



Brede aanpak digitale weerbaarheid (water)sportbedrijven en havens

Met een breed programma worden de watersport- en recreatiebedrijven weerbaarder op het gebied van cyber (digitaal gedrag) en bewust van de risico's die ze lopen. Er wordt een breed programma opgesteld (in het kader van vitaal platteland) om bedrijven weerbaarder te maken op het gebied van cyberveiligheid en hen bewust te maken van de risico's, wat ook bijdraagt aan een duurzame samenwerking van de betrokken partners.

Doelen:

1. De watersportbranche in Fryslân bewust maken van de risico's die bedrijven lopen op gebied van ondermijning en slachtofferschap van cybercriminaliteit.
2. Digitaal weerbaar maken en houden van een grote hoeveelheid aan watersportbedrijven.
3. Uitrol van de ontwikkelde aanpak in Nederland via HISWA-RECRON op gebied van voorlichting en preventie bij digitalisering.

Daarnaast worden drie beoogde eindresultaten/-producten benoemd:

1. Een fact sheet met resultaten, aanbevelingen en geleerde lessen.
2. Een uitgegeven plan van aanpak dat elders zo overgenomen en uitgevoerd kan worden.
3. Actieve faciliterende rol van de HISWA-RECRON op gebied van voorlichting en preventie bij digitalisering.

Doelgroep: recreatiebedrijven in Friesland.

Stakeholders

- Gemeente Súdwest-Fryslân
- Samenwerking met buurgemeenten Leeuwarden, de Fryske Marren en Harlingen
- Politie
- PVO Noord Nederland en Oost Nederland
- MKB Fryslân
- MKB Cyber Campus
- Applicatieleveranciers
- Firda (onderwijsinstelling)
- HISWA-RECRON

Verloop interventie:

- Doelgroep en werving: er hebben 80, van de 100-150 beoogde, bedrijven deelgenomen aan de interventie. De deelnemers zijn op verschillende manieren geworven; er is

een brief vanuit de burgemeester aan watersportbedrijven gestuurd en er is een event met HISWA-RECRON georganiseerd. Ook zijn sociale media, de website en lokale kranten ingezet voor de werving.

- Samenwerking: alle respondenten waren positief over de samenwerking met HISWA-RECRON. Verder waren er uitdagingen in de samenwerking; de agenda's van samenwerkingspartners lieten een snelle overgang van zaken niet altijd toe. Ook was de taakverdeling niet altijd duidelijk en liep de communicatie soms moeizaam.

Doel behaald?

Het is nog onduidelijk of de cyberweerbaarheid is verhoogd, vooral de gemeenten zijn sceptisch of dit doel is behaald. Volgens mkb Cyber Campus zijn de doelen behaald.

Succesfactoren

Samenwerking. De competenties van de partners waren goed voor de samenwerking. Branchepartij HISWA-RECRON bracht een groot bereik en kende de doelgroep goed. Dit was te zien in de bijeenkomst die in samenwerking was georganiseerd.

Belemmerende factoren

Communicatie. De communicatie tussen de gemeenten en de MKB Cyber Campus verliep soms moeizaam. De gemeenten gaven aan geen updates te ontvangen, terwijl de MKB Cyber Campus juist stelde deze wel te hebben gestuurd. Beide partijen erkenden een verschil in ervaring, mede door wisselingen van rollen bij de gemeenten. Het bereik werd verschillend beoordeeld: de MKB Cyber Campus en HISWA-RECRON waren tevreden, maar de gemeenten misten duidelijkheid over deelnemende bedrijven en het aantal.

Doorontwikkeling

Er zijn geen concrete plannen voor een doorontwikkeling. De ervaringen worden meegenomen door gemeenten voor bijvoorbeeld het nieuwe integraal veiligheidsplan.

Implementatie elders

- Er zijn momenteel geen concrete plannen om de interventies op andere locaties te implementeren.
- Logistieke aspecten, zoals afstand, zijn een probleem om het plan zelf verder op te schalen.

Tips voor het opzetten van een cyberproject

Ga je aan de slag met dit of een ander cyberproject? Bekijk de [CCV-site voor een paar essentiële tips](#). Die informatie kan je helpen met een gestructureerd verloop van het cyberproject en een kwalitatieve evaluatie. Zo maak je echt verschil in cyberweerbaarheid.