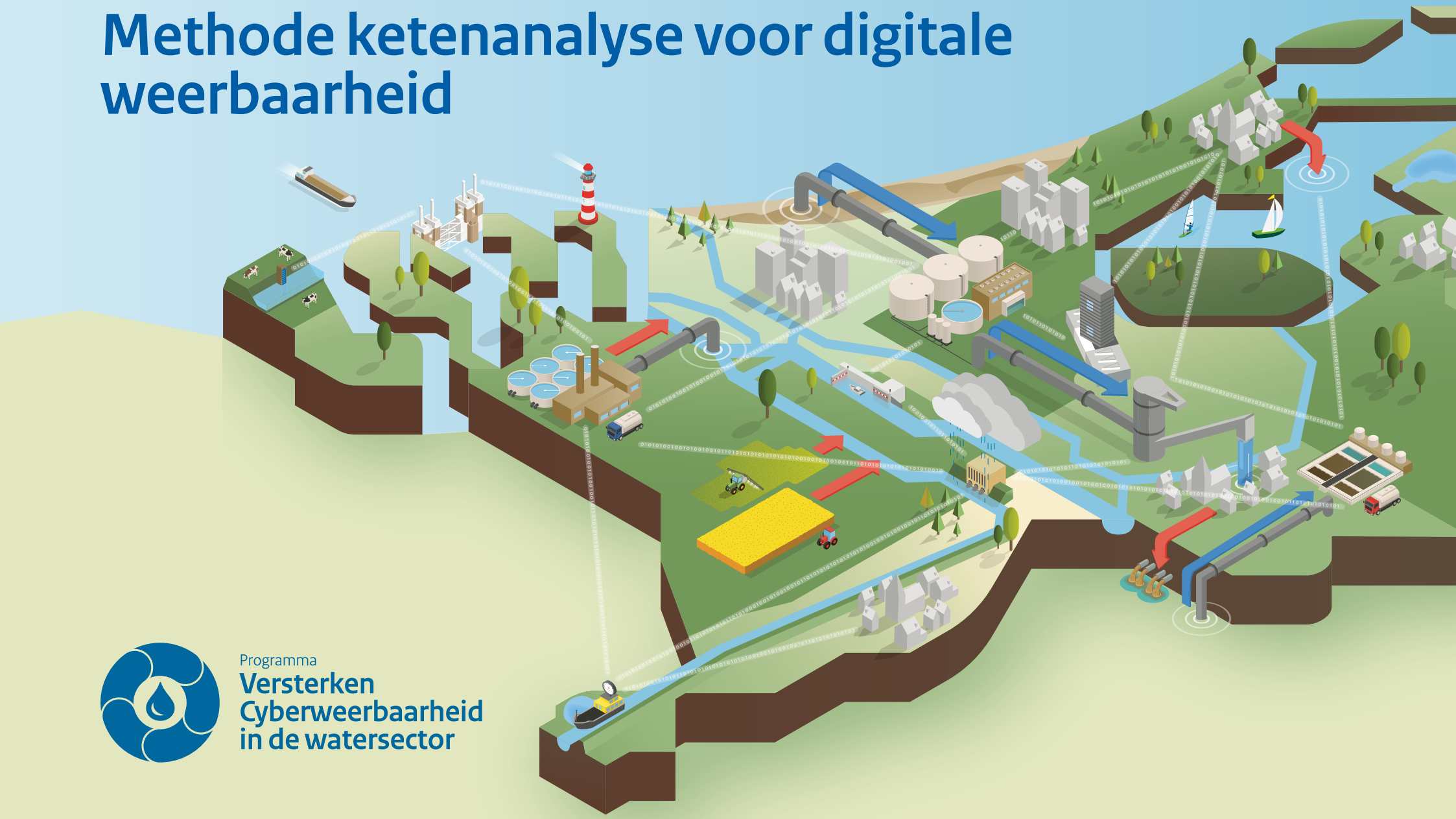
Ministerie van Infrastructuur
en Waterstaat

Samen werken aan sterkere ketens

Methode ketenanalyse voor digitale weerbaarheid



Programma
Versterken Cyberweerbaarheid in de watersector

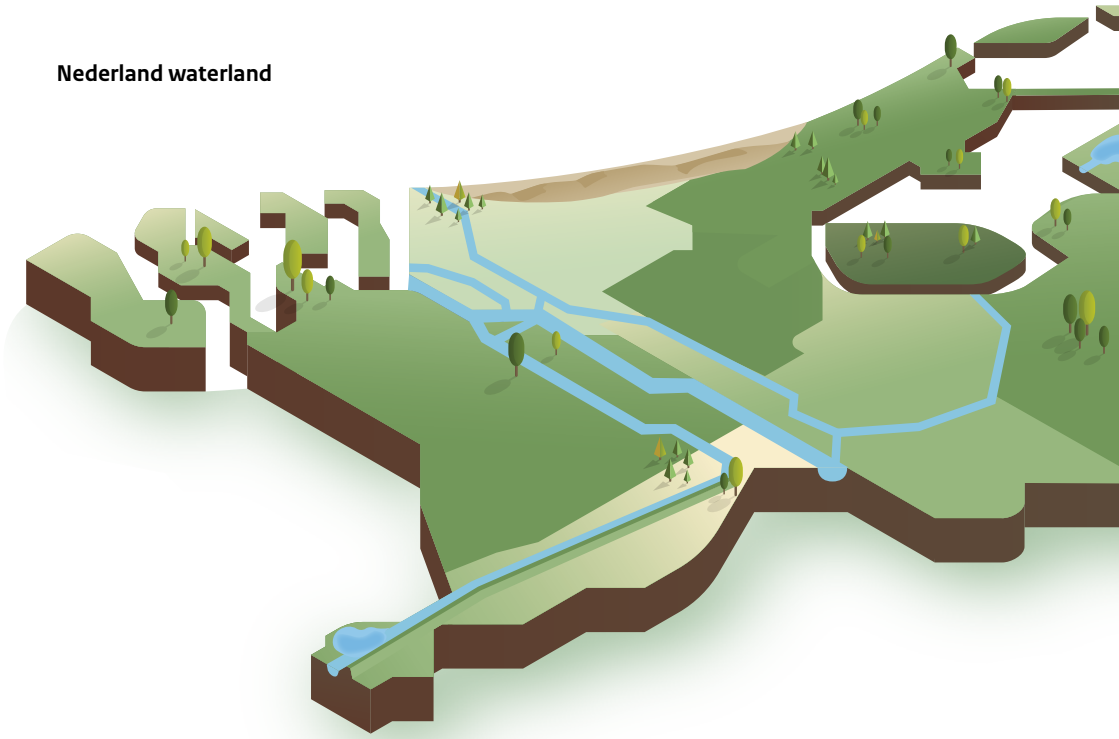
Het belang – Verhogen van de weerbaarheid tegen cyberrisico's

Voor vitale sectoren als de watersector is het belangrijk om inzicht te hebben in risico's die zich in de hele procesketen kunnen voordoen. De watersector heeft veel ervaring met het identificeren van fysieke risico's, zoals overstromingsrisico's of vervuiling van het drinkwater. Dit gebeurt op organisatieniveau, maar ook binnen ketenprocessen van organisaties die samen verantwoordelijk zijn voor vitale voorzieningen. Omdat kwetsbaarheden en dreigingen steeds vaker digitaal van aard zijn is het van belang om binnen de keten ook samen te werken rond cyberrisico's. Zo werken Rijkswaterstaat, waterschappen, drinkwaterbedrijven, gemeenten en provincies nauw samen om het beheer van oppervlaktewater en de drinkwatervoorziening in stand te houden.

Kwetsbaarheden en dreigingen zijn echter steeds vaker niet fysiek, maar digitaal van aard. Cyberaanvallen op processen en systemen voor bijvoorbeeld de drinkwatervoorziening, de riolering en het keren en beheren van oppervlaktewater, kunnen grote maatschappelijke en economische impact hebben. Partijen in de watersector en het ministerie van Infrastructuur en Waterstaat hebben daarom de handen ineengeslagen om de digitale weerbaarheid te versterken. Binnen het programma Versterken Cyberweerbaarheid in de Watersector pakken we samen digitale ketenrisico's aan. Dit doen we onder andere door het gezamenlijk uitvoeren van ketenanalyses.

Ketenanalyses kunnen ook voor vitale procesketens buiten de watersector van grote toegevoegde waarde zijn. Bijvoorbeeld voor het vervoer over het hoofdwegennet of de elektriciteitsvoorziening. Ook organisaties die betrokken zijn bij dergelijke procesketens kunnen daarom de methode uit deze brochure gebruiken.

Nederland waterland



De methode – Stapsgewijs naar inzicht in ketenrisico's en cyberweerbaarheid

Stap 1: scope keten — **Stap 2:** beschrijven keten — **Stap 3:** cyberdreigingen en impact — **Stap 4:** risico's keten

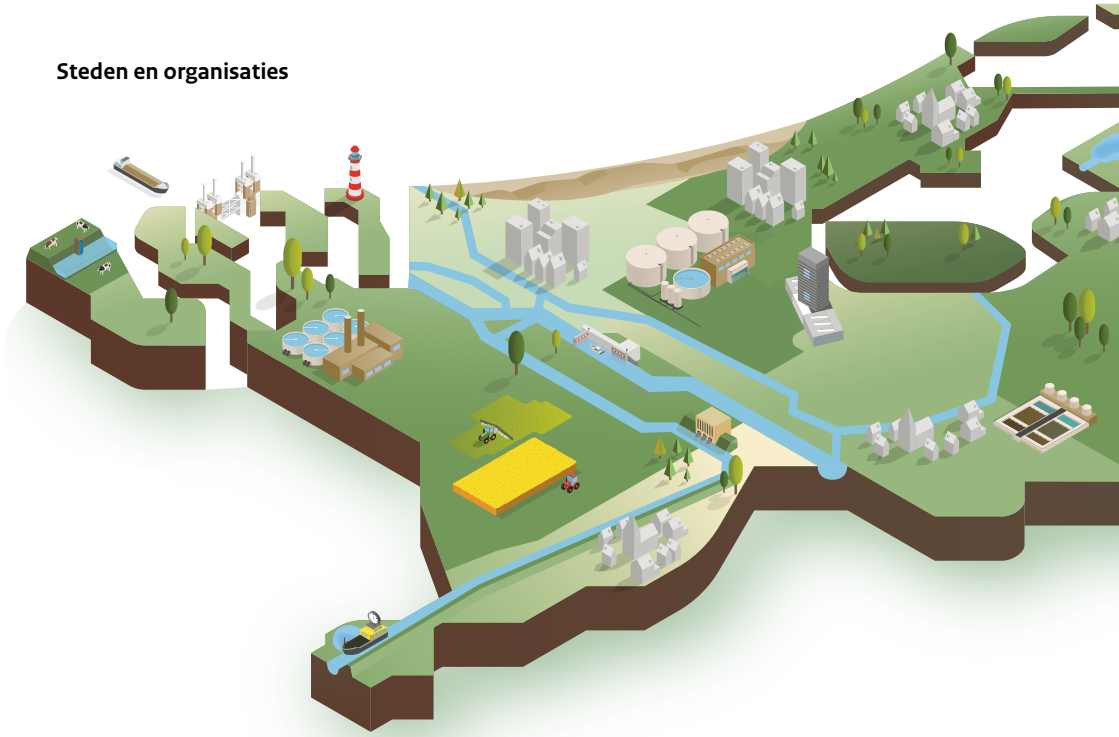
De cyberweerbaarheid van een keten in de watersector is even sterk als zijn zwakste schakel. Vanwege de grote onderlinge verwevenheid en afhankelijkheid, hebben (cyber)incidenten bij één organisatie al snel gevolgen voor andere organisaties. In het ergste geval komt een vitaal proces in het geding. Met een ketenanalyse kunnen partijen in de watersector de risico's en weerbaarheid van de afzonderlijke schakels én van de keten als geheel in kaart brengen. Op basis hiervan kunnen ze maatregelen nemen om risico's te verminderen en de cyberweerbaarheid te versterken.

Binnen een ketenanalyse gaan deelnemers van verschillende organisaties onder professionele begeleiding aan de slag. Samen analyseren ze de keten waarvan ze deel uitmaken, de organisaties die hierin samenwerken en de systemen die ze gebruiken. Deelnemers krijgen door de ketenanalyse meer inzicht in de informatiestromen, systemen en componenten, onderlinge afhankelijkheden en de te stellen proces- en systeemeisen. Deze kennis is niet alleen essentieel om te bepalen waar eventuele risico's van een cyberaanval liggen. Ze stelt deelnemers ook in staat om betekenisvol te communiceren over veiligheid en beveiliging en elkaar hierin te ondersteunen.

De ketenanalyse bestaat maximaal uit zes workshops: een voorbereidende, een afrondende en hiertussen vier bijeenkomsten waarin telkens één stap in de methodiek centraal staat. Per stap neemt het detail en daarmee ook de diepgang van de ketenanalyse toe. Op de volgende pagina lichten we deze stappen nader toe.

De deelnemers aan de ketenanalyse bakenen eerst de keten af en beschrijven die. Bijvoorbeeld de aanvoer van schoon oppervlaktewater voor de drinkwatervoorziening of de afvoer van overtollig regenwater. Aan de hand van deze scope bekijken ze welke aanvullende expertise ze moeten inschakelen bij de ketenorganisaties.

Steden en organisaties



De methode – Stapsgewijs naar inzicht in ketenrisico's en cyberweerbaarheid

Stap 1: scope keten — **Stap 2:** beschrijven keten — **Stap 3:** cyberdreigingen en impact — **Stap 4:** risico's keten

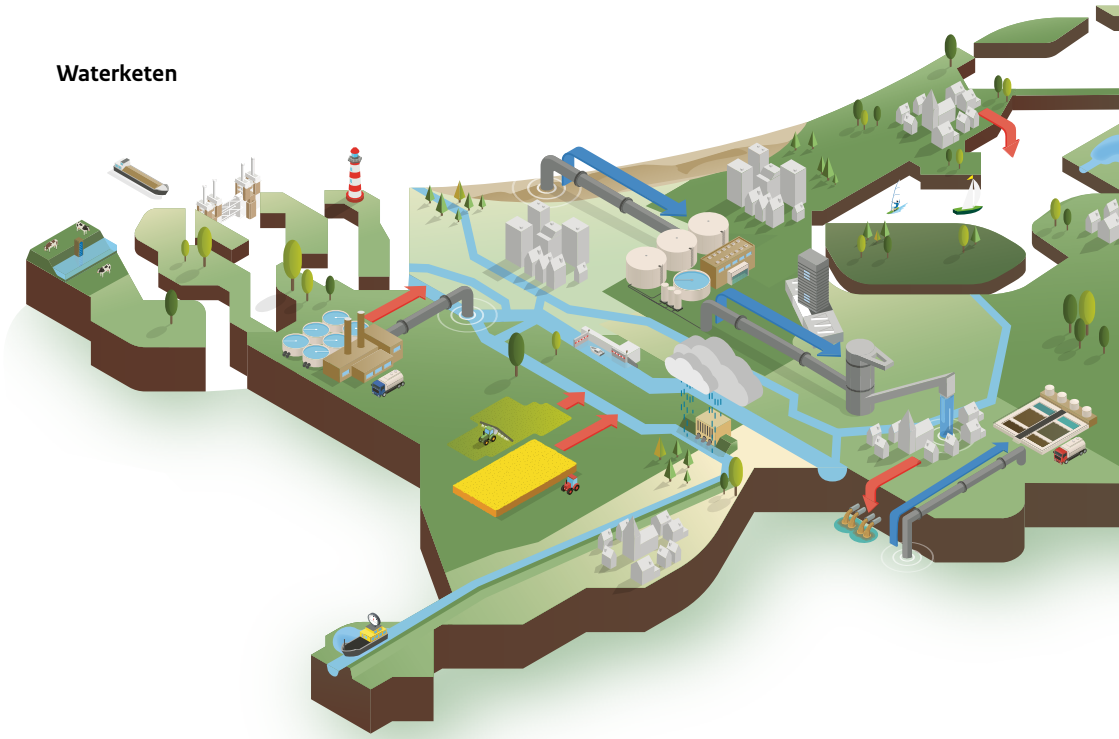
Vervolgens kijken de deelnemers in meer detail naar de naar de gebruikte ICT systemen en de ondelinge informatiestromen die hiervoor nodig zijn. Ze brengen de informatiestromen in kaart en identificeren mogelijke cyberscenario's die de systemen en de informatiestromen kunnen verstoren. Ook bepalen ze in welke mate de verschillende organisaties kwetsbaar zijn voor die scenario's.

Cyberrisico's verschillen in waarschijnlijkheid en impact. Daarom is het belangrijk om verschillende scenario's te doorlopen. Raken meetinstrumenten verstoord door een ransomware-aanval?

Dan zorgt dit ervoor dat informatie over de kwaliteit en kwantiteit van water tijdelijk niet beschikbaar is. Betrokken organisaties zullen deze verstoring snel opmerken. Daardoor kunnen ze maatregelen nemen om de gevolgen te mitigeren. Maar als een hacker erin slaagt om de data te manipuleren, dan zullen de betrokken organisaties dit vaak niet door hebben. Daardoor zullen drinkwaterbedrijven misschien vervuild water innemen. Weer anders is de situatie in een scenario waarin een cyberaanval een gezamenlijke leverancier treft. Dit zal dan alle organisaties raken die de systemen van deze leverancier gebruiken.

In een gezamenlijke werksessie bespreken de deelnemers de risico's voor de afzonderlijke organisaties. Vervolgens analyseren ze op basis van de onderlinge afhankelijkheden de impact op ketenniveau. Aan het eind van deze gezamenlijke analyse hebben de deelnemers alle cyberrisico's in beeld: zowel op organisatieniveau als voor de gehele keten.

Waterketen



Het resultaat – stevige schakels en een sterke keten

Het gezamenlijke beeld van de risico's en weerbaarheid op ketenniveau stelt organisaties in staat om te bepalen waar extra inspanning nodig is. Dit kan er bijvoorbeeld toe leiden dat de bescherming van bepaalde cruciale systemen extra aandacht krijgt. Maar ook dat een informatiestroom die niet noodzakelijk is voor het functioneren van de keten wordt afgesloten, met minder kwetsbaarheid tot gevolg. Het blijkt verder erg nuttig dat professionals van verschillende organisaties tijdens de ketenanalyse met elkaar sparren en van elkaar leren. Zowel op technisch als op relationeel niveau ontstaan er zo stevigere schakels en een sterkere keten.

Meer informatie

Wilt u meedoen aan een ketenanalyse? Of meer weten over deze methode? Neem dan contact op met het programma Cyberweerbaarheid in de Watersector via cyberweerbaarheidwater@minienw.nl. U kunt ook kijken op www.versterkencyberweerbaarheid.nl.

Het programma ontwikkelt verder samen met TNO een spel voor managers. Door het spelen van dit spel kunnen organisaties oefenen met het nemen van maatregelen en de samenwerking in de keten. Ook voor informatie over dit spel kunt u ons benaderen via cyberweerbaarheidwater@minienw.nl.

Dit is een uitgave van
Ministerie van Infrastructuur en Waterstaat

Augustus 2022

Inzicht in informatiestromen