# Hoe staat onze organisatie ervoor? Cybersecurity in de bestuurskamer

**Checklist voor bestuurders en toezichthouders, op basis van NIS2 en de Cyberbeveiligingswet**

Sinds 15 augustus 2026 geldt de Cyberbeveiligingswet (Cbw), de Nederlandse uitwerking van de Europese NIS2-richtlijn. De wet legt de verantwoordelijkheid nadrukkelijk bij het bestuur: het bestuur keurt de maatregelen goed, ziet toe op de uitvoering en is aanspreekbaar bij nalatigheid. Met deze checklist toets je in een paar minuten of je organisatie dat aantoonbaar op orde heeft.

| Vraag | Ja | Nee |
|---|---|---|
| **BESTUUR EN VERANTWOORDELIJKHEID** | | |
| 1. **Het bestuur heeft de cybersecuritydoelstellingen en de risicobereidheid vastgesteld.**<br>Bijvoorbeeld: beveiliging van klant- of cliëntgegevens conform marktstandaarden, in balans met de werkbaarheid. Vastgestelde doelstellingen maken keuzes over maatregelen en budget uitlegbaar. | ☐ | ☐ |
| 2. **Bestuurders hebben een passende training gevolgd.**<br>De Cbw vraagt dat bestuurders voldoende kennis hebben om cyberrisico's en de genomen maatregelen zelf te kunnen beoordelen. | ☐ | ☐ |
| 3. **De verantwoordelijkheid voor cybersecurity is belegd: de portefeuille cybersecurity ligt bij een bestuurder met affiniteit voor het onderwerp.**<br>Deze bestuurder is binnen het bestuur het aanspreekpunt voor de rest van de organisatie. Zo is duidelijk wie de voortgang bewaakt en wie het bestuur informeert, ook richting IT-leveranciers en adviseurs. | ☐ | ☐ |
| 4. **Het bestuur weet of de Cbw op de organisatie van toepassing is.**<br>Essentiële en belangrijke entiteiten registreren zich bij het NCSC. Valt je organisatie er niet onder, dan kan de wet je via klanten of de keten toch raken. De zorgplicht blijft een goede maatstaf. | ☐ | ☐ |
| **ZORGPLICHT: PASSENDE EN EVENREDIGE MAATREGELEN** | | |
| 5. **Risicobeheer: kritieke processen, systemen en gegevens zijn in kaart gebracht.**<br>De belangrijkste risico's zijn geïdentificeerd en er ligt een roadmap met mitigerende maatregelen, zodat investeringsbesluiten geïnformeerd genomen worden. | ☐ | ☐ |

| Vraag | Ja | Nee |
|---|---|---|
| **6. Beveiliging van de leveranciersketen: contracten met IT-leveranciers bevatten beveiligingsafspraken.**<br>De organisatie voert regie op haar IT-partijen en weet wie via een leverancier toegang heeft tot systemen en gegevens. | ☐ | ☐ |
| **7. Toegangsbeheer: autorisaties worden periodiek herzien en vervallen direct bij vertrek.**<br>Multifactorauthenticatie (MFA) is ingericht en er is een wachtwoordbeleid met wachtwoordmanager ingevoerd. | ☐ | ☐ |
| **8. Netwerk- en systeembeveiliging: systemen worden tijdig bijgewerkt en gegevens zijn versleuteld.**<br>Patchmanagement is integraal op orde. Prioritering voor bedrijfskritische applicaties. | ☐ | ☐ |
| **9. Business continuity wordt periodiek getest.**<br>Er is een plan om kritieke processen na een incident te hervatten, met afgesproken hersteltijden. | ☐ | ☐ |
| **10. De cybersecuritygerelateerde maatregelen zijn getoetst aan een erkende standaard.**<br>Een periodieke toets (bijvoorbeeld aan de hand van CIS, ISO 27001 of NEN 7510) maakt zichtbaar waar de organisatie staat en wat de delta is. | ☐ | ☐ |
| **GEDRAG EN CULTUUR** | | |
| **11. Bewustwording: medewerkers worden periodiek getraind en hebben een geheimhoudingsverklaring getekend.**<br>Er is een meldcultuur waarin een verdachte klik of een incident zonder schaamte en direct gemeld wordt. | ☐ | ☐ |
| **12. Het bestuur geeft zelf het goede voorbeeld en volgt dezelfde regels als iedereen.**<br>Geen uitzonderingen voor de top bij MFA, wachtwoorden of het delen van bestanden. Bestuurders zijn een geliefd doelwit, bijvoorbeeld bij CEO-fraude. Wat het bestuur zelf doet, bepaalt wat medewerkers normaal vinden. | ☐ | ☐ |
| **13. Medewerkers worden gesteund als ze een verzoek eerst controleren, ook als het van een leidinggevende lijkt te komen.**<br>Een onverwacht betaalverzoek of een vraag om gegevens altijd via een tweede kanaal checken, zoals terugbellen op een bekend nummer, is de norm. Wie even vertraagt om te controleren, krijgt daar geen gedoe over. | ☐ | ☐ |
| **14. Het bestuur bespreekt incidenten en bijna-incidenten open, zonder schuldvraag, en stuurt op wat de organisatie ervan leert.**<br>De vraag is niet "wie heeft dit gedaan?" maar "hoe voorkomen we dit de volgende keer?". Zo worden problemen eerder gemeld en worden dezelfde fouten niet herhaald. | ☐ | ☐ |

| Vraag | Ja | Nee |
|---|---|---|
| **CRISISBEHEER EN MELDPLICHT** | | |
| **15. Er is een crisisresponsplan, en het is duidelijk wie wat wanneer meldt bij wie.**<br>Bij een significant incident (Cbw): een vroegtijdige waarschuwing binnen 24 uur en een melding binnen 72 uur aan het CSIRT en de bevoegde autoriteit. Bij een datalek met persoonsgegevens: binnen 72 uur aan de Autoriteit Persoonsgegevens (AVG). | ☐ | ☐ |
| **16. Het crisisresponsplan is geoefend, ook met het bestuur.**<br>In een crisis is er geen tijd om rollen en mandaten uit te zoeken. Een oefening laat zien of het plan in de praktijk werkt. | ☐ | ☐ |

**MEER JA KUNNEN ANTWOORDEN?**

Wil je op meer punten ja kunnen antwoorden, of een onafhankelijke toets op de antwoorden van je organisatie? NoordPunt biedt een second opinion tussen CISO en bestuur, training NIS2 en Cbw voor bestuurders en een vaste sparring partner, ook in een crisis. Neem geheel vrijblijvend contact met ons op.

**janot@noordpunt.nl · lotta@noordpunt.nl · noordpunt.nl**

Bronnen: Cyberbeveiligingswet (in werking sinds 15 augustus 2026), NIS2-richtlijn (EU) 2022/2555, AVG art. 33. Deze checklist is een hulpmiddel en geen juridisch advies; stand november 2026.