

City Deal

Lokale Weerbaarheid Cybercrime



Cybercriminaliteit stijgt en toch onderschatten veel burgers en bedrijven digitale risico's. Ze worden hierdoor gemakkelijk doelwit en slachtoffer. Om de cyberweerbaarheid bij inwoners en bedrijven te vergroten, is in 2020 de City Deal Lokale Weerbaarheid Cybercrime afgesloten. Dit samenwerkingsverband is met 17 nieuwe preventieve cyberprojecten in 2022 versterkt.

Wat we doen in deze City Deal

De City Deal Lokale Weerbaarheid Cybercrime verbindt partijen in hun aanpak van lokale cyberveiligheid. Op lokaal niveau zijn veel creatieve en innovatieve ideeën over hoe gemeenten, regionale samenwerkingsverbanden en Platforms Veilig Ondernemen (PVO's) de cyberweerbaarheid van inwoners en bedrijven kunnen versterken. Om gedragsverandering te bereiken en handelingsperspectief te bieden worden pilots opgezet. Sinds 2020 zijn een aantal zeer veelbelovende lokale cyberprojecten van de grond gekomen. We gaan in 2022 door met 17 nieuwe projecten. Nieuw is dat 2 van de 17 projecten zich richten op het thema online aangejaagde ordeverstoringen.

Doelen City Deal

1. Bundelen innovatiekracht

Door het bundelen van innovatiekracht, van elkaar te leren, samen te werken en goede initiatieven met elkaar te delen en te gebruiken, maken we meer impact.

Experimenteren, gelijkwaardigheid en innoveren zijn kernbegrippen in City Deals. City Deals zijn een initiatief van het programma Agenda Stad dat in 2015 door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ontwikkeld is.

2. Koppeling landelijke initiatieven op thema cybercrime

De leden van de stuurgroep en de deelnemers van het coalitieoverleg van de City Deal onderhouden diverse contacten met andere initiatieven op het gebied van (lokale) weerbaarheid cybercrime, zoals:

- Bestuurlijke aanpak lokale cyberveiligheid (JenV, CCV, G4, G40 en de VNG)
- Convenant 'Eerst checken dan klikken'
- Agenda Digitale Veiligheid (VNG)
- Impact Coalitie Safety en Security (ICSS)
- Nederlandse Cybersecuritystrategie (NLCS)
- Digital Trust Center (DTC)
- Platform cyberburgemeesters
- RAAK publiek – onderzoekscollectief Cybercrime & Cybersecurity
- Expertisecentrum Cybersafety en IT Security
- MKB Nederland – Cybersecurity
- Project Online content moderatie (JenV)

Door dit netwerk worden innovatieve trends op het gebied van cyberime en online ordeverstoringen tijdig gesignaleerd en in de aanpak van de City Deal verwerkt.

3. Ontwikkelen en verspreiden van nieuwe kennis

Met behulp van de Lokale Cyberwegenkaart maakt het CCV inzichtelijk welke vier wegen gemeenten moeten nemen om een cyberweerbare gemeente te worden. De bijbehorende menukaart biedt voor de cyberweg 'Cybercrime en gedigitaliseerde criminaliteit' vijf succesvolle City Deal interventies. In een opslag is duidelijk wat deze projecten opleveren en hoeveel tijd en geld het kost om ze te implementeren.

Alle cyberprojecten van de City Deal staan in de CCV-database lokale cyberprojecten. Via deze database is de lokaal opgedane kennis toegankelijk voor elke belangstellende. In deze database staan cyberprojecten onder andere uitgesplitst naar de doelgroepen jongeren, bewoners, bedrijfsleven en de gemeentelijke organisatie. Zo wordt het makkelijker om goede initiatieven te vinden die passen in het eigen organisatiebeleid.

4. Bestuurlijke agendering thema lokale aanpak cybercrime

Net als andere City Deals, is ook deze City Deal een samenwerkingsverband waarin gemeenten, ministeries en andere maatschappelijke partners en/of marktpartijen op basis van gelijkwaardigheid samenwerken. Door de bundeling van krachten ontstaat een podium waarmee bestuurlijke aandacht voor de aanpak van cybercrime versterkt kan worden. Bestuurlijke aandacht en structurele financiering zijn essentieel om cyberprojecten duurzaam te maken en te borgen voor de gemeentelijke praktijk. Met behulp van 'roadshows' wil het CCV laten zien dat cyberveiligheid op een makkelijke toepasbare manier is op te nemen in de Integrale Veiligheidsplannen (IVP's). Het CCV organiseert deze bijeenkomsten met regionale samenwerkingsverbanden en/of netwerken openbare orde en veiligheid.

Partners van de City Deal

- Het ministerie van JenV spant zich in om de resultaten van deze City Deal te integreren in de landelijk JenV-aanpak van de preventie, opsporing en vervolging van cybercrime en de daarbij behorende beleidsmatige, juridische en financiële kaders.
- Het ministerie van BZK spant zich in om - mede in het kader van de Agenda digitale overheid - de (tussen) resultaten van deze City Deal in te zetten voor een veilig gebruik van een veilige digitale infrastructuur, zodat inwoners en bedrijven vertrouwen kunnen houden in de digitale samenleving.
- Het ministerie van EZK, het Digital Trust Center (DTC), spant zich in om ondernemend Nederland in staat te stellen om haar digitale veiligheid te vergroten.
- Het CCV en de VNG zetten zich in om de resultaten van deze projecten breed onder alle gemeenten, regionale samenwerkingsverbanden en PVO's te verspreiden zodat het tegengaan van cybercrime onderdeel wordt van de integrale veiligheidsplannen op lokaal, regionaal en nationaal niveau.
- De kennisinstellingen begeleiden een aantal projecten en streven ernaar om alle deelnemende projecten op effect te evalueren. Hiernaast worden verkenningen uitgevoerd op het gebied van bestuurlijke bevoegdheden en interventies in de onlinewereld, waardoor de praktijkkennis verder wordt ontwikkeld.

Evidence based

In de City Deal Lokale Weerbaarheid Cybercrime zijn we een groot voorstander van projecten die 'evidence based' zijn opgezet. Het streven is om alle deelnemende projecten op een wetenschappelijke wijze te evalueren.

Meer informatie

Het secretariaat van de City Deal Lokale Weerbaarheid Cybercrime wordt gevoerd door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Stuur voor meer informatie een mail naar sten.meijer@hetccv.nl of kijk op de CCV-site: <https://hetccv.nl/onderwerpen/cybercrime/city-deal-lokale-weerbaarheid-cybercrime/>

Projectdoelstellingen

De cyberprojecten hebben tot doel:

A. Het verhogen van de cyberweerbaarheid van het MKB

De laatste jaren is de digitalisering in de samenleving toegenomen. De benodigde beveiligingsmaatregelen zijn niet in gelijke mate opgelopen waardoor de beveiliging bij veel kleine MKB-ers achterloopt. Ook zijn veel MKB-ers zich nog onvoldoende bewust van de gevaren van cybercrime waardoor zij onvoldoende preventieve maatregelen nemen om hen buiten de deur te houden. Er wordt ingezet op de preventie van cybercrime om de digitale weerbaarheid van MKB-bedrijven op orde te krijgen.

Of:

B. Het verhogen van cyberweerbaarheid op wijkniveau en kwetsbare groepen

Jongeren, ouderen en laaggeletterden lopen een groot risico om slachtoffer te worden van cybercrime. Jongeren zijn erg actief op internet maar hebben niet altijd een goed beeld van de risico's en welk gedrag wel of niet strafbaar is. Senioren worden steeds handiger achter de computer maar voelen zich vaak kwetsbaar. Daarnaast kent ons land veel laaggeletterden (ongeveer 1 op de 6 mensen in Nederland) die moeite hebben met digitale vaardigheden en voor wie informatie over cybercrime lastig is om te begrijpen. Gemeenten hebben een belangrijke rol in het voorkomen van slachtofferschap onder deze kwetsbare groepen.

Of:

C. Het versterken van de lokale en regionale aanpak van online aangejaagde ordeverstoringen

Gemeenten lijken steeds vaker geconfronteerd te worden met ordeverstoringen die online beginnen of online versterkt worden. Het gaat dan bijvoorbeeld om onrust rondom politieke besluiten, overlast door (jeugd)groepen en individuen, oproepen tot demonstraties en illegale evenementen. Deze projecten gaan in op hoe een gemeente effectief toezicht houdt en handhaaft bij online aangejaagde ordeverstoringen.

Cyberprojecten

re_BooTCMP

Bureau Regionale Veiligheidsstrategie i.s.m. Noord-Holland Samen Veilig, Regio Limburg en Veiligheidsnetwerk Oost-Nederland

De innovatieve re_BooTCMP maakt jongeren die affiniteit hebben met IT, weerbaar tegen het ontwikkelen van een criminele cybercarrière. Jongeren - en hun ouders - worden geïnformeerd over wat wel en niet mag op het internet. Jongeren leren hoe ze hun IT-skills op een positieve manier kunnen inzetten. Dit om de (online)wereld een stukje mooier en veiliger te maken. Re_BooTCMP is een coalitie dat bestaat uit gemeente, politie, cybersecuritybedrijven en het onderwijs.

ConNect: Samen bouwen aan online interventiematrix

Gemeente Amsterdam / Actiecentrum Veiligheid en Zorg (Veiligheidshuis)

Dit project levert een online interventiematrix op om online opjutting en uitdaging tegen te gaan. Dit project is een samenwerkingsverband tussen het Actiecentrum Veiligheid en Zorg (AcVZ) Amsterdam- Amstellandgemeenten, de NHL Stenden Hogeschool en de Rijksuniversiteit Groningen.

Project 'Digitale Inclusie'

Gemeente Amersfoort in samenwerking met stichting HackShield

Het project 'Digitale Inclusie' richt zich specifiek op kinderen op in kwetsbare wijken. Deze kinderen zijn vaak minder digitaal geletterd en ze zijn vatbaarder voor online criminaliteit. Met het project gaan gemeente Amersfoort en Stichting HackShield niet alleen in de gemeente Amersfoort de kwetsbare wijken in. Maar ook in Amsterdam, Rotterdam en Utrecht gaan ze het gesprek aan met de leraren, ouders, broers en zussen van de kinderen die ze willen bereiken. Dit doen ze samen met en via (digitale) wijkagenten, AZC's, moskeeën, bibliotheken en bijvoorbeeld jongerenwerk.

Youth Cyber Team

Gemeente Arnhem

Dit project richt zich op het versterken van de cyberweerbaarheid van kwetsbare jongeren uit twee Arnhemse wijken: Presikhaaf en Malburgen. Hier hebben veel bewoners een niet-Westerse afkomst en leven in onstabiele gezinssituaties. Jongeren worden op straat geronseld als zogenoemde geldezels. Daarnaast worden ze ook steeds vaker verleid tot het plegen van cybercriminaliteit. Waaronder online fraude, mensen online verleiden om phishinglinks te volgen en het afpersen van mensen via sociale media.

DigiKamer voor gemeenten

Gemeente Breda

Openbare ordeverstoringen vinden steeds vaker hun oorsprong in het digitale domein. Met deze pilot wil gemeente Breda, met inachtneming van de wettelijke privacyregels, meer

gebruik maken van openbare bronnen voor het veilig houden van de stad. Denk aan het analyseren van social media sentiment, nieuwsberichten en overige openbare bronnen. Door een 'DigiKamer' in te richten met de juiste hard- en software, wordt een centrale plek gecreëerd waar men met digitale zoekvragen terecht kan en waar men van elkaar kan leren. Politie Breda is betrokken bij deze pilot. De pilot wordt nadrukkelijk niet ingezet om personen of groepen te monitoren.

Gastveilig Hazeldonk - Digitaal Vitaal Breda

Gemeente Breda

Gastveilig Hazeldonk is een veelomvattend programma rondom veiligheid, toegepaste digitale technologie en -data op bedrijventerreinen. Bedrijventerrein Hazeldonk is hiervoor de proeftuin. Het project voor lokale weerbaarheid cybercrime is een onderdeel van dat programma en specifiek gericht op gedragsverandering voor cyberweerbaarheid. In het project zijn de activiteiten gericht op de toepassing binnen de primaire bedrijfsprocessen van de logistieke bedrijven. Het voordeel daarvan is dat gemeente Breda intensief contact heeft met de medewerkers in die bedrijven waardoor cyberweerbaarheid een onderdeel van de dagelijkse werkzaamheden wordt. Ervaringen uit de proeftuin worden breed gedeeld met andere bedrijventerreinen in Zeeland en West-Brabant.

Serious game cyberweerbaarheid laaggeletterden

Gemeente Dordrecht/Coevorden

Er wordt een fysieke serious game ontwikkeld waar een krachtige metafoor rondom de digitale online omgeving wordt gesteld. Een vrijwilliger speelt als spelbegeleider het spel samen met een laaggeletterde. Dit vindt plaats in een taalhuis, bibliotheek of in een andere organisatie in het sociaal domein. Het is van belang extra aandacht te geven aan kwetsbare groepen om hen te helpen zich veilig online te begeven.

Living Lab Cyberweerbaarheid & Ransomware MKB

Gemeente Groningen

In de Living Labs komen alle activiteiten samen die tot nu toe door publiek-private samenwerking in de regio Noord Nederland zijn ontplooid op het gebied van bijvoorbeeld bewustwording, training en scans. De nadruk ligt in eerste instantie op ransomware bij de financieel dienstverleners. Vergroting van bewustwording over en versterking van de weerbaarheid tegen ransomware is de basis voor de selectie van nauw verwante vraagstukken vanuit het MKB. Deze worden vervolgens met de Overheid, het Onderwijs en de Ondernemers (de drie O's) gezamenlijk opgepakt. Het Living Lab Cyberweerbaarheid wordt ondergebracht op drie bestaande fysieke locaties in Noord Nederland waar partijen al samenwerken.

Digitaal Veilig in Limburg

Gemeente Heerlen namens de Taskforce Cyber Limburg

De Taskforce Cyber Limburg is een gemeentelijk initiatief. Het

is een samenwerking van meer dan 16 gemeenten in Limburg. De Taskforce werkt daarbij samen met partners zoals politie, OM, Provincie Limburg, PVO/ECCW en de Veiligheidsregio's. Doel is om te komen tot een gezamenlijk cyberbeleid met gezamenlijke prioriteiten, preventieve acties en budget. De wens is om gezamenlijk en uniform naar buiten te treden waar dat effectief is. Daarnaast ondersteunen en coördineren ze de lokale behoefte en invulling.

Brede aanpak digitale weerbaarheid (water)sportbedrijven en havens

Gemeenten Súdwest-Fryslân en De Fryske Marren

Beide gemeenten hebben veel watersportgebieden met watersportbedrijven, zoals (jacht)havens, aanleg- en stallingsplekken en botenverhuurbedrijven. Het is een bekend gegeven dat deze MKB-bedrijven vaker dan gemiddeld slachtoffer zijn van digitale/cybercriminaliteit. Bovendien is er door de ligging in het omvangrijke buitengebied minder toezicht. Gemeente Súdwest-Fryslân voert beleid uit om het platteland vitaal en gezond te maken en houden, dit project wordt hier integraal onderdeel van.

Digitale Cybersecurity Ster voor KVO-B

Gemeente Veenendaal

De Bedrijvenkring Ondernemend Veenendaal heeft al jaren het Keurmerk Veilig Ondernemen Bedrijfsterreinen (KVO-B) op orde. Binnen de KVO-B is cybersecurity nog geen meetbaar item. Het doel van dit project is het cybersecurity niveau meetbaar maken en naar betrokken bedrijven terug te koppelen. En om dit te valideren en te waarderen met een 'digitale cybersecurity ster' als onderdeel of aanvulling op het KVO-B. De inzet van de digitale ster wordt dan ook een wezenlijk onderdeel van het KVO-B traject.

Juice of (fake-)news?

Gemeenten Amstelveen-Aalsmeer

Het project is erop gericht om te werken aan '21st century-skills' van jongeren. Zoals onderzoeksvaardigheden en kritisch denken om ze te leren door de bomen het bos wél te zien. Jongeren krijgen meer inzicht in de online bubbel; hoe kom je erin (en er weer uit) en vooral hoe onderzoek en beoordeel je de informatie die je tegenkomt? Wat zijn goede bronnen en hoe filter je de belangen van een contentmaker uit de informatie die wordt verspreid?

Evidence based cybersecurity gedragsinterventie gericht op drie basisprincipes van veilig ondernemen

PVO Den Haag

In dit project ontwikkelt PVO Den Haag een interventie die gericht is op drie van de vijf basisprincipes van veilig digitaal ondernemen: inventariseer kwetsbaarheden, voer updates uit en voorkom malware. Onderdeel van de interventie is het aanbieden van een handelingsperspectief voor deze drie maatregelen. Deze maatregelen zijn goed meetbaar te maken waardoor de interventie getoetst kan worden.

Sterkere schakels versterken de keten!

Regiobureau Integrale Veiligheid Oost-Brabant

De keten is zo sterk als de zwakste schakel. Dit geldt ook voor de cybersecurity in de keten van toeleveranciers van grote bedrijven. Grote bedrijven hebben over het algemeen meer financiële middelen en kennis in huis om de informatiebeveiliging op orde te hebben en te houden. Kleinere bedrijven hebben per definitie minder financiële middelen en kennis om dit te doen. Dit leidt tot kwetsbaarheden voor de gehele keten. Dit project ontwikkelt een methodiek waarbij de grote bedrijven de kleinere toeleveranciers ondersteunen bij het opschrijven van de informatiebeveiliging. Daar plukken de individuele bedrijven – en daarmee de gehele keten – de vruchten van.

Regionaal Expertteam Digitale Veiligheid

Regiobureau Integrale Veiligheid Oost-Brabant

Vooral in kleinere gemeenten met een beperkt aantal medewerkers is vaak geen tijd en capaciteit om een cyberinterventie te implementeren. Regiobureau Integrale Veiligheid Oost-Brabant wil zijn 32 gemeenten ondersteunen op het gebied van Digitale Veiligheid. Ze willen goedwerkende cyberinterventies aanbieden en hen zoveel mogelijk ontzorgen.

Interactieve training cyberweerbaarheid senioren

VeiligheidsAlliantie regio Rotterdam (VAR)

In dit project wordt een interactieve film ontwikkeld, waarmee gemeenten via ouderenwerk, politie, bibliotheken etc. het gesprek aan kunnen gaan met senioren over veilig internetgebruik. In de film zitten keuzemogelijkheden waarbij de film wordt stopgezet en aan de senioren wordt gevraagd wat zij in deze situatie zouden doen. De film gaat daarna verder met de keuze die gemaakt is. Door te ervaren wat er gebeurt als er een verkeerde keuze wordt gemaakt, blijft de opgedane kennis beter hangen. Onderwerpen die aan bod komen zijn: hulpvraagfraude/Whatsapp fraude, helpdeskfraude, phishing/ smishing, spoofing en datingfraude.

Internetveiligheid - Risk Factory Nederland

Veiligheidsregio Twente

Risk Factory is een interactief veiligheidseducatiecentrum. De activiteiten zijn met name gericht op het primaire onderwijs (groep 8). De kinderen komen in een veilige omgeving in aanraking met risico's passend bij hun leefwereld. Zij leren hoe ze hiermee om moeten gaan. Dit doen zij door meerdere scenario's te doorlopen. Denk aan ondermijning, brandveiligheid, sexting, verkeersveiligheid, melden van incidenten (112) en internetveiligheid. Het project maakt gebruik van een internetscenario dat aansluit op het programma HackShield.

Bekijk alle cyberprojecten in de [CCV-database Lokale cyberprojecten](#).