18 Juni - Festival CyberSecurity in de Zorg

NIS2: Het spook van de Spreekkamer?

Don Eijndhoven

Introductie

Don Eijndhoven

- Oprichter en voorzitter **Dutch Cyber Warfare Community**
- Researcher, schrijver en spreker over Cyber Warfare en Digitale Geopolitiek
- MSc Cyber Security Governance, Leiden University

Tevens

- **CEO cybersecurity bedrijf Argent Consulting B.V.**
- Interim Chief Information Security Officer (CISO), Enterprise Security Architect, Strategist
- Gastlector Nyenrode Business University
- Voormalig secretaris Stichting **Connect2Trust**

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.

Inhoud

- Context
- Voorgeschiedenis: NIS Directive 2016/1148
- NIS Directive 2022/2555 (NIS2)
  - Waarom een opvolger van NIS maken?
  - Wat is er nieuw in deze update?
- Wat staat er in de CyberBeveiligingsWet?
- Discussie: Dekt dat de dreiging? Wat is de definitie van ‘Goed’ in de Nederlandse Zorg?

Uitleg van termen

- Europese Richtlijn (Directive): Europese ‘opdracht’ aan de lidstaten om een bepaald resultaat te behalen. Ieder land maakt zn eigen wet om aan de richtlijn te voldoen.
  - Bijvoorbeeld: AVG is de Nederlandse verordening om aan het Europese GDPR te voldoen
- De Nederlandse invulling van de EU NIS heet de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni)
- De Nederlandse invulling van de EU NIS2 heet straks de Cyberbeveiligingswet (CBW).
- De term NIB2 is hetzelfde als NIS2

NIS Directive 2016/1148: Network and Information Security Directive

Een Europese informatie beveiligingsnorm gericht op het beschermen van 6 kritieke sectoren:

Financieel	**Water**
Energie	**Gezondheidszorg**
Transport	**Digitale Infrastructuur**

NIS Directive 2022/2555: Network and Information Security Directive 2

Waarom een update van NIS?

- Dreiging neemt toe - Meer gebruik van technologie en overheden nemen steeds meer deel aan het digitale slagveld
- Het aantal aanvallen neemt nog steeds toe en de schade wordt steeds groter
- Er is meer inzicht: de onderlinge relatie tussen sectoren maakt dat alles veel gevoeliger is dan gedacht
- Scope te klein en te weinig daadkracht in doorvoeren NIS(1) - Weinig toezicht en geen boetes

WAT IS ER NIEUW: UITBREIDING SCOPE

Essentieel	Belangrijk
Energie	Digitale aanbieders
Transport	Post- en Koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur	Levensmiddelen
Financiële markt	Chemische stoffen
Gezondheidszorg	Onderzoek
Drinkwater	Vervaardiging / Manufacturing
Digitale infrastructuur	
Beheerders van ICT Diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	

Wat is er nieuw in NIS2?

- De scope is flink uitgebreid; Meer sectoren en betere duiding:
  - Essentiële organisaties: Grote organisaties opererend in de kernsectoren.
  - Belangrijke organisaties: Grote en middelgrote organisaties in de kernsectoren én de additionele sectoren of een kritieke schakel in de toeleveringsketen voor een grote organisatie in die sectoren.
- Toezicht en Registratieplicht
- Bestuurlijke aansprakelijkheid en kennis-eis aan bestuurders

- Rapportageplicht significante incidenten bij CSIRT toezichthouder
  - Initiële melding binnen 24 uur na ontdekking;
  - Update binnen 72 uur;
  - Eindrapportage binnen één maand na de update;
  - Alle afwijkingen moeten binnen 24 uur gemeld worden.
- Stevige boetes bij overtreding van de norm
  - Essentiële entiteiten: €10 miljoen of 2%
  - Belangrijke entiteiten: €7 miljoen of 1.4%

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.

Definities

Een organisatie is ‘groot’ als er:

1. Minimaal 250 personen werkzaam zijn OF;
2. Er sprake is van een jaaromzet van meer dan 50 miljoen euro, en een balanstotaal van meer dan 43 miljoen euro

Een organisatie is ‘middelgroot’ als er:

1. Minimaal 50 personen werkzaam zijn OF;
2. Er sprake is van een jaaromzet van meer dan 10 miljoen euro, en een balanstotaal van meer dan 10 miljoen euro

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.

Zorgplicht: Het nemen van maatregelen

Artikel 21 lid 2:

De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.

Maar wat staat er nu concreet in de Cyberbeveiligingswet?

Het belangrijkste verschil: De Zorgplicht

Artikel 23 (zorgplicht)

1. Iedere essentiële entiteit en belangrijke entiteit neemt passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. Ook neemt zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken.

2. De in het eerste lid bedoelde maatregelen zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de in het eerste lid bedoelde risico's. Bij het nemen van de maatregelen houdt de entiteit in ieder geval rekening met de stand van de techniek, de uitvoeringskosten en, indien van toepassing, de desbetreffende Europese en internationale normen. Ten aanzien van de evenredigheid van de in het eerste lid bedoelde maatregelen houdt de entiteit naar behoren rekening met de mate waarin zij aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

3. De in het eerste lid bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen.

4. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de in het eerste lid bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten.

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.

Artikel 26: Governance

1. 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.

2. Ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit beschikt over kennis en vaardigheden om:

   a) risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren;
   b) risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen; en
   c) de gevolgen van de risico's en risicobeheersmaatregelen voor de diensten die door de entiteit worden verleend te kunnen beoordelen.

3. Ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit voldoet binnen twee jaar na de inwerkingtreding van het tweede lid aan het bepaalde in het tweede lid. Indien een lid na de inwerkingtreding van het tweede lid wordt benoemd, voldoet dit lid binnen twee jaar na diens benoeming aan het bepaalde in het tweede lid.

4. Ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit houdt de kennis en vaardigheden, bedoeld in het tweede lid, aantoonbaar actueel.

5. Met het oog op het aantonen van de kennis en vaardigheden moet een lid van het bestuur van een essentiële entiteit of belangrijke entiteit een certificaat van deelname overleggen, waaruit de deelname blijkt aan een training die de onderwerpen, bedoeld in het tweede lid, behandelt.

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.

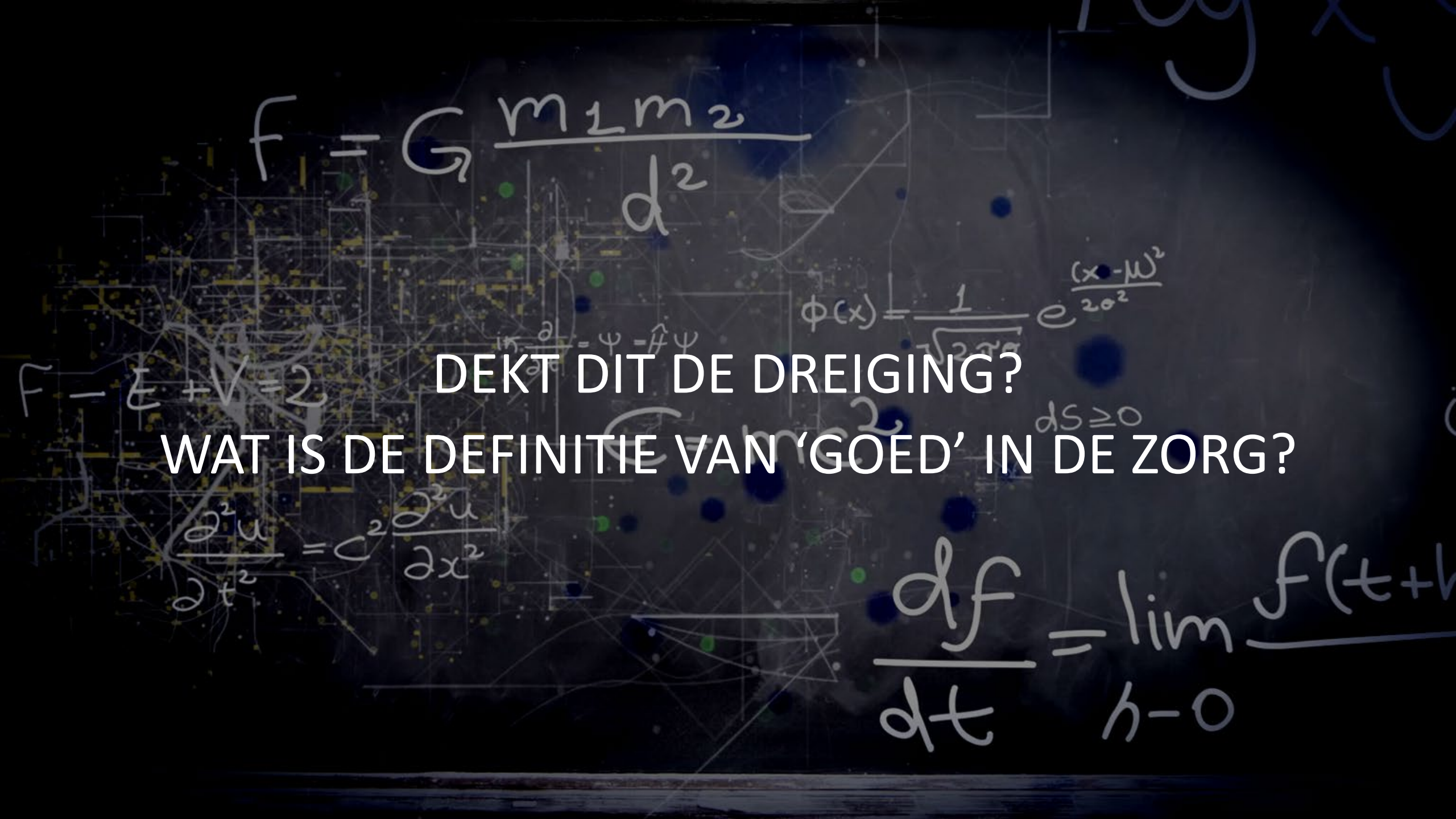
Samenvattend

- Weinig concreet: Welke maatregelen moet je nu nemen?
- Vage terminologie: “Passend en Evenredig” zijn in cybersecurity (meestal) tegengestelde belangen en “Stand der Techniek” is een nauwelijks toetsbaar concept
- Onduidelijk: Wat betekent “rekening houden” met “Europese en Internationale normen” in deze context?
- Ineffectief: Het Governance hoofdstuk is het meest helder en toch geenszins steekhoudend.

Het liberaal gebruik van de term “Algemene Maatregel van Bestuur” betekent dat, bij twijfel, de Toezichthouder bepaalt.

Alvast wat vragen beantwoordt..

- Dekt je cyber verzekering je als bestuurder tegen een NIS2 boete?
  - Nee. Maar niet om de reden die je zou verwachten.
- Hoe wordt er straks gehandhaafd?
  - Voor Essentiële entiteiten moet je pro-actief compliant zijn. Belangrijke entiteiten retro-actief en die zullen dus waarschijnlijk pas bij een incident onder de loep komen.
- Wie is toezichthouder van de Zorg?
  - In ieder geval het Ministerie van VWS. Waarschijnlijk zal de Inspectie Gezondheidszorg en Jeugd (IGJ) het werk uitvoeren
- Hebben die toezichthouders al een antwoord klaar op waar je aan moet voldoen binnen iedere sector?
  - Dat lijkt er momenteel in ieder geval nog niet op.



DEKT DIT DE DREIGING?

WAT IS DE DEFINITIE VAN ‘GOED’ IN DE ZORG?

Contact informatie

Argent Consulting B.V.

Don Eijndhoven

D.Eijndhoven@argentconsulting.nl

Twitter: @argentconsultin

+31 6 450 850 21

Copyright 2020 by Argent Consulting B.V. All rights reserved. Please do not distribute without express written consent of the author.