BMC
YACHT GROUP

Is uw gemeente eind 2019 klaar voor de BIO?

Weerbaar met de Baseline Informatiebeveiliging Overheid

Partners in verbetering

Waar staan we?

De Nederlandse gemeenten hebben sinds 2013 gewerkt aan informatiebeveiliging op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). In eerste instantie op basis van een VNG-resolutie, sinds 2015 op basis van een convenant. Vanaf 2017 leggen gemeenten hierover verantwoording af via de systematiek van ENSIA (Eenduidige Normatiek Single Information Audit). BMC heeft gemeenten de afgelopen jaren ondersteund bij de implementatie van de BIG, onder andere met het opstellen van beleid, de invoering van maatregelen uit de BIG, ondersteuning van CISO's en de inrichting van ondersteunende tooling, zoals Scienta, ter voorbereiding van ENSIA en verwante audits.

In 2016 is een initiatief gestart om een overheids-brede baseline voor informatiebeveiliging op te zetten, onder andere na vragen uit de Tweede Kamer. Dit is uitgemond in de Baseline Informatiebeveiliging Overheid (BIO), die is gebaseerd op de internationale normenreeks ISO 27001:2013 en ISO 27002:2013. De BIO is door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) van een positief advies voorzien en ter besluitvorming voorgelegd aan de Ministerraad. Tevens is de BIO tot standaard verklaard door de VNG. Daarmee is de BIO verplicht voor gemeenten en niet - zoals de BIG - slechts een onderling commitment. De BIO geldt voor gemeenten vanaf 1 januari 2020; dit betekent in 2019 veel werk om tijdig aan de BIO te voldoen.

De wereld verandert

Sinds de ontwikkeling van de BIG is er veel veranderd. Intussen is de nieuwe Europese Privacywet, de Algemene Verordening Gegevens-bescherming (AVG), ingevoerd, die extra eisen stelt aan de beveiliging van persoonsgegevens. Buitenlandse inmenging in verkiezingen en hacking van overheidssystemen zijn geen hypothetische scenario's meer. Soms gebruiken hackers geavanceerde methoden, soms wordt er gewerkt met phishing-e-mails en andere methoden die door hobbyisten op dit gebied kunnen worden gehanteerd. De recente aanval op het Duitse parlement is daarvan een voorbeeld. Zulke inbreuken schaden mogelijk niet alleen de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens van burgers, maar ook het vertrouwen van burgers in de overheid. Dit maakt informatiebeveiliging nog noodzakelijker voor het goed functioneren van het openbaar bestuur. Daarbij past ook dat de BIO een meer verbintelijk karakter zal hebben dan de BIG tot nu toe. In de BIG stond een risicogebaseerde aanpak centraal. Deze aanpak wordt in de BIO aangevuld met basisniveaus met verplichte maatregelen. Deze worden aangevuld met maatregelen op basis van een risicoafweging. De BIO wordt vanaf 2020 ook in de ENSIA-audits opgenomen. Verder zullen toezichthouders, zoals de Autoriteit Persoonsgegevens, de BIO gaan gebruiken als maatstaf voor adequate informatiebeveiliging.

Hoofdlijnen blijven, maar er zijn ook belangrijke verschillen

De aanpak van informatiebeveiliging in de BIO verschilt niet fundamenteel van die in de BIG. Het werk dat de afgelopen jaren in de implementatie van de BIG is gestoken vormt de basis om de BIO te implementeren. Er zijn echter wel enkele belangrijke verschillen, zowel in de opzet als in de inhoud van de maatregelen.

In de opzet zien we het volgende:

- De onderdelen beleid en organisatie sluiten beter aan bij de internationale norm en zijn generieker, waar de BIG meer gemeente-specifiek is.
- Er zijn verplichte maatregelen ingevoerd als basisbeveiligingsniveau.
- Er zijn basisbeveiligingsniveaus (BBN) uitgewerkt, waarbij we ervan uitgaan dat gemeenten in principe aan het hogere BBN2 moeten voldoen, gezien de gevoeligheid van gegevens, o.a. in het sociaal domein en veiligheid en handhaving.
- Verantwoordelijkheden van de gemeente-secretaris, proceseigenaren en diensten-leveranciers zijn in de norm belegd, niet alleen

in het beleid van de eigen organisatie.
- Er ligt meer nadruk op risicomanagement voor risico's die het basisbeveiligingsniveau overstijgen.
- De BIO sluit nauw aan bij de internationale norm met iets meer dan 100 maatregelen, en werkt deze uit, zodat het totale aantal items op meer dan 200 komt. Dat is beduidend minder dan de 300 maatregelen van de BIG.

Inhoudelijk zien we de volgende verschillen:

- Een aantal maatregelen is algemener geformuleerd, waardoor sommige details uit de BIG vervallen.
- Een aantal maatregelen is juist concreter uitgewerkt, bijvoorbeeld:
  - het afronden van een i-bewustzijnstraining binnen 3 maanden na indiensttreding;
  - het formaliseren van bevoegdheden voor het beslissen over autorisaties in een mandaatregister;
- het bewaken van systemen met SIEM en/of SOC.
- Er zijn een aantal aanvullingen gedaan op de internationale norm, zoals het aansluiten op een klokkenluidersregeling.

Al met al ligt de lat bij de BIO net wat hoger dan bij de BIG en doordat de insteek van de BIO minder vrij-blijvend is, wordt 2019 voor veel organisaties een uitdagend jaar.

Hoe pakt u dit aan?

Allereerst is het belangrijk om te kijken waar de organisatie staat door middel van een zelfevaluatie of een assessment. Bij een zelfevaluatie oordelen medewerkers uit uw organisatie zelf in een workshop of een interview over het voldoen aan maatregelen.
Bij een assessment wordt er een oordeel gevormd door een externe adviseur op basis van gesprekken, workshops en documentatie.
In beide gevallen gaat het zowel om de implementatie van maatregelen als om de positionering in de organisatie. Zijn zaken alleen 'op papier' goed geregeld of ook in de praktijk? En is dit aantoonbaar?

Er wordt een overzicht gemaakt van gegevensverzamelingen om zicht te krijgen op de risicogevoeligheid en wie daarvoor verantwoordelijk is. Vervolgens worden deze gewaardeerd op basis van vertrouwelijkheid, integriteit en noodzakelijke beschikbaarheid. We noemen dit ook wel 'dataclassificatie'.

Een volgende stap is het uitvoeren van een brede risicoanalyse aan de hand van bedreigingen.

Wanneer er nog veel te doen is om op het vereiste basisbeveiligingsniveau te komen, kan de risicoanalyse helpen om prioriteiten te stellen. Wanneer het vereiste basisbeveiligings-niveau is bereikt, helpt een risicoanalyse om aanvullende maatregelen op te stellen. In dat geval is een processpecifieke risicoanalyse zinvol.

Op basis van de zelfevaluatie of het assessment, de dataclassificatie en de risicoanalyse wordt een plan van aanpak opgesteld om beleid op te stellen of aan te passen, maatregelen in te voeren en informatieveiligheid verder in de organisatie in te bedden vanuit de gedachte van de PDCA-Cyclus. Waar mogelijk wordt dit geïntegreerd met uit te voeren acties rond privacy. Waar nodig worden er keuzes gemaakt tussen zelfdoen en uitbesteden, bijvoorbeeld naar gemeenschappelijke infrastructuren.

Op die manier voldoet de organisatie tijdig aan de BIO en worden de gegevens van burgers en medewerkers adequaat beschermd in een tijd waarin wekelijks meldingen van inbreuken op de informatiebeveiliging bekend worden.

Voor meer informatie en voor het maken van een (vrijblijvende) afspraak kunt u contact opnemen met:

ir. Julius Duijts
Senior adviseur CISSP CIPP/E
julius.duijts@bmc.nl
06 29 52 55 31

Martijn van Engelen MSc
Adviseur Informatieveiligheid
martijn.van.engelen@bmc.nl
06 10 58 00 34

Lisanne van Boekel
Account manager
lisanne.van.boekel@bmc.nl
06 12 97 26 14

BMC helpt

Bij de gehele implementatie van de BIO helpt BMC u verder.

- BMC helpt u met het uitvoeren van zelf-evaluaties, assessments, dataclassificatie en het opstellen van beleid en de implementatie daarvan. BMC heeft daartoe
  - instrumenten ontwikkeld voor zelfevaluaties en assessments en kan deze begeleiden en samen met uw medewerkers uitvoeren;
  - een set beleidsdocumenten ontwikkeld waarin de eisen van de BIO worden vertaald in concreet toepasbare beleids- en gedragsregels en concrete eisen aan processen, ICT-infrastructuur en -applicaties. De beleidsdocumenten zijn verdeeld in disciplines, zoals HR, Facilitair, Inkoop en ICT, zodat afdelingen niet door de hele BIO heen hoeven, maar zich kunnen richten op de maatregelen die voor hen relevant zijn.
- BMC-adviseurs snijden de sjablonen voor beleid en procedures samen met uw organisatie toe op uw situatie en ondersteunen daarmee het draagvlak voor maatregelen.
- BMC beschikt voor het gehele traject over ervaren begeleiders met projectmanagementervaring en inhoudelijke deskundigheid.
- BMC vult de rol van CISO a.i. in.
- BMC levert operationele ondersteuners voor de CISO.

BMC kent de gemeentelijke organisatie, weet de mensen mee te krijgen en maakt de verbinding tussen de dagelijkse praktijk en de eisen van de BIO.

Door de BMC-aanpak en -sjablonen kan uw organisatie snel aan de slag om voor 2020 de nodige stappen te kunnen zetten.

Kijk voor meer informatie ook eens op onze website **www.bmc.nl**