

DLA ICT

CYBERBEVEILIGINGSWET (CBW)

Bent u voorbereid als het morgen misgaat?



DLA ICT

INHOUD

- 01 Introductie
- 02 De wet en uw organisatie
- 03 Wat verwacht de wet
- 04 Waar staat uw organisatie?
- 05 Toezicht & Handhaving
- 06 Morgen beginnen



INTRODUCTIE



WIE IS

DLA ICT?



WIE ZIJN WIJ?

Berend Wopereis



Sammy Pattimukaij



EVEN PEILEN:

Wie denkt dat zijn of haar organisatie voldoet aan de cyberbeveiligingswet?

Zeker wel



Twijfel



Zeker niet



WAT GEBEURT ER ALS U MORGEN WORDT GEHACKT?

ERP niet beschikbaar

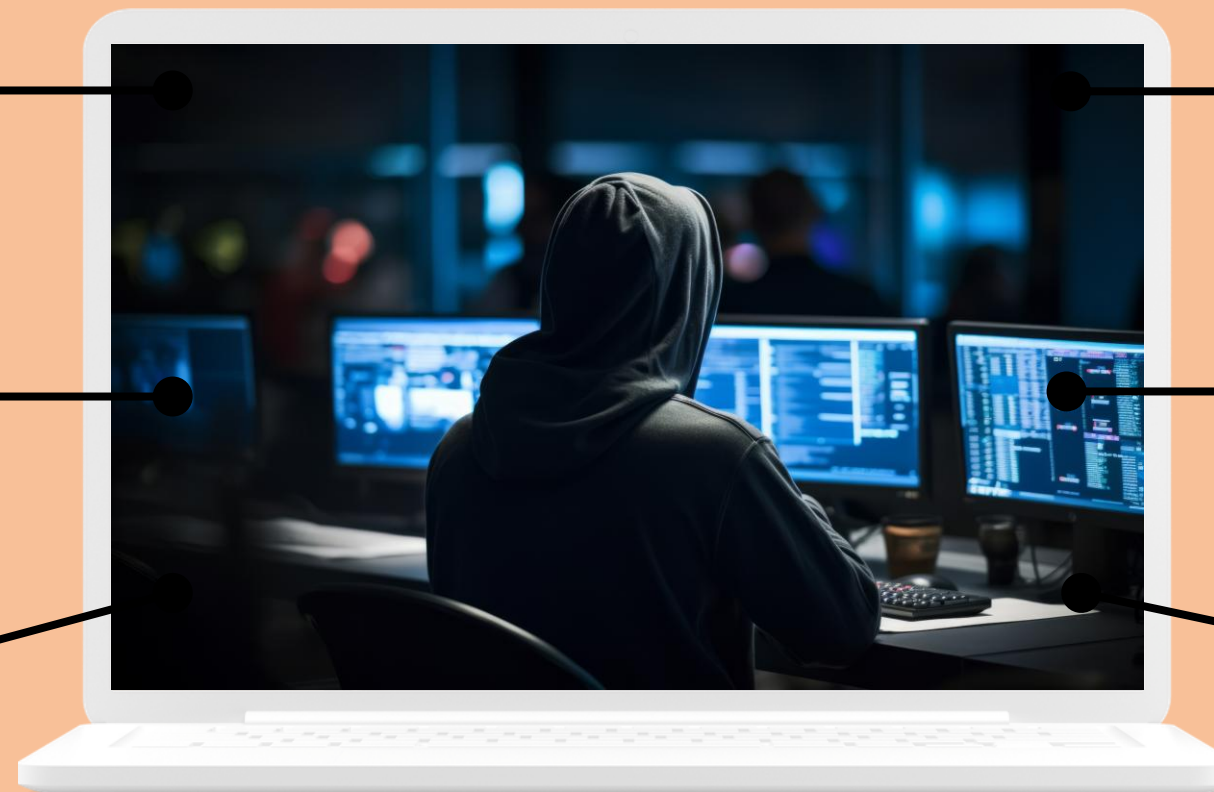
Geen communicatie

Productie stopt

Paniek en chaos

Conclusie

Meldplicht



DE WET EN UW ORGANISATIE



DE WET IN 1 MINUUT

Sinds 15 augustus 2026 van kracht

Registratie- plicht

In het entiteits-
register (NCSC)

Zorgplicht

Risicoanalyse,
incidenten-Beheer,
continuïteit en
cyberbeveiliging

Meldplicht

Eerste melding
binnen 24 uur

VALT MIJN ORGANISATIE ONDER DE WET?

1. Binnen welke sector valt uw organisatie?

Energie

Vervoer

Bankwezen

Gezondheidszorg

Drinkwater

Afvalwater

Digitale infrastructuur

Overheid

Ruimtevaart

Infrastructuur voor de financiële markt

Post- en koeriersdiensten

Afvalstoffenbeheer

Vervaardiging

Digitale aanbieders

Onderzoek

Vervaardiging, productie en distributie van chemische stoffen

Productie, verwerking en distributie van levensmiddelen



VALT MIJN ORGANISATIE ONDER DE WET?

2. Hoe groot is uw organisatie?

Essentieel

Kritieke sectoren (zoals: energie, zorg, overheid en digitale infrastructuur)

- Grote organisatie (250+ medewerkers en een jaaromzet van minimaal 50 miljoen euro)

Belangrijk

Overige sectoren (zoals: maakindustrie, afvalbeheer, logistiek of digitale diensten)

- Grote organisatie (250+ medewerkers en een jaaromzet van minimaal 50 miljoen euro)
- Middelgrote organisatie (tussen 50-250 medewerkers en een jaaromzet van maximaal 50 miljoen euro)



Organisaties zijn zelf verantwoordelijk om te toetsen of zij onder de wet vallen.

OOK INDIRECT KRIJGT U ERMEE TE MAKEN

Uw klant:
Vraagt aantoonbare
beveiliging & continuïteit



Uw leverancier:
Moet risico's in de keten
beheersen

Uw organisatie:
Legt eisen, rollen en
bewijs vast

WAT VERWAACHT

DE WET



WAT MOET U CONCREET ORGANISEREN?



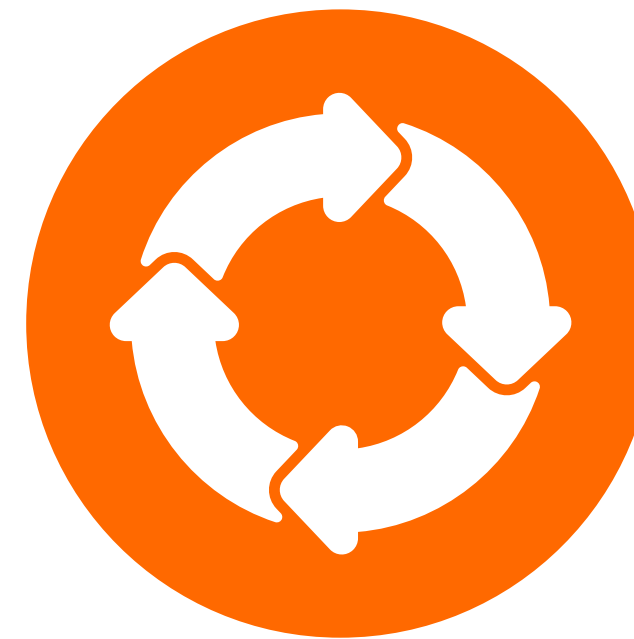
Risicoanalyse
(Wat kan er misgaan?)



Maatregelen
(Hoe verkleinen we
de kans?)



Incidentproces
(Wie doet wat bij een
incident?)



Continuïteit
(hoe blijven of
komen
we in bedrijf?)

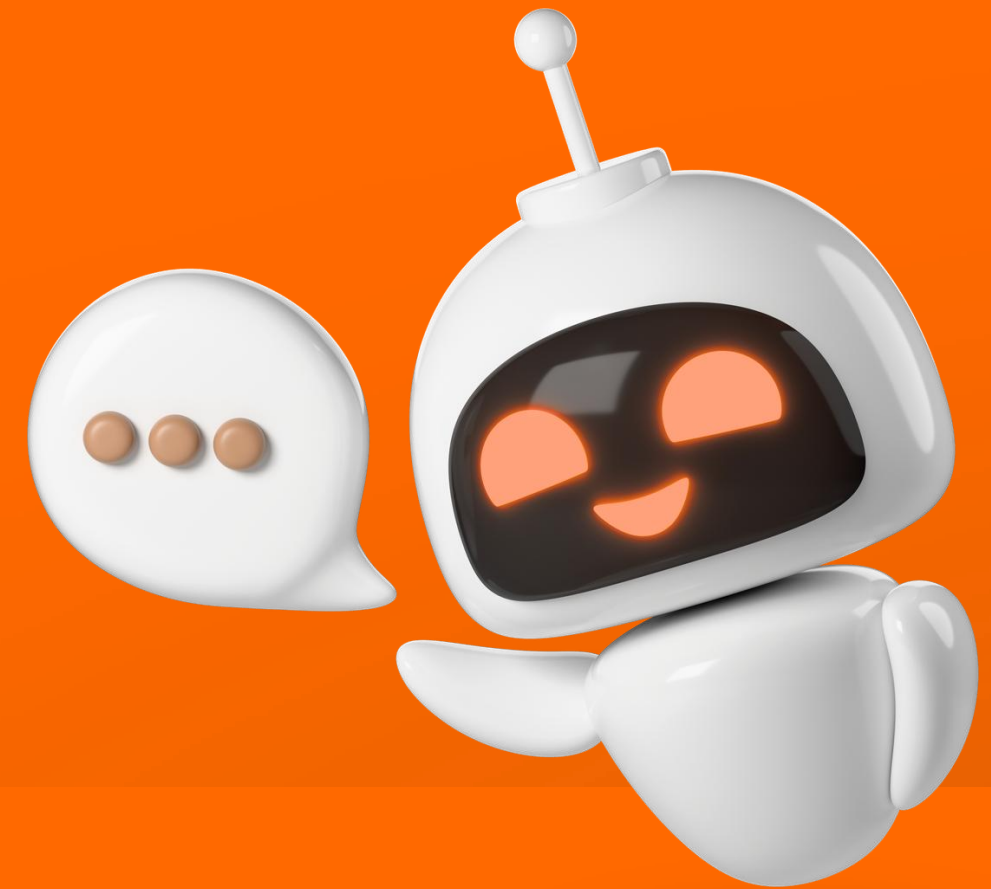


Ketenbeveiliging
(Welke afhankelijkheden
accepteren we?)

BESTUURDERS OPGELEET:

Verwachtingen van bestuursleden zijn:

1. Cyberrisico's begrijpen
2. Richting geven en besluiten nemen
3. Zorgen voor middelen en capaciteit
4. Toezicht houden op de uitvoering
5. Verantwoordelijkheid afleggen
6. Scholing volgen



BESPREKEN - BESLUITEN - TOEZICHT

WAAR STAAT UW
ORGANISATIE?



MINI-SCAN

Geef 0 of 1 punt, dmv het opsteken van vingers.

Scope Weet u zeker of uw organisatie onder de CBW valt?

0

1

Betrokkenheid bestuur Staat cybersecurity elk kwartaal op de agenda

0

1

Risicoanalyse Is er in de afgelopen 12 maanden een risicoanalyse uitgevoerd?

0

1

Incidentrespons Is er een incidentresponsplan aanwezig en getest?

0

1

Meldplicht Weet uw organisatie wie er verantwoordelijk is voor een melding van een significant cyberincident?

0

1

MINI-SCAN

Geef 0 of 1 punt, dmv het opsteken van vingers.

Continuïteit

Heeft u actuele back-up- en herstelprocessen die periodiek worden getest?

0

1

Leveranciers

Beoordeelt u leveranciers op cybersecurityrisico's en legt u hierover afspraken vast?

0

1

Awareness

Volgen medewerkers periodiek security- of phishing-training?

0

1

Aantoonbaarheid

Zijn uw beveiligingsmaatregelen aantoonbaar?

0

1

Bestuurders

Is de directive getraind in cyberrisico's?

0

1

0-4: voldoet niet 5-7: basis aanwezig 8-10: gericht verbeteren

TOEZICHT & HANDHAVING



GAAT DE OVERHEID TOEZIEN?

Toezicht:
Toezichthouders
controleren naleving



Werkelijke impact:
Stilstand, omzetverlies en
verlies van vertrouwen

Handhaving:
Niet voldoen kan leiden
tot maatregelen vanuit
de toezichthouder

MORGEN
BEGINNEN



5 ACTIES OM DIRECT MEE TE STARTEN:



Bepaal of de wet
van toepassing is



Maak kritieke processen
en afhankelijkheden
zichtbaar



Voer een
risico-
analyse uit



Leg verantwoordelijk-
heden en
incidentprocessen
vast



Test maatregelen,
herstel en
communicatie

DE KERNBODDSCHAP:

Ken uw risico's, neem passende maatregelen en wees voorbereid op incidenten.

Cybersecurity is onder de CBW een bestuurlijke verantwoordelijkheid, geen puur IT-vraagstuk.

hoe goed bent u voorbereid als het morgen gebeurt?

CYBERSECURITY EVENT

Datum: 4 november

Gastspreeker: Dave Maasland

Ben je geïnteresseerd?

Meld je aan via events@dla.nl

