Namens de brancheverenigingen OIZ en Nedxis maak ik graag van de gelegenheid gebruik om commentaar te geven op de implementatie van de NIS2

OIZ vertegenwoordigt circa 70 ICT-leveranciers in de Zorg, waaronder nagenoeg alle EPD-leveranciers. Nedxis vertegenwoordigt alle eerstelijns leveranciers voor huisarts- en apotheek systemen.

3 Kernpunten

1. Schaarse deskundigheid (zowel kennis als ervaring)

De komende jaren staat de arbeidsmarkt al voldoende onder druk en zal de schaarste in deskundigheid op het gebied van informatiebeveiliging alleen maar toenemen. Volgens ons is het in Nederland al goed geregeld. Voorkom dat NIS2 weer tot nieuwe instanties en procedures leidt. Zorg dat NIS2 wordt gebruikt om procedures juist eenduidiger te maken.

Ons advies: Kijk kritisch naar hoe goed het in Nederland al op basis van zelfregulering is geregeld en zorg voor minder bureaucratie. Concentreer dit soort toezicht bij nationale instanties, die zich hier al bewezen voor hebben gepositioneerd. Voor de zorg zou dat Z-Cert zijn.

2. Slechte uitwerking van de 'overall' governance

Met de IGJ en de AP zijn er al 2 toezichthouders die zich met dit onderwerp bezighouden en daarnaast heb je nog Z-Cert en NCSC. Bovendien wordt er in het kader van de Nationale Visie en Strategie op het gezondheidsinformatiestelsel nog nagedacht over een nieuwe autoriteit. Wie ziet tegenwoordig nog de bomen door het bos, of is dat juist de bedoeling?

Zowel de IGJ als de AP hebben een bewerkelijke meldprocedure. Als overheid kun je ook zorgen, dat die dubbelslagen juist stoppen. Wellicht biedt de NIS2 mogelijkheden om die dubbeling te stoppen. Als het informatiebeveiliging betreft zou die melding bij 1 instantie moeten plaatsvinden en dan moeten de IGJ en de AP maar afspraken maken hoe ze dit met elkaar uitwisselen.

De Ministeries en betrokken autoriteiten moeten op dit vlak streven naar synergie in plaats van overlappende werkzaamheden en versnippering van kennis en ervaring.

Ons advies: één (netwerk-)organisatie, die in de zorg gaat over het toezicht op de informatiebeveiliging en cybersecurity. Waar Nederland behoefte aan heeft, is meer duidelijkheid door minder instanties, minder versnippering, betere slagvaardigheid en meer bevoegdheden.

3. Geen/onvoldoende aandacht voor de Nederlandse praktijk van zelfregulering via NEN 7510 en ISO 27001

Ons advies;

1. omarm de NEN 7510 en ISO 27001. In de verwerkersovereenkomsten met leveranciers stellen zorgaanbieders dit al als vereiste. Voor de ICT-leveranciers is informatiebeveiliging een onderdeel van hun zorgplicht. Sluit de NIS2 hierop aan. Maak duidelijk wat er qua meldplicht additioneel speelt en hoe dit door zorgaanbieders en hun leveranciers moet worden ingevuld. In Nederland heb je de NIS2 dan feitelijk geregeld. En vanzelfsprekend ook graag een efficiënt meldproces met minder loketten.
2. Zorg voor VWS-coördinatie op dit punt. Kennelijk heeft VWS nog geen relatie gelegd met NIS2 in de opdracht voor de NEN 7510. Momenteel wordt de NEN7510 herzien en gaat die in de zomervakantie (juli) in publieke consultatie vanwege update van ISO. Wij vragen om rekening

te houden met NIS2 (momenteel in NL in publieke consultatie), omdat vanuit leveranciers en hun zorgaanbieders een enorme behoefte leeft om 7510 certificering te kunnen gebruiken om aan te tonen dat men aan NIS2 voldoet.

Namens Silizo, OIZ en Nedxis,

Robert van Wijk

27 juni 2024