Ministerie van Justitie en Veiligheid

Minister van Justitie en Veiligheid

Ministerie van Justitie en Veiligheid
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
12 juni 2024

Ons kenmerk
5526814

nota

Samenhangend Inspectiebeeld cybersecurity vitale processen

1. Aanleiding

Met als doel gezamenlijke inzichten te bundelen en uitwisseling van kennis en expertise te faciliteren is afgesproken dat de Rijksinspectie Digitale Infrastructuur samen met andere rijksinspecties en toezichthouders zorg draagt voor een Samenhangend Inspectiebeeld cybersecurity vitale processen. Dit onder regie van de minister van Justitie en Veiligheid.

De toezichthouders op de Wet beveiliging netwerk- en informatiesystemen (Wbni) samenwerken, te weten: Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS), Autoriteit Persoonsgegevens (AP), De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd (IGJ), Inspectie Leefomgeving en Transport (ILT) Inspectie Justitie en Veiligheid (IJenV) en Rijksinspectie Digitale Infrastructuur (RDI) hebben gezamenlijk het Samenhangend Inspectiebeeld cybersecurity vitale processen 2024 opgesteld.

2. Geadviseerd besluit

- U wordt gevraagd akkoord te gaan met bijgaande Kamerbrief en deze met het inspectiebeeld op 14 juni te verzenden aan de Tweede Kamer.
- U wordt gevraagd akkoord te gaan met bijgaande brieven aan uw collega bewindspersonen waarvan de toezichthouders hebben meegewerkt aan het Inspectiebeeld

De uitkomsten van het samenhangend inspectiebeeld worden betrokken bij de Voortgangsrapportage op de Nederlandse Cybersecuritystrategie die aan de Kamer is toegezegd voor het najaar van 2024. In deze voortgangsrapportage wordt de Kamer geïnformeerd over de voortgang en eventuele bijstelling van de Nederlandse Cybersecuritystrategie.

3. Kernpunten

De focus van de toezichthouders lag in 2023 op het meerjarige thema risicomanagement. Ze merken op dat de vitale aanbieders steeds meer aandacht hebben voor de certificering van het information security management system (ISMS) en onderschrijven het belang hiervan. De toezichthouders hechten daarnaast veel betekenis aan het aansluiten van het ISMS op het Enterprise Risk Management (ERM) van de organisatie. Een ISMS bekijkt de risico's rondom informatiebeveiliging. ERM kijkt organisatie breed naar risico's. Het expliciet

vastleggen van de risicobereidheid is essentieel bij het implementeren van zowel een ERM als een ISMS en is in enkele sectoren dan ook verplicht gesteld door de toezichthouders.

Verder vinden de toezichthouders het belangrijk dat organisaties een governancestructuur hebben. De toezichthouders zien ruimte voor verbetering op het gebied van risicomanagement op bestuursniveau. De belangrijkste verbeterpunten zijn:

- Vanuit een risico-oogpunt actuele ontwikkelingen, zoals artificiële intelligentie en quantumcomputers, volgen.
- De aansluiting tussen het ERM-systeem en het ISMS waarborgen.
- De effectiviteit van het ERM-systeem en de ISMS onafhankelijk laten beoordelen.

Het toezicht op cybersecurity wordt de komende periode aanzienlijk uitgebreid door de komst van de Critical Entities Resilience-richtlijn (CER) en de Network and Information Security-richtlijn (NIS2). Om de governance rondom samenwerking te verstreken is daarom recentelijk het 'directeurenoverleg toezicht digitale weerbaarheid' opgericht. Dit gremium fungeert als opdrachtgever van de werkgroep 'samenwerkend toezicht digitale toezichthouders'. Hiermee beogen de toezichthouders dat het toezicht effectief en efficiënt ingericht wordt, en de gezamenlijke toezichtlast voor organisaties zo laag mogelijk blijft. Aan het meerjarige thema risicomanagement wordt voor het volgende inspectiejaar 2024 het thema assetmanagement toegevoegd.

4. Toelichting

4.1 Politieke context

Het inspectiebeeld biedt inzicht in de stand van de resultaten van toezicht op cybersecurity bij vitale processen en wordt jaarlijks opgesteld. Daarnaast biedt het de gelegenheid om - indien nodig - passende maatregelen te nemen. De uitkomsten van dit rapport komen terecht in de Voortgangsrapportage op de Nederlandse Cybersecuritystrategie die al aan Kamer is toegezegd voor het najaar van 2024.

4.2 Communicatie

De Rijksinspectie Digitale Infrastructuur (RDI) zal namens alle genoemde toezichthouders ook het Inspectiebeeld online publiceren. Hierover is afstemming tussen communicatie van JenV en RDI.

5. Informatie die niet openbaar gemaakt kan worden

5.1 Toelichting

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.