel of niet te doen en de consequenties hiervan.
- Zorg als CISO voor voldoende steun en verantwoordelijkheid vanuit het management. U moet immers adequaat kunnen optreden in onveilige situaties.
- Zorg ervoor dat verantwoordelijkheden goed verankerd worden in het gemeentelijk informatiebeveiligingsbeleid.

ANALYSE ORGANISATIE EN INFORMATIEVEILIGHEID

Een eerste stap die u als CISO neemt, is onderzoek doen naar hoe het met de informatieveiligheid binnen de gemeente gesteld is. Het stappenplan voor de invoering van de BIG voor kleine gemeenten kunt u hiervoor als leidraad gebruiken. Ook de GAP-analyse die de IBD voor de BIG heeft opgesteld, is hiervoor een prima hulpmiddel. De GAP-analyse is een methode om een vergelijking te maken tussen de huidige en de gewenste situatie en de maatregelen uit de baseline. Het is mogelijk om met het hoog over doorlopen van de GAP-analyse een goed inzicht te krijgen. Zoek niet te lang het gaat om een algehele indruk.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIEBEVEILIGINGSPLAN

De resultaten uit het onderzoek en de GAP-analyse gebruikt u vervolgens om een actieplan op te stellen en van start te gaan. Enkele voorbeelden van actiepunten die u in het actieplan kunt opnemen:

- Opstellen of aanpassen van het gemeentelijk informatiebeveiligingsbeleid.
- Vastleggen verantwoordelijkheden met betrekking tot informatiebeveiliging.
- Vaststellen welk aanvullend informatiebeveiligingsbeleid noodzakelijk is.
- Starten met bewustwording, bijvoorbeeld ondersteund door resultaten van een mystery guest.
- Definiëren welke beveiligingsprocessen op korte termijn nodig zijn, bijvoorbeeld incidentmanagement of patchmanagement.

BEWUSTWORDING

Naast de technische maatregelen voor het informatiebeveiligingsbeleid is het ook belangrijk aandacht te besteden aan de bewustwording van risico's op informatiebeveiligingsvlak bij de medewerkers in de organisatie. Een goed begin zou kunnen zijn om medewerkers bij de VNG Academie de e-learning modules iBewustzijn Overheid te laten volgen.

BORGING DOOR ISMS

Het is aan te bevelen de borging van informatiebeveiliging vorm te geven door de invoering van een Information Security Management System (ISMS). Het doel van het ISMS is onder andere het continue beoordelen van welke beveiligingsmaatregelen passend zijn en deze indien nodig bij te stellen. Het is een voortdurend proces dat binnen de gemeente uitgevoerd wordt. Meer informatie over ISMS is ook terug te lezen in het BIG OP-product 'Information Security Management System (ISMS)'.

OVERLEG

Op verschillende niveaus vraagt u als CISO aandacht voor informatiebeveiliging en informatieveiligheid in brede zin. Daarom neemt u ook deel aan verschillende overleggen. Dit is mede belangrijk, omdat uw bijdrage hieraan ook een bewustwordingseffect heeft. Afhankelijk van de grootte van uw gemeente bestaan er verschillende overlegvormen. In ieder geval is het aan te bevelen om regulier overleg met uw bestuurder of de verantwoordelijk wethouder te voeren en de lijnmanagers. Tijdens dit overleg bespreekt u onder andere de voortgang van de invoering van de BIG. Daarnaast voert u maandelijks overleg met de afdeling ICT over de technische aspecten rondom de BIG. In elke regio vindt ook regionaal overleg plaats met CISO's van andere gemeenten. Doel van dit overleg is onder andere het delen van kennis en ervaring, bekijken van mogelijkheden voor gezamenlijke inkoop en gebruik van tooling.

RAPPORTEREN

Als CISO rapporteert u minimaal jaarlijks aan het bestuur en management de stand van zaken van de informatiebeveiliging van uw gemeente. In een startfase is het verstandig om vaker te rapporteren om beter inzicht in de voortgang te hebben.

KENNIS

Om uw functie als CISO goed uit te kunnen voeren, is het belangrijk om altijd over de juiste en actuele kennis van nieuwe technologische ontwikkelingen te beschikken. Dit kan op verschillende manieren. We geven u hieronder een aantal tips:

- Onderhoud contact met de leveranciers van uw gemeentelijke software via bijvoorbeeld beurzen of sluit aan bij gebruikersgroepen van bepaalde producten.
- Volg aanvullende opleidingen. Om een goede keuze te maken uit het grote aanbod raden wij u aan om te kijken naar een opleiding die in het verlengde ligt van de ISO 27001 en 27002, omdat dit aansluit bij de BIG. Heeft u interesse in het halen van een certificering? Dan is de opleiding ISFS een interessante optie of een van de vervolgopleidingen ISMAS, CISSP, ISSMP.
- Word lid van een vakvereniging. Soms is een vakvereniging verbonden aan een van de eerder genoemde certificeringen, bijvoorbeeld (ISC)2. Er is ook een Nederlandse vakvereniging, het Platform voor Informatiebeveiliging (PvIB).
- Meld u aan voor de community Informatiebeveiliging van de IBD. Een digitaal platform waarop u als gemeente samen met collega-gemeenten informatie met elkaar kunt delen, vragen kunt stellen en documenten uit kan wisselen.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.