

## NIS2 opmerkingen

### A) Privacy impact (algemeen punt):

Er zitten ongetwijfeld goede kanten aan deze wet, maar ook hele gevaarlijke kanten. Daar mogen we de ogen niet voor sluiten. Mij ontbreekt een privacy impact assessment voor de Nederlandse burger. Deze wet heeft betrekking op digitale infrastructuren waar heel veel data van Nederlandse bedrijven en van alle Nederlanders toe behoren, in situ of in transit, in binnen- en buitenland. De privacy impact assessment is belangrijk vanwege o.a. de volgende redenen:

- Artikel 17 lid 2a geeft aan wat CSIRT's moeten kunnen: *monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau;*
- Artikel 17 lid 2d geeft aan *“het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging.”*
- Wat betekent dit voor informatie van Nederlandse bedrijven en burgers in andere landen binnen Europa?
- Informatie komt beschikbaar op Europees niveau bij Europese organen. Hoe liggen daar de bevoegdheden?

Ik heb tot nu toe niet gelezen hoe ver deze bevoegdheden gaan en waar de grens is, en wie dat bewaakt. Krijgen we met de CSIRT's allemaal nieuwe AIVD'tjes die (zeker in het begin) hun weg moeten gaan zoeken en gaan 'hobbyen' met data? Zijn mijn persoonlijke online-gegevens wel veilig, worden de informatiestromen van mijn bedrijf straks tegen mij gebruikt?

Conclusie: Ik verwacht bij deze wet een privacy impact assessment met een raadpleging van de Autoriteit Persoonsgegevens. Ik verwacht regels aan bevoegdheden.

### B) Het middel is erger dan de kwaal (algemeen punt).

Ik ben mij er volledig van bewust dat dit een onomkeerbaar proces is en dat dit een weinig zinnig statement is, maar ik zeg het toch: Waar zijn we met z'n allen mee bezig? Ja, het middel is erger dan de kwaal en wel hierom.

- In par. 8.3 van de Memorie van Toelichting wordt een inschatting gemaakt van de budgettaire kosten per departement (incl. Wwke). Het plaatje is verre van compleet, maar zal in totaal waarschijnlijk boven de 100 miljoen per jaar liggen. En dan (extra) kosten van CSIRTS, implementatiekosten bij de bedrijven, de Europese organen en overlegstructuren. En dan zijn wij nog een relatief kleine lidstaat, en dat keer 27 lidstaten.
- We zijn dus jaarlijks vele miljarden kwijt aan ambtenaren, inrichting en uitvoering, zonder garantie dat er geen hacks meer zullen plaatsvinden. En die hacks gaan echt plaatsvinden.
- De rekening komt uiteindelijk weer bij de burger, de consument. Niet alleen financieel, maar ook qua privacy. Vreselijk.

Conclusie:

Een negatieveling zou zeggen: De kans die we liepen om gehackt te worden en geld kwijt te raken was klein, maar is nu een zekerheid geworden: We zijn het geld altijd kwijt, maar nu aan andere 'boeven'.

### **C) Transparant over de kosten (algemeen punt)**

Entiteiten krijgen te maken met gedwongen winkelnering van een CSIRT. Dat is een dienstverlening waar op dit moment nog behoorlijk voor betaald moet worden. Ik lees in de MvT dat departementen de kosten dragen van onder meer de CSIRT's.

Het is wenselijk om snel met een transparant te verwachten kostenplaatje te komen voor de entiteiten. Ook als er geen kosten doorberekend worden voor bijvoorbeeld de dienstverlening van een CSIRT etc. is het wenselijk om dat te communiceren.

### **D) Artikel 4 (jurisdictie en territorialiteit)**

De schrijvers dienen zich af te vragen of het wetsvoorstel de juiste prioriteiten stelt en wel voldoende toekomstbesteding is. Drie voorbeelden:

1. Is een auto een vervoermiddel met een computer, of is het ondertussen een computer die dient als vervoermiddel? Autofabrikanten zetten miljoenen auto's op de (Europese) markt. Stel dat fabrikant T. gehackt wordt en de hackers alle auto's van merk T. op volle snelheid kunnen laten rijden, dan heeft dat direct vele slachtoffers, een verkeerschaos en een zorginfarct tot gevolg. Dit zal heel Nederland/Europa ontwrichten.
2. Een aanbieder van AI kan zich mogelijk -door zich slim te positioneren- aan deze wet onttrekken.
3. Daar staat tegenover dat 'Tante Aartje', een door mij verzonden kleine woonzorglocatie in een dorpje in Groningen - en net groot genoeg om als essentiële entiteit aan te merken - te maken krijgt met een behoorlijke lastenverzwaring. En dat terwijl de zorg best een tijdje door kan zonder ICT, want zorg is vooral ook mensenwerk.

Conclusie:

- 1) Er wordt qua scope en reikwijdte hier en daar de boot gemist.
- 2) Weer wordt de gezondheidssector over één kam geschoren, terwijl er zo veel verscheidenheid is in deze sector. Is 'Tante Aartje' *een kritieke maatschappelijke of economisch belangrijke functie of activiteit die in stand gehouden moet worden?* (het doel van deze wet?) Een nadere differentiatie van de gezondheidssector zou de beperking van de lastenverzwaring voor de zorg ten goede komen.

### **E) Artikel 26 (governance):**

- Ik kan mij vinden in deze governance verplichtingen aangezien ik regelmatig in de praktijk merk dat zij door onbegrip of onwil geen middelen beschikbaar stellen. Een versoepeling van dit artikel is een slecht signaal.
- Artikel 26 lid 1 is boterzacht geformuleerd, daarom het volgende tekstvoorstel: *De maatregelen, bedoeld in artikel 23, zijn onderworpen aan goedkeuring door het bestuur van de desbetreffende essentiële entiteit of belangrijke entiteit. Het bestuur ziet toe op de maatregelen en de uitvoering van de maatregelen door controles te laten uitvoeren, de interne controle- of auditrapporten tijdens haar overleg te*

behandelen en daarop te sturen. Het bestuur zorgt ervoor dat haar activiteiten aantoonbaar en navolgbaar zijn in bijvoorbeeld de vastlegging van de bijeenkomsten.

**F) Artikel 68 (controlefunctionaris)**

Ik vind het op deze wijze kunnen aanstellen van een controlefunctionaris door de bevoegde autoriteit, op kosten van de entiteit, een beetje te kort door de bocht. Daarom dit tekstvoorstel:

Lid 1: *Indien de essentiële entiteit geen controlefunctionaris heeft aangesteld of deze op aangeven van de bevoegde autoriteit niet kan of wil aanstellen kan de bevoegde autoriteit deze voor een bepaalde periode aanwijzen*

Lid 3: De essentiële entiteit draagt de kosten van de controlefunctionaris, tenzij een bij algemene maatregel van bestuur omschreven geval zich voordoet waarin de betrokken entiteit deze kosten niet hoeft te dragen. De tijdsduur van de inzet en het tarief van de door de bevoegde autoriteit aangestelde controlefunctionaris is marktconform.