Reactie Internetconsultatie Cyberbeveiligingswet

Vooraf heb ik de andere reacties doorgenomen, met de meeste van de opmerkingen ben ik het eens. De door anderen gemaakte opmerkingen zal ik zoveel mogelijk niet herhalen. Hieronder volgen enkele aanvullende opmerkingen van mezelf.

Zorgplicht / Risicoanalyse (art 23)

- In art 23 wordt de zorgplicht beschreven. De zorgplicht bestaat uit het nemen van passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Het passend zijn van de maatregelen vloeit voort uit het analyseren van risico's. Er moet in ieder geval daarbij rekening gehouden worden met de stand van de techniek, de uitvoeringskosten en Europese en internationale normen. De woorden 'in ieder geval' in lid 2 geven al aan dat er bij een risicoanalyse met veel meer zaken rekening moet worden gehouden.
- Was het niet beter geweest te stellen dat de risicoanalyse moet voldoen aan relevante normen op dat gebied. Voorbeelden zijn ISO 27001 Managementsystemen voor informatiebeveiliging, de hoofdsstukken 6 en 8. Deze verwijst naar de ISO 31000 Risicomanagement – Principes en richtlijnen. De guidance uit 27005 Guidance om managing information security risks is ook waardevol.
- Zie verder ook het ENISA document Interoperable EU Risk Management Framework (Methodology for assessment of interoperability among risk management frameworks and methodologies, Updated Report, December 2022).
- Gevolgen van de huidige teksten:
    - Nog steeds beperkte bemoeienis van bestuurders met risicomanagement.
    - Risicomanagement die niet aantoonbaar onvoldoende is, onvoldoende voldoet aan relevante eisen.
    - Er worden nog steeds onverantwoorde risico's gelopen.

Governance (art 26)

- In art 26 wordt geschreven over de instemming die het bestuur moet geven aan de te nemen maatregelen (lid 1) en de kennis en vaardigheden die het daarvoor moet hebben (lid 2).
  - Opmerkingen daarbij:
    - De betrokkenheid van het bestuur moet breder zijn dan alleen het instemmen met maatregelen. Het bestuur moet eveneens instemmen als bijvoorbeeld het beleid rondom risicoanalyse, risicoacceptatie (-criteria) etc. Zie ISO 27001 H6.
    - Het stellen van eisen aan kennis en vaardigheden van bestuursleden kan nooit een doel zijn. Het door bestuurders voldoen aan die eisen is slechts een middel bij het verkrijgen van leiderschap en commitment van het management bij het uitvoeren van risicomanagement het realiseren en continue verbeteren van de informatiebeveiliging. Zie ISO 27001, par 5.1 .
    - Merkwaardig hierbij is de expliciete aandacht voor het aantoonbaar zijn van de kennis en vaardigheden van bestuurders. Voor het geheel van de zorgplicht en de governance geldt dat aantoonbaarheid van sturing en uitvoering belangrijk is.
      Vwb het hebben van kennis en vaardigheden: zie ISO 27001 par 7.2 Competentie.
      Vwb de aantoonbaarheid van specifiek de aanwezigheid van kennis en vaardigheden: In zijn algemeenheid het geheel van het managementsysteem rondom informatiebeveiliging (het ISMS): zie ISO 27001 par 7.5 Gedocumenteerd informatie.
    - Het met behulp van het analyseren van risico's en het treffen van maatregelen is een (te) enge benadering van het voldoen aan de zorgplicht van entiteiten. Om te zorgen dat een passend niveau van informatiebeveiliging aanwezig is zal een zgn. ISMS (Information Security Management System) aanwezig moeten zijn. Een managementsysteem is een geheel van samenhangende of elkaar beïnvloedende elementen van een organisatie om een beleid en doelstellingen vast te stellen, alsmede de processen om die doelstellingen te bereiken (zie ISO 9001, 3.5.3). Het analyseren en mitigeren van risico's is slechts een onderdeel van een ISMS.
    - In een dergelijk managementsysteem is ook aandacht voor continue verbetering via de PDCA-cyclus. Deze aandacht ontbreekt in dit wetsvoorstel. Ten onrechte. Doel van de Cbw is gericht op het verhogen van de cyberbeveiliging (art 2). Ik hoop dat dit niet

alleen initieel moet gebeuren, maar dat een continue activiteit is. De hackers worden steeds beter, die hebben wel een PDCA-cyclus.
    - Gevolgen:
        - Beperkte betrokkenheid van het bestuur, dat beperkt zich tot risicomanagement en de kennis en vaardigheden daarvoor.
        - Een middel, het stellen van eisen aan kennis en vaardigheden van bestuurders, wordt tot doel verheven.
        - Veel aandacht voor aantoonbaarheid van de kennis en vaardigheden van het bestuur. Onvoldoende aandacht voor de aantoonbaarheid van alle andere onderdelen van het ISMS.
        - Onvoldoende invulling zorgplicht, onvoldoende aantoonbaar risicomanagement.
- Significante incidenten (art 27 ev)
  Een eigenschap van kwetsbaarheden en de daaruit voortvloeiende (significante) incidenten is dat deze zich in meer of mindere mate voordoen bij vele netwerk- en informatiesystemen en dat ze zich niet houden aan grenzen van sectoren en/of EU-lidstaten. Kortom als zich een significant incident voordoet is het aannemelijk dat daar vele entiteiten uit vele sectoren en vele landen bij betrokken zijn. Bij de oplossing van een dergelijk incident is haast geboden om eventuele schade zo veel mogelijk te beperken. Hoe slim is het dan om als cybercrisisbeheerautoriteit (Min JV) minimaal met 7 CSIRT's en met 7 bevoegde autoriteiten aan tafel te moeten zitten en besluiten te moeten nemen. Hoe minder partijen, hoe sneller?
  Gevolgen:
    - Onvoldoende snel en eenduidig oplossen van gemelde significante incidenten, waardoor onnodig schade wordt gelopen.
    - De vraag is in hoeverre de overheid, na in werking treden van de Cbw aansprakelijk kan worden gesteld bij nalatigheden?
- Aanwijzing en taken bevoegde autoriteit (art 16), Aanwijzing en taken CSIRT (art. 17), Aanwijzing en taken coördinator bekendmaking kwetsbaarheden (art. 18), aanwijzing taken cybercrisisbeheerautoriteit en Toezicht en handhaving (H16).
  Bestuursleden van entiteiten dienen aantoonbaar bepaalde kennis en vaardigheden te hebben (art. 16, lid2). Is het, in het verlengde daarvan, wellicht verstandig dergelijke expliciete eisen ook te stellen t.a.v. bestuurders/medewerkers van bevoegde autoriteiten, CSIRTs, de coördinator bekendmaking kwetsbaarheden, de cybercrisisbeheerautoriteit, de toezichthouders en de handhavers en de werkzaamheden die zij uitvoeren? Weliswaar vallen deze entiteiten ook onder de Cbw (?), maar het belang ervan kan niet genoeg benadrukt worden. Ook op allerlei activiteiten in dit gebied zijn er normen aanwezig, bv de ISO 19011 Richtlijnen voor het uitvoeren van audits van managementsystemen.
  Gevolgen:
    - Onvoldoende invulling van taken van belangrijke overheidsentiteiten binnen de Cbw, waardoor onnodig risico's worden gelopen en daaruit voortvloeiende significante incidenten onnodige te langzaam worden opgelost.

Overig
- In de NIS2 is aandacht voor het gebruik van Europese Cyberbeveiligingscertificeringsregelingen (art. 24) en normalisatie (art. 25 Normalisatie).
  Die aandacht is er in het wetsvoorstel vwb normalisatie in mindere mate. Bij het nemen van de maatregelen houdt de entiteit in ieder geval rekening met o.a. desbetreffende Europese en internationale normen (art. 23).
  Die aandacht is er vwb een certificeringsregeling niet, terwijl al vele jaren gecertificeerd kan worden tegen ISO 27001 en dat heel waardevol is. Ook ter vergelijking: in het kader van eIDAS worden uitgevers van eIDAS diensten (ook overheidspartijen) al jaren gecertificeerd en dat is een breed geaccepteerde werkwijze.
  Gevolgen:
    - Onvoldoende aandacht voor certificering en normalisatie.
    - Onvoldoende kwaliteit van cyberbeveiliging. Onnodig lopen van risico's.
    - Inefficiënte cyberbeveiliging, de keten is zo sterk als de zwakste schakel.
- In art 76a van het wetsvoorstel wordt geregeld dat de artikelen 74, 75 en 76 niet van toepassing zijn op overheidsinstanties. Artikel 74 betreft het stellen van een einddatum voor beëindiging van een overtreding. Artikel 75 betreft het indienen van een verzoek tot schorsing certificering of vergunning. Artikel 76 betreft het indienen van een verzoek tot schorsing leden van het bestuur.
  Waarom er voor overheidsinstanties geen einddatum gesteld kan worden en er niet geschorst kan worden is me niet duidelijk. Schorsen gebeurt in het kader van het leveren van elektronische identificatie en vertrouwensdiensten (eIDAS) toch ook.

Vwb de uitzondering t.a.v. het schorsen van leden van het bestuur merk ik het volgende op: de overheidsdiensten hebben bepaald een reputatie als het aankomt om het niet nakomen van wet- en regelgeving (bv BIO, AVG en Archiefwet), terwijl de overheid een voorbeeldfunctie heeft (zoals vermeld in de Memorie van Toelichting, 5.1.1.3).
Gevolgen:
- Overheidsentiteiten langer dan wenselijk niet voldoen aan de Cbw en daardoor de aan haar toegedachte voorbeeldfunctie niet voldoende invult.

- Aan de Nationale CyberBeveiligingsStrategie (art. 20) worden geen eisen gesteld, zoals in NIS2 art7 wel gebeurt.
Gevolgen: onvoldoende kwaliteit Nationale CyberBeveiligingsStrategie.

Memorie van Toelichting
In 5.1.1.3 Overheidsinstanties wordt volgende gesteld:

- Overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van de nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving zijn uitgesloten van het toepassingsbereik van de NIS2-richtlijn (zie artikel 2, zevende lid, van de NIS2-richtlijn). De verplichtingen uit de NIS2-richtlijn zijn dan ook niet op hen van toepassing, zie artikel 6 Cbw. Omdat het kabinet er aan hecht dat de hiervoor genoemde, blijven voldoen aan een hoog cyberbeveiligingsniveau, zullen zij blijven voldoen aan verplichtingen zoals bij de Rijksdienst thans geregeld in het VIR 2007, het VIR – BI 2013, en de BIO en in toepasselijke verplichtingen van internationale herkomst.
De redenen voor deze uitsluiting worden niet gegeven. Hebben deze entiteiten geen netwerk- of informatiesystemen of zijn ze niet belangrijk (genoeg)? Is de keten niet zo sterk als de zwakste schakel?
- Maar inhoudelijk: het VIR beschrijft vooral de verantwoordelijkheden van het lijnmanagement voor de beveiliging van zijn informatiesystemen. Het VIR-BI gaat vooral over rubricering van Bijzondere Informatie en de gevolgen die dat heeft voor de aan de beveiliging te stellen eisen (risicomanagement en verplichte maatregelen?).
De BIO is in de basis een kopie van de ISO 27002 (2013). Deze ISO 27002 is een uitwerking van de Bijlage A van de ISO 27001 en die bijlage is bedoeld om de volledigheid van de risicoanalyse te toetsen (Zie ISO 27001, 6.3.1 Behandeling van informatiebeveiligingsrisico's, onderdeel c.). In de BIO is de risicoanalyse uitgekleed tot een impactanalyse, waarbij veelal standaard uitgekomen wordt op BBN2. Zie hiervoor ook de Evaluatie BIO (Berenschot, 17nov 2022).
- Naast deze beperkingen van de 3 genoemde documenten is het de vraag in hoeverre er bij deze uitgesloten entiteiten sprake is van een hoog cyberbeveiligingsniveau indien wordt voldaan aan de 3 genoemde documenten. In ieder geval wordt dat niet met regelmaat aangetoond. Eveneens is het toezicht niet geregeld.
- Inmiddels wordt gewerkt aan een nieuwe versie van de BIO, de BIO 2.0, en heeft het kabinet de ambitie uitgesproken om informatiebeveiligingsregelgeving overheidsbreed te harmoniseren. De BIO zal ook wettelijk verankerd worden. Op zich is dat een nobel streven. De vraag is of het nieuwe kabinet ook daarnaar gaat streven. Maar waarom al deze inspanningen. Simpeler en beter is het de ISO 27001 en certificering daartegen verplicht voor te schrijven (ook voor de overheid) of in ieder geval art 76a te schrappen. Daarmee wordt dan ook een bijdrage geleverd aan het streven uit de NIS2 naar normalisatie en certificering (art 24 en 25). De overheid moet tenslotte het goede voorbeeld geven.
Gevolgen:
  - Voor onderdelen van de overheid gelden andere regels (de BIO i.p.v ISO 27001).
  - De ISO 27001/2 wordt onderhouden door ISO. De overheid besteed veel tijd aan beheer en onderhoud van de BIO. Dat is weinig efficiënt.
  - Het toezicht op de BIO is niet geregeld.
  - Deze aanpak doet afbreuk aan het streven naar normalisatie en certificering.
  - De overheid geeft niet het goede voorbeeld.
  - Er worden onnodig risico's gelopen bij betreffende overheidsonderdelen. De beveiliging blijft zo sterk als de zwakste schakel.

Slordigheden

- In art. 18 staat dat bij AMvB de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden wordt aangewezen. In art 17 (Aanwijzing en taken CSIRT), lid 2h staat "indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 18 (Aanwijzing en taken coördinator bekendmaking kwetsbaarheden) bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden". Voor de goede orde er komen meerdere CSIRT's, waarvan er één coördineert?

- Verwijzingen:
    - In Art 1 Bevoegde Autoriteit wordt verwezen naar art 16. Moet dan niet art. 15 zijn?
    - In Art 1 Coördinator wordt verwezen naar art 12. Moet dan niet art. 18 zijn?
    - In Art 1 cybercrisisbeheerautoriteit wordt verwezen naar art 15. Moet dan niet art. 19 zijn?