Auteurs: Dit artikel is geschreven door het team Informatieveiligheid, onderdeel van de directie Digitale Samenleving bij het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK). We werken met alle bestuurslagen (Rijk/ZBO's, provincies, gemeenten en waterschappen), private partners en wetenschap aan de maatschappelijke taak dat overheden adequaat omgaan met informatiebeveiliging. Voor informatie kijk op: www.digitaleoverheid.nl/contact.

Over risico's en kansen: BIO2 & NIS2

Als we willen dat digitale technologie voor onze samenleving toegevoegde waarde heeft, moet digitalisering waardengedreven en mensgericht zijn. *De Werkagenda Waardengedreven Digitaliseren (1) (zie het kader op pagina 19)* van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (geactualiseerd in 2023) gaat uit van vijf principes. Als we deze principes willen realiseren moeten we als maatschappij met elkaar flinke stappen zetten. In de fysieke wereld hebben we wetten en regels die onze veiligheid waarborgen. Het principe van regels vooraf en toezicht hierop is ook wenselijk in de digitale wereld.

In dit artikel gaan we in op de positie van de Baseline Informatiebeveiliging Overheid (BIO) als belangrijk basis-normenkader voor informatiebeveiliging bij de overheid. Ook geven we een kijkje in de keuken ten aanzien van de recente ontwikkelingen rondom de Europese richtlijn Network and Information Security 2 (NIS2).

Aanloop naar een nieuwe BIO

De Rijksoverheid, Provincies, Waterschappen en Gemeenten werkten allemaal met verschillende baselines (BIG, BIR, BIWA en IBI) (2). Dit was geen ideale situatie. De behoefte groeide om tot één uniforme baseline te komen: de BIO, met een verplichtend karakter op basis van zelfregulering (besluit Ministerraad 2018). Belangrijk is te weten dat de BIO is gebaseerd op de internationale normen: NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017. Ze zijn als verplicht te gebruiken normen opgenomen in de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie.

Doel van de BIO

De BIO is een kader en geeft handvatten om de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen. Invulling daarvan is daar waar mogelijk risicogestuurd. De gedachte is dat ketenpartners in de overheidssector op deze manier elkaar kunnen vertrouwen bij eventuele gegevensuitwisseling. Doel van de BIO is om de informatieveiligheid overheidsbreed op een acceptabel basisniveau te brengen. Daarnaast hebben overheidsorganisaties met de BIO een instrument in handen om extern en intern transparant te zijn over het beveiligingsniveau. Met de invoering van de BIO hanteert de overheid één gezamenlijke taal en doel voor informatiebeveiliging.

Evaluatie en de BIO2

Bij de beslissing om de BIO via zelfregulering te verplichten voor de overheid, werd ook bepaald dat de BIO in 2023 moest worden geëvalueerd en vernieuwd. Ontwikkelingen, zoals de vernieuwde NEN-EN-ISO 27002 haalde de beoogde evaluatie naar voren. Ook werd ondertussen duidelijk dat de NIS2-richtlijn (3) van kracht zou worden. Deze richtlijn biedt de gelegenheid om de BIO wettelijk te verankeren: de zorgplicht van NIS2 wordt grotendeels ingevuld door de BIO. In december 2022 is de evaluatie van de BIO versie 1.04 (4) afgerond. In de analyse zijn de beleidsdoelen opgenomen, de opzet van het instrument BIO en de toetsing en verantwoording. Om ervoor te zorgen dat de huidige BIO meegaat met de ontwikkelingen en dat er wordt aangesloten op de nieuwe nummering en inrichting van de NEN-EN-ISO 27002, is op 1 juni 2023 de handreiking BIO2.0-opmaat (5) opgeleverd. In deze handreiking is dezelfde indeling toegepast: de controls, doelstellingen en overheidsmaatregelen. Ook is er een aantal overheidsmaatregelen geactualiseerd, vanwege nieuwe dreigingen, zoals ransomware.

Ontwikkeling van de BIO2

De ontwikkelingen buitelen over elkaar heen. De overheid moét meebewegen. Een aantal van deze ontwikkelingen zijn bepalend voor de BIO2:

1. Risicomanagement: in de nieuwe BIO komt meer aandacht voor risicomanagement en worden de beveiligingsniveaus (BBN's) losgelaten. Het toepassen van de BBN's werkte in de hand dat de focus op het classificeren van de individuele systemen op de BBN kwam te liggen en daardoor minder op algemeen risicomanagement en de specifieke risico's voor informatiesystemen. Risicomanagement als uitgangspunt van de organisatie is ook in lijn met doelen uit de NEN-EN-ISO 27001 en de NIS2.
2. Voldoen aan wet- en regelgeving: uit de evaluatie blijkt dat het opnemen van verwijzingen naar wet- en regelgeving onduidelijkheid oproept bij de gebruikers. Deze expliciete doelstelling zal daarom verdwijnen uit de BIO2. Verwacht mag worden dat in lijn met risicomanagement een organisatie zelf haar context met de daarin van toepassing zijnde wet- en regelgeving analyseert.
3. Invulling maatregelen NIS2: de NIS2 schrijft de zorgplicht van een entiteit voor en geeft ook definities voor digitale basishygiëne. De maatregelen uit de NIS2 bestaan uit verplichte maatregelen en maatregelen die situationeel zijn. Een gedeelte wordt niet gedekt door de BIO. Vanuit een interbestuurlijke werkgroep BIO is een inventarisatie gemaakt van de aanvullende, noodzakelijke en wenselijke maatregelen op basis van de NIS2.
4. Aandacht voor andere IT-omgevingen: de BIO is een norm voor alle overheidslagen en sluit geen systemen uit. Het is dus belangrijk dat de BIO ruimte geeft om alle omgevingen veilig te maken. Overwogen wordt bijvoorbeeld het aandachtsgebied zorg en Internet of Things (IOT) onder de paraplu van de BIO te brengen.

Vervolgacties doorontwikkeling BIO

De eerste acties zijn gericht op afstemming met de vier overheidslagen. In estafettesessies zijn de CISO's binnen de overheid meegenomen en betrokken in de verdere ontwik-

Toezicht speelt een belangrijke rol in de naleving van wet- en regelgeving

keling van de BIO. De resultaten daarvan worden nu verwerkt in het functioneel ontwerp voor de BIO2. Daarna wordt tot de zomer 2024 gewerkt aan het omzetten van de huidige 'BIO opmaat' naar de BIO2. Als het functioneel ontwerp vastgesteld is, zullen we dit in een vervolgartikel in het iB-Magazine delen.

Toezicht informatieveiligheid bij de overheid

Toezicht speelt een belangrijke rol in de naleving van wet- en regelgeving en meer algemeen in het beschermen van publieke belangen. Toezicht op informatieveiligheid is niet nieuw bij de overheid. Een voorbeeld zijn de DigiD-assessments bij gemeenten; gemeenten moeten vooraf aantonen dat hun informatieveiligheid op orde is om diensten te kunnen aanbieden via DigiD. Wel is het bestaande toezicht versnipperd. Overheidsorganisaties en met name medeoverheden hebben daardoor een forse administratieve last. In de Werkagenda Waardengedreven Digitaliseren is toezicht op informatieveiligheid opgenomen als actie met als doel de bestaande auditlast te verlagen (7). Het organiseren van toezicht wordt verder geholpen door NIS2, waarin toezicht verplicht wordt gesteld. Bij de uitwerking van het toezicht is een aantal uitgangspunten relevant:

1) Het toezicht moet proportioneel zijn en aansluiten bij de te beschermen belangen;
2) Het toezicht wordt vormgegeven op basis van bestaande verantwoordings- en toezichtstructuren in alle overheidslagen;
3) Het toezicht vindt plaats op basis van de BIO;
4) Het toezicht moet onafhankelijk zijn.

Het risico bestaat dat de BIO wordt gebruikt als checklist en dat leidt af van het verbeteren van de feitelijke veiligheid van overheidsorganisaties. Dat wordt een belangrijk aandachtspunt bij de inrichting van het toezicht. In het toezicht zal centraal staan dat overheidsorganisaties risicomanagement hanteren en maatregelen treffen op basis van risicoafweging.

Tot slot

Met de eerdergenoemde Werkagenda wordt hard gewerkt aan een veilige digitale wereld waarin iedereen mee kan doen. De BIO2, in lijn met de NIS2, legt hier een belangrijke basis voor. Er is veel in ontwikkeling: de implementatie van de NIS2 in nationale wetgeving, de ontwikkeling van een nieuwe BIO en de inrichting en het uitwerken van toezicht. Met dit artikel is een inkijkje gegeven in deze ontwikkelingen. De digitale wereld is continu in beweging en het kan verleidelijk zijn om af te wachten hoe deze ontwikkelingen verder gaan.
Ons advies: ga en blijf aan de slag, dreigingen wachten niet op nieuwe wet- en regelgeving. Dus blijf werken aan het verbeteren van de informatieveiligheid binnen je organisatie!

- Hanteer de bestaande BIO om je informatieveiligheid binnen de organisatie op orde te brengen en maak daarbij gebruik van de verplichte standaarden;
- Volg de communicatie over de bredere thema's zoals CSIRT en toezicht. www.digitaleoverheid.nl is dé plek waar alle informatie te vinden is;
- Start in ieder geval met een risicoanalyse, inclusief je leveranciers en andere partijen in de keten.

Werkagenda Waardengedreven Digitaliseren in thema's

1. Iedereen kan deelnemen aan de digitale wereld. We moeten zorgen voor digitale vaardigheden bij iedereen, inclusief het bewustzijn over kansen en risico's van digitale technologie. Online overheidsdiensten zijn makkelijk te begrijpen en toegankelijk voor iedereen.
2. Iedereen kan de digitale wereld vertrouwen. Er is bescherming tegen online criminaliteit, discriminatie en haat zaaien. En online-informatie is betrouwbaar. Overheidsorganisaties zijn weerbaar tegen digitale aanvallen en hebben herstelmaatregelen georganiseerd voor als het toch mis gaat.
3. Iedereen heeft grip op het digitale leven. Iedereen heeft inzicht in en controle over de eigen persoonlijke gegevens en online aanwezigheid. Door gegevens in te kunnen zien, te kunnen delen en te kunnen corrigeren.
4. Als digitale overheid geven we het goede voorbeeld door open en waardengedreven te werken. Hiermee zetten we als overheid de standaard als het gaat om het verantwoord inzetten van digitale technologie.
5. Versterken van de digitale samenleving in het Caribisch deel van het Koninkrijk. Hiermee zetten we als overheid in op verantwoorde inzet van digitale technologie in het Caribisch deel van het Koninkrijk.

Referenties

(1) www.rijksoverheid.nl/documenten/rapporten/2023/12/22/geactualiseerde-werkagenda-waardengedreven-digitaliseren-2024
(2) BIG staat voor Baseline Informatiebeveiliging Gemeenten, BIWA voor Baseline Informatiebeveiliging Waterschappen, IBI voor Interprovinciale Baseline Informatiebeveiliging en BIR voor Baseline Informatiebeveiliging Rijksdienst.
(3) NIS staat voor Network and Information Security. Dit is de nieuwe Europese cybersecurityrichtlijn die organisaties beter moet beschermen tegen cyberaanvallen.
(4) De evaluatie vind je op www.digitaleoverheid.nl
(5) De handreiking BIO2.0-opmaat beschikbaar op www.BIO-overheid.nl
(6) www.digitaleoverheid.nl/werkagenda-waardengedreven-digitaliseren/#Versterken-cybersecurity-Acties