

Onderzoek Cybersecurity

Rekenkamer WSHD · VV commissie MBH · 11 november 2026

Waar gaat dit onderzoek over?

CENTRALE VRAAG

Hoe beheerst WSHD de cybersecurityrisico's van de assets — gemalen, sluizen, rwzi's — en hoe worden die risico's inzichtelijk gemaakt voor de VV?

Afbakening

Procesautomatisering van de assets; niet de kantoor-ICT. Verkennend; geen technische audit.

Aanpak

Documentstudie, technische vragen, interviews binnen en buiten WSHD, enquête onder VV-leden.

Normen

Waterschapswet, BIO2, NIS2; de Cyberbeveiligingswet als voorbereidingsnorm. Mei 2025 – februari 2026.

De organisatie zet aantoonbaar stappen

Risico’s in beeld

- Cybersecurityteam gestart in 2024.
- Gezamenlijke werkwijze met Het Waterschapshuis.
- Sinds eind 2025 risico’s per asset in kaart; nulmeting volgt in 2026.

Monitoring

- Realtime technische monitoring via de waterschapsbrede regiekamer.
- SIEM signaleert ongeoorloofde toegangspogingen.
- Buitendienst is getraind en geïnstrueerd.

Opgave: borgen

- CISO herpositioneerd naar de concernstaf.
- D&H heeft de NIS2-opleiding gevolgd.
- De vraag is nu wat in 2026 en verder nodig is om het bereikte te borgen.

Sturing en controle blijven achter

1 Opvolging audits

GEEN ACTUEEL OVERZICHT

Niet alle auditrapporten bereiken D&H. De CISO/FG-jaarrapportage 2024 werd pas na acht maanden besproken. Welke actiepunten openstaan, is niet zichtbaar.

2 Informatie aan de VV

ONREGELMATIG

De VV hoort vooral over de veiligheidsladder en het volwassenheidsniveau. Beleid en CISO/FG-rapportages komen niet bij de VV.

3 Rol van de VV

NIET BENUT

Eén VV-besluit (2022). Geen vragen of moties. Vier aanmeldingen voor een presentatie. Wel een duidelijke wens tot meer betrokkenheid.

De wet geldt nu, de VV hoort erbij

CYBERBEVEILIGINGSWET

Sinds augustus 2026 van kracht

De eindverantwoordelijkheid ligt bij het dagelijks bestuur. Toezicht moet aantoonbaar en gedocumenteerd zijn. De rolverdeling tussen VV, D&H en organisatie moet belegd zijn.

VERTROUWELIJKHEID

Gevoeligheid erkend

Cybersecurity is een gevoelig onderwerp; niet alles kan openbaar. De Rekenkamer erkent dat. D&H betrekt het dilemma van openbaarheid en weerbaarheid bij de nieuwe governance.

Wat dit betekent voor de VV De VV stelt kaders en controleert; D&H stelt het beleid vast en legt verantwoording af. Vertrouwelijkheid vraagt een passende vorm van informeren; niet het ontbreken ervan.

Drie aanbevelingen aan de VV

1 Rol van de VV

BESTUURLIJK GESPREK

Geef D&H de opdracht een bestuurlijk gesprek voor te bereiden over de rol van de VV bij cybersecurity.

Doel: helderheid over de governance en afspraken over hoe en hoe vaak de VV wordt geïnformeerd.

2 Opvolging audits

MONITORINGSPROGRAMMA

Geef D&H de opdracht een monitoringsprogramma op te zetten voor actueel zicht op de opvolging van (externe) audits.

Licht van opzet: een doorlopend overzicht van open actiepunten, periodiek besproken in D&H.

3 Beleidskader

VOORLEGGEN AAN DE VV

Geef D&H de opdracht het beleidskader informatieveiligheid aan de VV voor te leggen, met de rol van elk orgaan.

Nu ontbreekt de VV als actor in het beleid en in het governanceplan.