Managementsamenvatting programma Digitale Veiligheid

Dit programma Digitale Veiligheid geeft u een handreiking om het onderwerp digitale veiligheid en criminaliteit te duiden, een serieuze plek te geven in uw (lokaal) veiligheidsbeleid en concreet aan de slag te gaan met interventies om slachtoffer- en daderschap te voorkomen.

Het programma Digitale Veiligheid is gebaseerd op de Regionale Veiligheidsstrategie 2019-2022 en wordt aangestuurd door de Taskforce Digitale Veiligheid. Daarin zijn politie, OM en alle districten in Midden-Nederland bestuurlijk vertegenwoordigd.

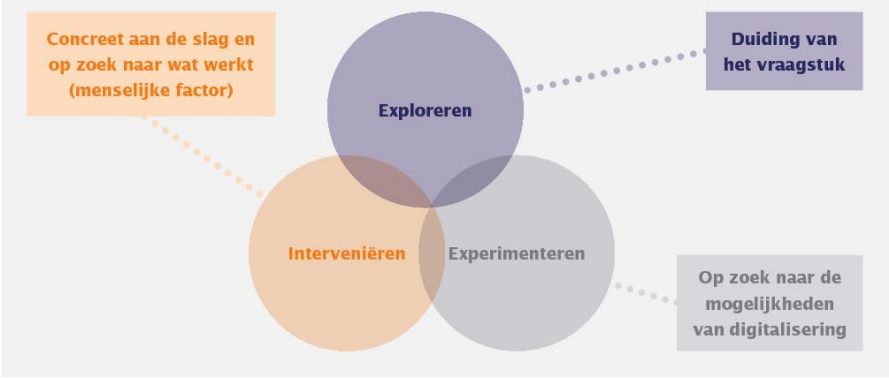
1. Naar een beter bescherming tegen digitale indringers en criminelen

In 2022 zijn we beter beschermd tegen digitale indringers en criminelen. En is de aanpak van digitale criminaliteit en onveiligheid net zo normaal als de aanpak van bijvoorbeeld woninginbraken en veelvoorkomende criminaliteit. Dat zijn de twee hoofddoelen van het Programma Digitale Veiligheid.

2. Wat gaan we doen?

Het programma Digitale Veiligheid is opgebouwd langs drie programmalijnen: exploreren, interveniëren en experimenteren (zie figuur 1). Centraal staat de mens als zwakste en tevens sterkste schakel in de informatiebeveiliging.

Figuur 1: Toelichting programmalijnen



Exploreren: duiding van het vraagstuk

Deze pijler richt zich op het verduidelijken van het probleem en de opdracht rondom digitale criminaliteit en (on)veiligheid. Dit gebeurt door het organiseren van diverse masterclasses en trainingen. Daarnaast door het opstellen van een periodiek cyberbeeld voor de regio Midden-Nederland om beter zicht te krijgen op de problematiek. De domeinen Veiligheid en Informatiebeveiliging spelen beiden een belangrijke rol in de aanpak van digitale (on)veiligheid. Om die reden wordt vanaf de start van het programma de verbinding gelegd tussen deze twee domeinen.

Experimenteren: concreet aan de slag en op zoek naar wat werkt

Concreet aan de slag met interventies om slachtofferschap en daderschap te voorkomen. Denk bijvoorbeeld aan (digitale) weerbaarheidstrainingen voor ondernemers, knock & talkgesprekken met zogenaamde moneymules, games voor jongeren en digitale buurtpreventie. Specifiek voor medewerkers worden trainingen georganiseerd om misleiding via social-engineering te voorkomen. En in samenwerking met politie, OM en J&V wordt een serie verhalende podcasts over slachtoffers en daders van digitale criminaliteit ontwikkeld. Het merendeel van deze interventies wordt via praktijkgericht wetenschappelijk onderzoek gemonitord en verbeterd.

Interveniëren: op zoek naar de mogelijkheden van digitalisering

Naast risico's en gevaren biedt digitalisering ook mogelijkheden om sociale veiligheidsvraagstukken op te lossen. De Veiligheidscoalitie biedt een platform voor experimenten, concepten en technologieën op het snijvlak van veiligheid, informatiebeveiliging en privacy. Met daarbij als belangrijke uitgangspunt het respecteren van de privacy en autonomie van mensen. Om die reden werken we de komende jaren mee aan een promotieonderzoek naar de toenemende invloed van digitalisering in het veiligheidsdomein en hoe veiligheidsprofessionals en bestuurders daar verantwoord mee om kunnen gaan. Dit promotieonderzoek leidt tot artikelen en lezingen en trainingen die breed toegankelijk zijn voor het netwerk.

3. Achtergrond: digitale criminaliteit en onveiligheid nemen toe

De geregistreerde criminaliteit in Nederland neemt al jaren af. Tegelijkertijd zijn er andere ernstige vormen van criminaliteit die toenemen en minder zichtbaar zijn in de politiecijfers. Digitale criminaliteit is daar een voorbeeld van. Van het stelen, verkopen of vernielen van onze (persoons)gegevens tot het platleggen van systemen die we elke dag gebruiken. En van het hacken van onze webshopaccounts tot afpersing met gijzelsoftware. Dit is een gevolg van de steeds verdergaande digitalisering. Die biedt ons veel voordelen, maar we denken onvoldoende na over de risico's en kwetsbaarheden en het nemen van beschermende maatregelen. We weten ons fysieke huis goed te beveiligen, maar de ramen en deuren van ons digitale huis staan vaak nog wagenwijd open. Alleen samen kunnen we daar wat aan doen.

4. Doelgroepen

Het programma Digitale Veiligheid richt zich in eerste instantie op jongeren, MKB-ondernemers en medewerkers binnen onze eigen organisaties. Jongeren en MKB'ers omdat ze het grootste risico lopen om slachtoffer te worden. Medewerkers omdat ze een belangrijke risicodoelgroep zijn vanwege de gegevens waar ze mee werken. Gegevens die, als ze in verkeerde handen vallen, tot ernstige maatschappelijke schade en slachtofferschap leiden. Niet voor niets worden gegevens inmiddels 'het nieuwe goud' genoemd.

Binnen het programma Digitale Veiligheid is maatwerk een belangrijk onderdeel en wordt ingespeeld op de lokale behoefte. Als bijvoorbeeld blijkt dat in een gemeente veel ouderen slachtoffer worden van cybercriminaliteit, wordt gekeken wat er vanuit het programma mogelijk is.