

Dialogtafel Digitale Weerbaarheid

3 september 2026

Twintig deelnemers van tien cbo's en andere stakeholders gingen in vier groepen met elkaar in gesprek over digitale weerbaarheid. De middag stond in het teken van kennisdeling, onderlinge uitwisseling en het vertalen van aandachtspunten naar concrete handelingsperspectieven.

Aanleiding en opzet

Het CvTA faciliteerde samen met Software Improvement Group (SIG), Wouter Knigge en Jasper Kuijpers de in het Jaarplan 2026 aangekondigde Dialogtafel Digitale Weerbaarheid voor de sector collectief beheer. Het CvTA heeft deze Dialogtafel ICT georganiseerd vanuit het publiek belang en om zo doende bij te dragen aan vertrouwen in het collectief beheer. Het doel van de dialogtafel ICT was bijdragen aan de verdere bewustwording van het belang van digitale weerbaarheid bij cbo's

Centraal stond de vraag hoe cbo's hun weerbaarheid kunnen versterken in een snel veranderende technologische omgeving.

Aan de bijeenkomst nam een gevarieerde groep van cbo's deel met vertegenwoordigers uit diverse lagen van de organisaties van Sena, BumaStemra, FAIR, Norma, Pictoright, IPRO, Service Bureau Filmrechten (Sekam, Sekam Video, StOPnl en FAIR), STAP en Videma. Ook VOI@E was aanwezig. De deelnemers, onder wie vertegenwoordigers van het CvTA, werkten in vier tafelgroepen aan vragen en praktische aandachtspunten. Deze samenstelling zorgde voor een energieke en geslaagde middag.

Wat wilden de deelnemers uit de middag halen?

Aan het begin van de sessie is gevraagd wat deelnemers uit de dialogtafel wilden meenemen. Drie behoeften kwamen het vaakst terug:

- Een concrete to-do-lijst: wat moet een organisatie nu daadwerkelijk oppakken?
- Meer grip op de omgang met externe partijen, waaronder leveranciers, partners en andere initiatieven.
- Inzicht in de effecten van nieuwe ontwikkelingen, zoals AI, op de eigen organisatie.

Overkoepelend bleek dat deelnemers veel waarde hechten aan het leren van elkaars ervaringen.

Kennisuitwisseling en onderling contact werden minstens zo belangrijk gevonden als concrete instrumenten.

Vier pijlers van digitale weerbaarheid

In het eerste inhoudelijke blok is digitale weerbaarheid verkend aan de hand van vier pijlers. De selectie kwam voort uit voorbereidende interviews met deelnemende cbo's en is gekoppeld aan de BIO-2 (Baseline Informatiebeveiliging Overheid) als raamwerk.

Pijler	Waar gaat het over?
1. Beheersbaarheid van systemen	Weten wie waarvoor verantwoordelijk is voor de IT, intern en extern, en dit structureel bewaken.
2. Continuïteit en redundantie	Zorgen dat de organisatie kan blijven functioneren en snel kan herstellen bij verstoringen.
3. Digitale soevereiniteit	Bewuste keuzes maken over waar data staat, bij wie en onder welke voorwaarden.
4. Privacy en gegevensbeveiliging	Grip houden op datastromen, het gebruik van gegevens en de bescherming daarvan, ook richting de toekomst.

Heatmap: waar staan de cbo's?

Vervolgens brachten de deelnemers met heatmaps in beeld waar hun organisaties op de vier pijlers staan. Daarbij ontstond ook zicht op verschillen tussen grotere en kleinere cbo's. De bespreking leverde per pijler het volgende beeld op.

Beheersbaarheid van systemen

ICT-verantwoordelijkheden zijn intern en extern doorgaans bekend en belegd. Periodieke monitoring van het werk van leveranciers blijft een uitdaging, vooral voor kleinere cbo's.

Continuïteit en redundantie

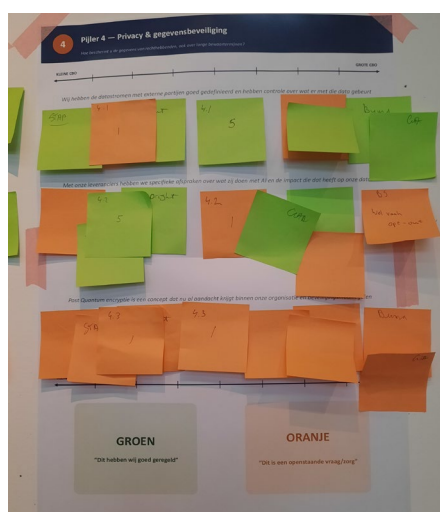
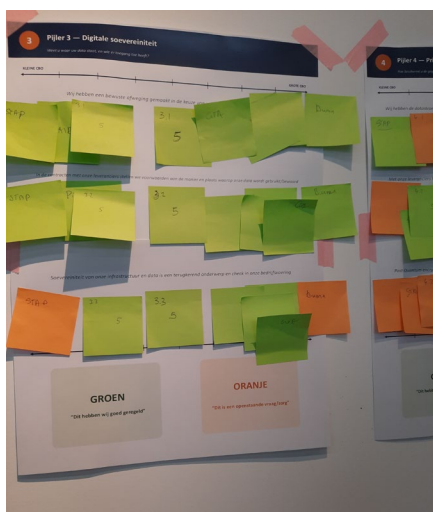
Het reguliere werk staat veelal niet ter discussie. Een gestructureerd plan om bij verstoringen snel tot verkenning en oplossing te komen, vraagt nog aandacht, met name bij kleinere cbo's.

Digitale soevereiniteit

Op dit onderwerp zijn relatief weinig zorgen. Er wordt bewust omgegaan met data en veiligheid. Tegelijk maken de kosten en de beschikbaarheid van alternatieven het lastig om daadwerkelijk andere keuzes te maken.

Privacy en gegevensbeveiliging

Deze pijler kent de meeste aandachtspunten. Het gaat om datastromen met externe partijen, afspraken over het gebruik van AI in interne processen en door externe partijen, en het vooruitkijken naar toekomstbestendige veiligheid.



Van inzichten naar concrete stappen

In het derde blok stelden de deelnemers gezamenlijk het Manifesto Digitale Weerbaarheid op. Het Manifesto is bedoeld als startpunt voor cbo's die hun digitale weerbaarheid willen versterken. Het volledige document is hieronder opgenomen (gemaakt door de Software Improvement Group).

MANIFESTO DIGITALE WEERBAARHEID

Startpunt CBO's aangaande digitale weerbaarheid

Tijdens de workshop 'Digitale Weerbaarheid' op 3 September 2026, hebben CBO's per pijler bepaald wat de eerste, concrete stappen zijn om digitale weerbaarheid onder controle te krijgen. Dit Manifesto vertaalt die uitkomsten naar vier pijlers met daarbinnen de belangrijkste aanbevelingen: het laaghangend fruit waarmee een (startende) CBO direct aan de slag kan.

1 Beheersbaarheid van systemen

Grip op welke systemen, data en afhankelijkheden er binnen en rond de CBO bestaan.

- **Inventarisatie ICT-landschap.** Leg vroegtijdig vast welke applicaties van belang zijn, welke data hierin staat, en wie voor deze elementen verantwoordelijk is.
- **Afhankelijkheden aangeven.** Houd een overzicht bij van afhankelijkheden van data, systemen en leveranciers; werk dit periodiek bij.
- **Ketens duiden.** Definieer de ketens (stromen) van data en partijen waar de CBO deel van is, met eigen rol en verantwoordelijkheid.
- **Risicoduiding.** Breng risico's in kaart in een jaarlijkse matrix; begin met veiligheid, financieel en continuïteit als belangrijkste categorieën.

2 Continuïteit en redundantie

Bedrijfsvoering en herstel waarborgen bij verstoringen of calamiteiten.

- **Crisismanagementplan.** Schrijf een plan uit voor de mogelijke crisis scenario's voor CBO's en oefen dit om praktische haalbaarheid te borgen.
- **Werkprocesdocumentatie.** Documenteer werkprocessen goed en zorg voor back-upverantwoordelijken.
- **Databeveiliging en -beschikbaarheid.** Bepaal expliciet hoe data beveiligd is, de beschikbaarheid bij calamiteiten en wie er toegang heeft.
- **Leveranciersbeoordeling.** Stel een gezamenlijke CBO richtlijn op voor evaluatie van leveranciers en verwachtingen in crisissituaties.

3 Digitale soevereiniteit

Grip houden op waar data staat, wie daarover beslist en hoe je dat communiceert.

- **Inventarisatie.** Maak inzichtelijk waar data staat en deel in op basis van gevoeligheid (privacy) en belangrijkheid (gelden).
- **Onderwerp van gesprek.** Agendeer IT/weerbaarheid in de jaarvergadering; bepaal transparantie en inspraak richting belanghebbenden.
- **Noodplannen.** Bepaal of noodplannen nodig zijn bij (toekomstige) richtlijnen over geografische dataverwerking.
- **Expliciete afweging.** Wees expliciet over de balans tussen goed databeheer en kosten; geef het bestuur een manier om hier een afweging te maken.

4 Privacy & gegevensbeveiliging

Persoonsgegevens beschermen gedurende het hele proces van verzameling tot verwerking.

- **Mapping data.** Breng in kaart waar privacygevoelige gegevens in het proces zitten en waar ze worden opgeslagen/verwerkt.
- **Autorisatie.** Houd bij wie toegang heeft tot gevoelige data en welke acties toegestaan zijn voor deze persoon.
- **Externe uitwisseling.** Stel regels op voor data-uitwisseling voor jezelf en ga in gesprek met partijen over uitwisselingsstandaarden.
- **Scholing medewerkers.** Zorg voor periodieke scholing en blijvende aandacht voor privacy/beveiliging in interne communicatie. Test deze scholing ook in de praktijk.

Terugblik

De dialoogtafel bracht organisaties met verschillende ervaringen en vraagstukken bij elkaar. De interactieve werkwijze maakte het mogelijk om kennis te delen, aandachtspunten gezamenlijk te onderzoeken en deze te vertalen naar praktische vervolgstappen. Deelnemers gingen naar huis met prioriteiten voor de eigen organisatie en met nieuwe contacten voor verdere onderlinge uitwisseling.

Het CvTA kijkt terug op een geslaagde middag en dankt de cbo's voor de actie bijdragen en Wouter en Jasper van de Software Improvement Group voor het mooie programma en de hartelijke samenwerking.