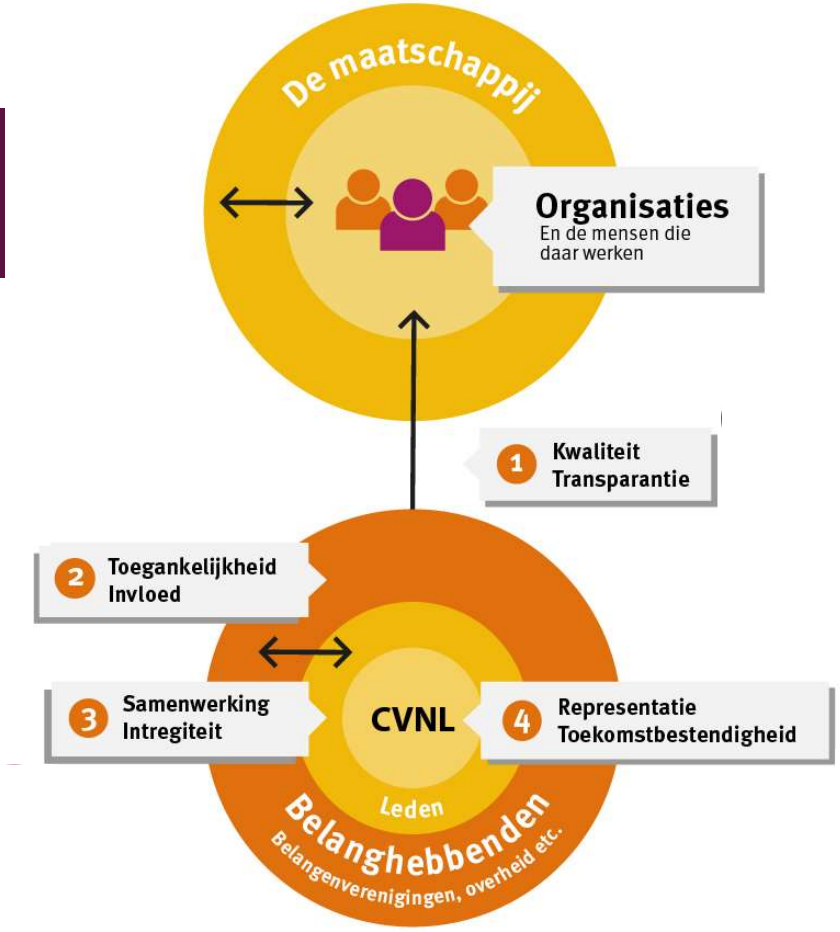
CYBERVEILIG NEDERLAND

Aan de slag met de Cbw (NIS2)

juni 2024

Cyberveilig NL ondersteunt haar leden in het weerbaar maken van de maatschappij

De expertise-gebaseerde drijfveer van CVNL staat aan de kern van onze identiteit als brancheverenigingen



De NIS2 zal worden omgezet in de Cyberweerbaarheidswet (Cbw)

Artikel 1

Onderwerp

1. Deze richtlijn voorziet in maatregelen die erop gericht zijn een hoog gemeenschappelijk niveau van cyberbeveiliging in de [Europese] Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

Sinds 2016 is er een Europese richtlijn die in de EU het niveau van cybersecurity moet verhogen

6 juli 2016

Network & Information Systems directive (NIS)

→

9 november 2018

Wet beveiliging netwerk- en informatiesystemen (Wbni)

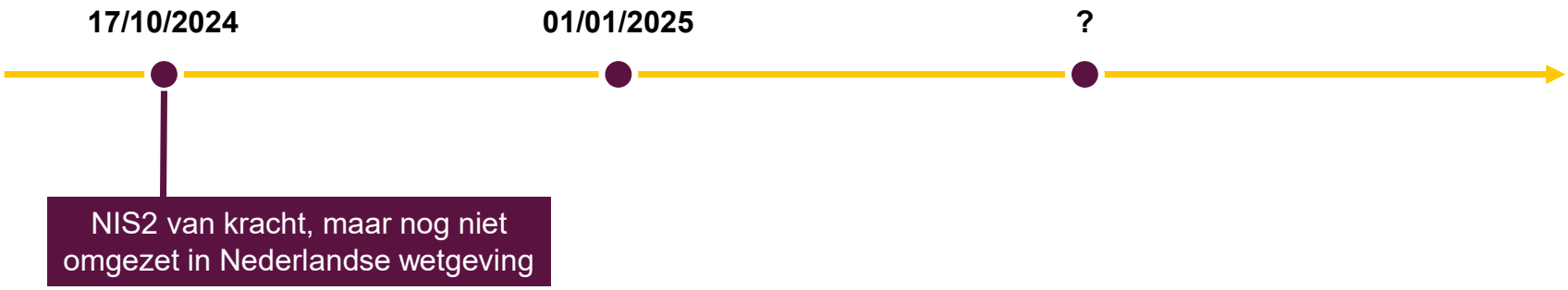
16 januari 2023

Network & Information Systems directive 2 (NIS2)

→

17 oktober 2024 =
implementatie datum Cyberbeveiligingswet (Cbw)
Deze wordt echter pas medio 2025 verwacht

Omdat de NIS2 vanaf 17 oktober 2024 van kracht is, maar nog niet is geïmplementeerd, is er sprake van een overgangssituatie



NIS2 van kracht, maar nog niet omgezet in Nederlandse wetgeving

Planning is eind 2024 stemming in Tweede Kamer en medio 2025 omgezet in Nederlandse wetgeving

Wbni blijft van kracht

Dit betekent dat organisaties die nog niet onder de Wbni vallen en wel onder de Cbw nog niet aan de (zorg- en meld)plichten hoeven te voldoen, maar wel (CSIRT) rechten kunnen ontlenen bij een incident

Cwb: ondersteuning door CSIRT's, zorgplicht én meldplicht

- Ontvangen van relevante dreigingsinformatie
- **CSIRT-ondersteuning** die aan **extra randvoorwaarden** moet voldoen **(artikelen 17 Cbw)**
- Voor de zorg wordt **Z-CERT** aangewezen

Het nemen van passende cybersecurity maatregelen waarbij een **minimale set van maatregelen** wordt vereist **(zie artikel 21 lid 2 NIS2)**

Digitale (bijna-) incidenten die voldoen aan **drempelwaarde** melden bij CSIRT (voor bijstand) en toezichthouder (controle)

Meldplicht (hfst. 9 Cbw): "early warning" binnen 24 uur, melding binnen 72 uur, eindverslag binnen 1 maand)

Rechten Cbw

Plichten Cbw

Bron: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders

De reikwijdte van de Cbw is breder: essentiële en belangrijke sectoren

NIS	NIS2	Toezicht
Sectoren	Essentiële sectoren	Proactief
• Energie • Vervoer • Bankwezen • Infrastructuur financiële markt • Gezondheidszorg • Drinkwater • Digitale infrastructuur	• Alle NIS-sectoren (muv DSP's) • Afvalwater • Beheer van ICT-diensten • Overheid • Ruimtevaart	De toezichthouder waar de aanbieder onder valt
	Belangrijke sectoren	Reactief
Digitale dienstverleners	• Post- en koeriersdiensten • Afvalstoffenbeheer • Chemische industrie • Levensmiddelenindustrie • Maakindustrie • Digitale aanbieders • Onderzoek	De toezichthouder waar de aanbieder onder valt
• Aanbieders van clouddiensten • Online zoekmachines • Online marktplaatsen		

Zelfevaluatie: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Bron: Bijlage I en II in de NIS2 - https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555

NHS England

NHS England — London

Search

About us | Our work | Contact us

NHS England — London

News

News

Update on cyber incident: Clinical impact in south east London – Friday 14 June 2024

14 June 2024

News

On Monday 3 June, a ransomware cyber attack was perpetrated against Synnovis, a pathology laboratory which processes blood tests on behalf of a number of NHS

14 June 2024

News

On Monday 3 June, a ransomware cyber attack was perpetrated against Synnovis, a pathology laboratory which processes blood tests on behalf of a number of NHS organisations, primarily in south east London.

The clinical impact of the attack has seen a significant reduction in the number of tests which can be processed and reported back to clinical teams.

In response, NHS England London declared a regional incident and has been coordinating work across affected services, as well as with neighbouring providers and national partners, in order to manage disruption.

Zorg als essentiële sector

	Essentieel	Belangrijk
De NIS2-richtlijn is van toepassing op alle organisaties in de gezondheidszorg die ook al onder de NIS-richtlijn vielen. Aangevuld met EU-referentielaboratoria, entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren en fabrikanten van medische hulpmiddelen, inclusief in-vitrodiagnostiek en medische hulpmiddelen die als kritiek worden beschouwd tijdens een noodsituatie op het gebied van volksgezondheid.	Een organisatie is groot als er minimaal 250 werknemers werken; of de organisatie een jaaromzet van meer dan 50 miljoen én een balanstotaal van meer dan 43 miljoen heeft.	Een organisatie is middelgroot als er minimaal 50 werknemers werken; of de organisatie een jaaromzet óf balanstotaal van meer dan 10 miljoen euro heeft.

Zorgplicht (artikel 23 Cwb)

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.

De extra maatregelen zien toe op een basisniveau van digitale veiligheid

Basismaatregelen vanuit de NIS2 (artikel 21 lid 2)	
a.	**Beleid** inzake **risicoanalyse** en **beveiliging van informatiesystemen**
b.	**Incidentenbehandeling**
c.	**Bedrijfscontinuïteit**, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer
d.	**Beveiliging** van de **toeleveringsketen**
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.	**Multifactor authenticatie**, **continue-authenticatieoplossingen**, **beveiligde communicatie**

Belangrijk is om te gaan redeneren vanuit de risico's

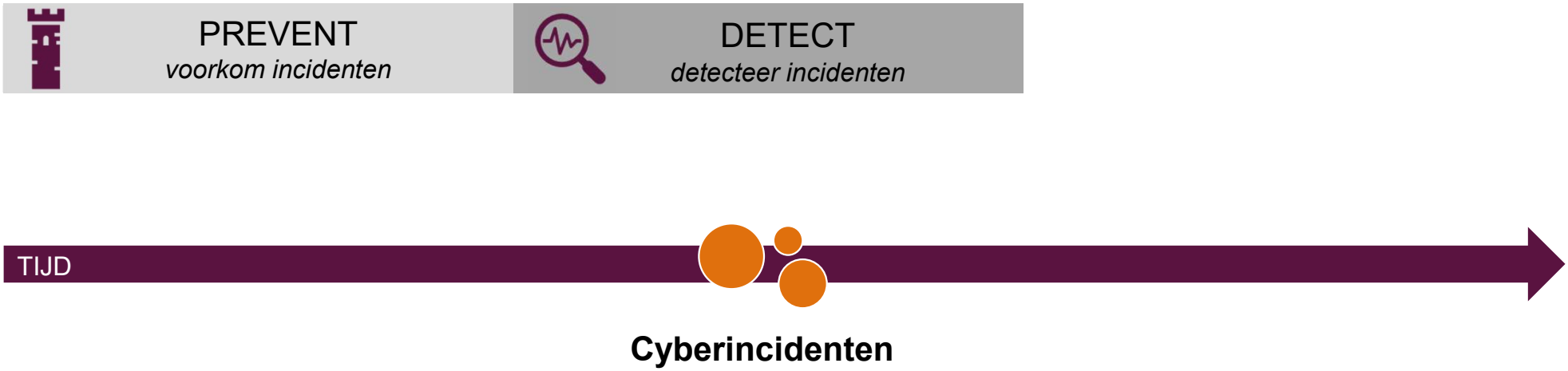
Cyberincidenten

We willen incidenten zoveel mogelijk voorkomen

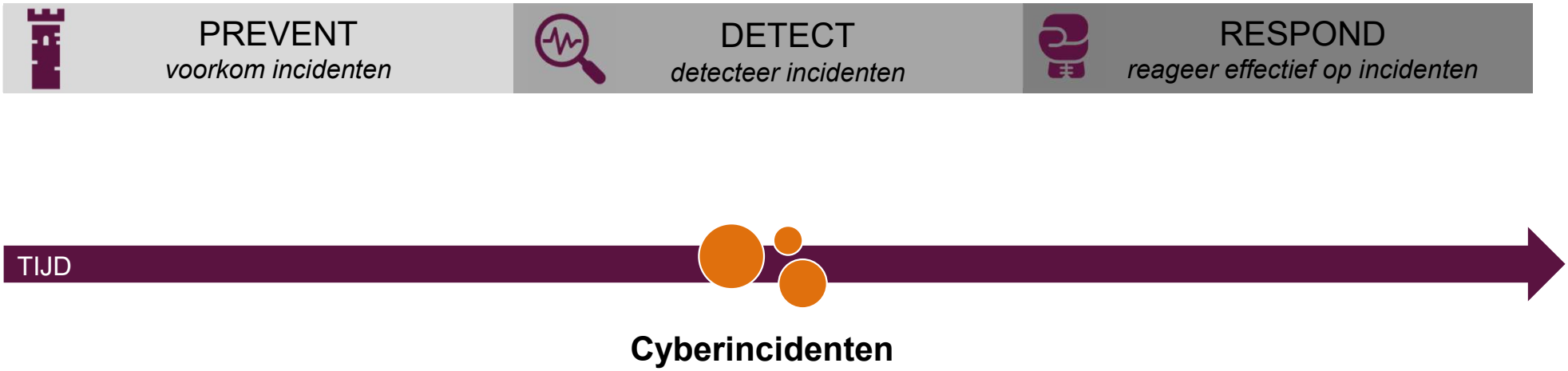
PREVENT
voorkom incidenten

Cyberincidenten

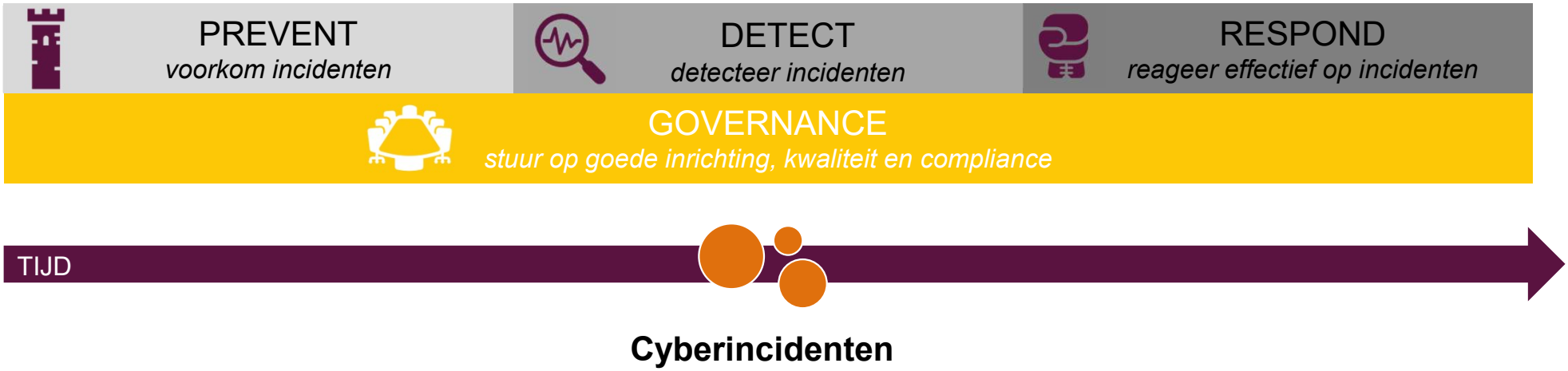
We willen incidenten zo snel mogelijk detecteren



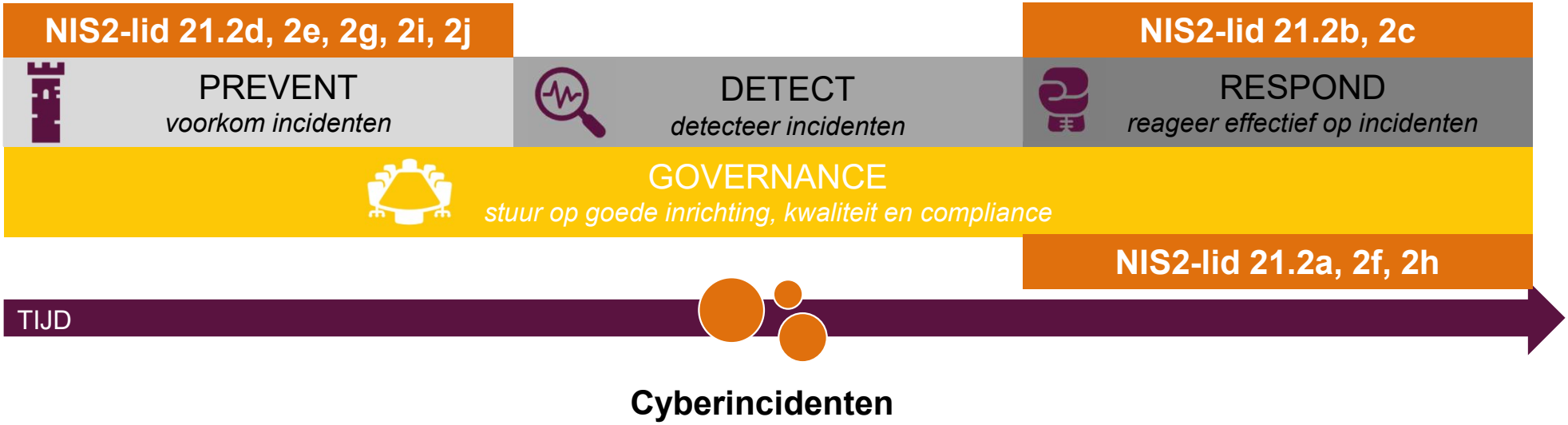
Als er (toch) incidenten zijn, willen we er effectief op reageren en de situatie herstellen



Tot slot willen we een goede governance inrichting



De Cbw maatregelen richten zich opvallend genoeg voornamelijk op PREVENT, RESPOND and GOVERNANCE



<u>Detectie</u> maakt echter een integraal onderdeel uit van de NIS2-maatregelen! De toezichthouders vinden het wel degelijk een onderdeel van de gewenste aanpak !

Cbw: Governance / bestuurder aan zet

In artikel 31 lid 4 en artikel 36 NIS2:

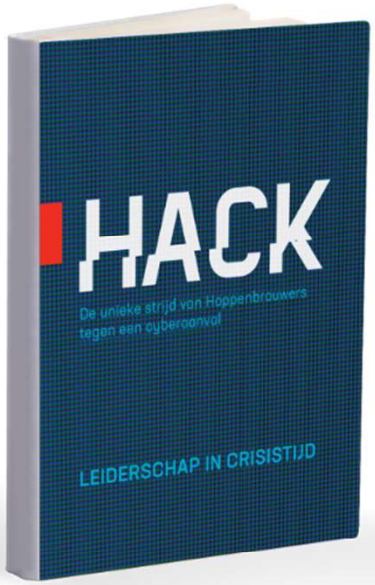
*…De lidstaten kunnen besluiten **passende**, **evenredige** en **doeltreffende toezichts- en handhavingsmaatregelen** ten aanzien van die instanties te nemen in overeenstemming met de nationale wetgevings- en institutionele kaders…*

*…De vastgestelde sancties moeten **doeltreffend**, **evenredig** en **afschrikkend** zijn…*

De consequenties, deels in uitzonderlijke situaties op te leggen, zijn uitgewerkt in de Cbw (art. 75-77):

- Handhavingsinstanties krijgen verregaande bevoegdheden tot ingrijpen
- Handhavingsinstanties krijgen verregaande bevoegdheden bij het uitblijven van maatregelen door een entiteit
  - Het opschorten van een vergunning of certificering van een essentiële entiteit
  - De algemeen directeur of wettelijke vertegenwoordiger van een essentiële entiteit tijdelijk verbieden leiding te geven
- Er kunnen boetes worden opgelegd (art. 77 Cbw) van 10 miljoen euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar

Tot slot: wees waar mogelijk transparant over incidenten en deel informatie



*"Om het groeiende probleem van ransomware de baas te kunnen worden, **is openheid over incidenten essentieel**. Veel bedrijven kiezen ervoor hierover te zwijgen, omdat ze vrezen voor reputatieschade. Of openheid reputatieschade veroorzaakt is echter nog maar de vraag. Bovendien kan openheid voor **meer bewustzijn** zorgen. Het delen van inhoudelijke informatie over incidenten draagt bovendien bij aan het **verhogen van de cyberweerbaarheid** van andere organisatie. Hopelijk bereiken we in de toekomst een situatie waarin het verzwijgen van incidenten leidt tot reputatieschade, maar zover zijn we helaas nog niet"*

Petra Oldengarm, directeur Cyberveilig Nederland in het voorwoord van Hack

Hopelijk bereiken we ooit de situatie dat een organisatie reputatieschade leidt door het verzwijgen van incidenten

Bron: https://www.cybersecurityraad.nl/binaries/Report_Scientific_Research_DBNO_20200211_DEF_tcm107-431346.pdf

CYBERVEILIG NEDERLAND

Liesbeth Holterman

liesbeth@cyberveilignederland.nl

www.cyberveilignederland.nl