

Webinar 08.12.2022

(Cyber)-Incident? Laat weten dat je ermee bezig bent!

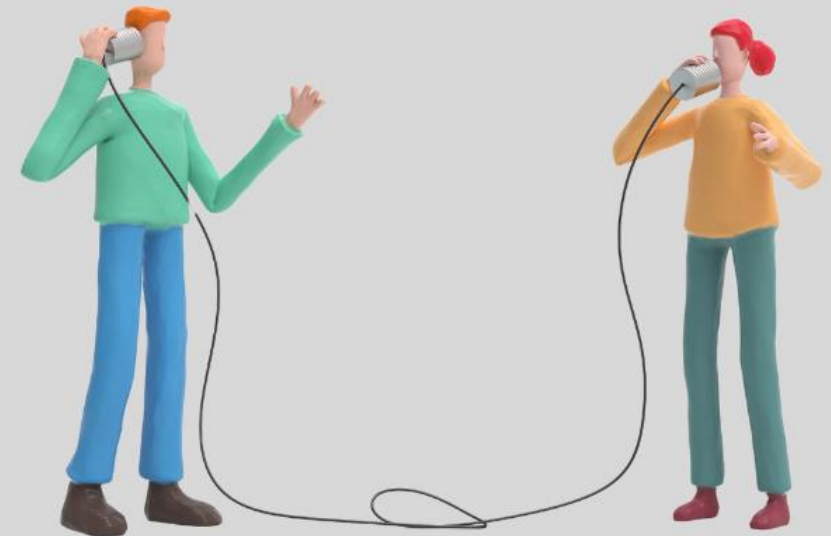
Welkom,
we starten om 10u.

We zenden uit via **MS Teams**. Volg via:

- Microsoft Teams App
- Browser (Chrome, Firefox of Edge)

Technische problemen?

Mail naar ann.ronsman@vvsg.be



Webinar 08.12.2022

(Cyber)-Incident? Laat weten dat je ermee bezig bent!

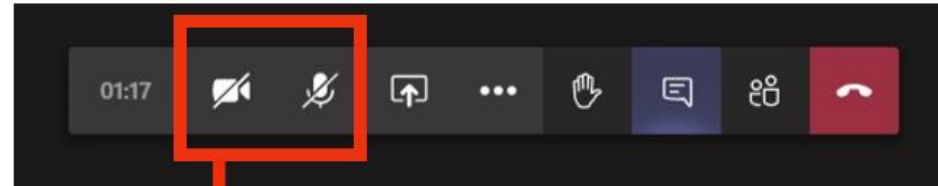
Welkom



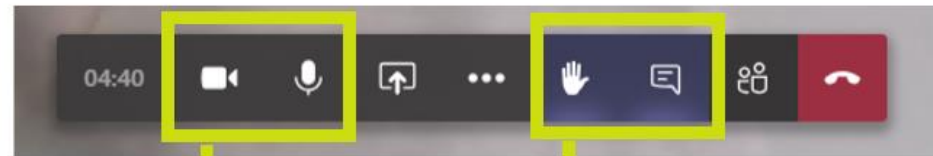
vvsg

Praktische afspraken

- Opname van deze sessie nadien op de website
- Heb je een vraag? Stel ze in de chat!
- Na afloop **evaluatieformulier**
Jullie feedback is heel erg waardevol!



Zet video en geluid uit



Zet uw micro en video aan
Nadien zet u ze weer uit

Vraag het woord via
de chat of klik op
het handje



Projectmedewerker Cyberveilige Gemeenten (VVSG)

- Jolien Schoonooghe
- Contact:
 - Jolien.Schoonooghe@vvsg.be



Projectmedewerker communicatie en kennisdeling

- Eliene Rijcken
- Eliene.Rijcken@vvsg.be

1. Korte inleiding | 10.00 uur tot 10.05 uur

- Jolien Schoonooghe, projectmedewerker cyberveilige gemeenten (VVSG)

2. Toelichting Toolkit Cybersecurity | 10.05 uur tot 10.30 uur

- Jolien Schoonooghe, projectmedewerker cyberveilige gemeenten (VVSG)

3. Toelichting over crisiscommunicatie bij een (cyber)-incident | 10.30 uur tot 11.10 uur

- Mieke De Meester, Coördinator crisiscommunicatie bij het Crisiscentrum van de Vlaamse overheid.

4. Q&A | 11.10 uur – 11.20 uur

5. Slotwoord | 11.20 uur – 11.30 uur

- In het kader van het **Project Cyberveilige Gemeenten**
 - Een samenwerking tussen de VVSG, het Agentschap Binnenlands Bestuur, Audit Vlaanderen en Digitaal Vlaanderen
 - In samenspraak met het Kabinet van Vlaams minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen
- Drie verschillende luiken:
 1. De ontwikkeling van een Toolkit Cybersecurity
 2. Een Traject Ethisch Hacken in samenwerking met Howest, waarbij het mogelijk is om dit te combineren met ICT-veiligheidsaudits met co- financiering via Audit Vlaanderen
 3. Bewustmaking en kennisdeling a.d.h.v. interactieve webinars en inspiratiesessies

Webinar 08.12.2022

Toolkit Cybersecurity

Jolien Schoonooghe
Projectmedewerker cyberveilige
gemeenten (VVSG)

vvsg



- Ga naar
 - [Menti.com](https://www.menti.com)

Code: **2546 9943**



Mentimeter

Toolkit Cybersecurity

- 12 verschillend tools
 - Een draaiboek Cybercrime
 - Een business continuïteitsplan sjabloon
 - Een crisiscommunicatieplan sjabloon
 - Een checklist crisisbeheer sjabloon
 - Een beleid voor responsible disclosure sjabloon
 - Een register voor cyberincidenten sjabloon
 - Een procedure melding cyberincidenten sjabloon
 - Een interne en externe contactenlijsten sjabloon
 - Richtlijnen Secure Software Development
 - Een veiligheids- en opvolgingsplan sjabloon
 - Richtlijnen organisatiebeheersing sjabloon
 - Cybertips en -tricks



Draaiboek Cybercrime



Business continuïteitsplan



Crisiscommunicatieplan



Checklist crisisbeheer



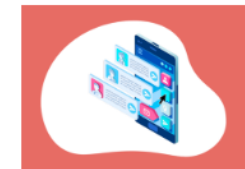
Beleid voor responsible disclosure



Register voor cyberincidenten



Procedure melding cyberincidenten



Interne en externe contactlijsten



Richtlijnen Secure Software Development



Veiligheids- en opvolgingsplan



Richtlijnen organisatiebeheersing



Cybertips en -tricks

Tools rond incident responds

Draaiboek Cybercrime

Crisiscommunicatieplan

Checklist crisisbeheer

Register voor cyberincidenten

Interne en externe contactlijsten

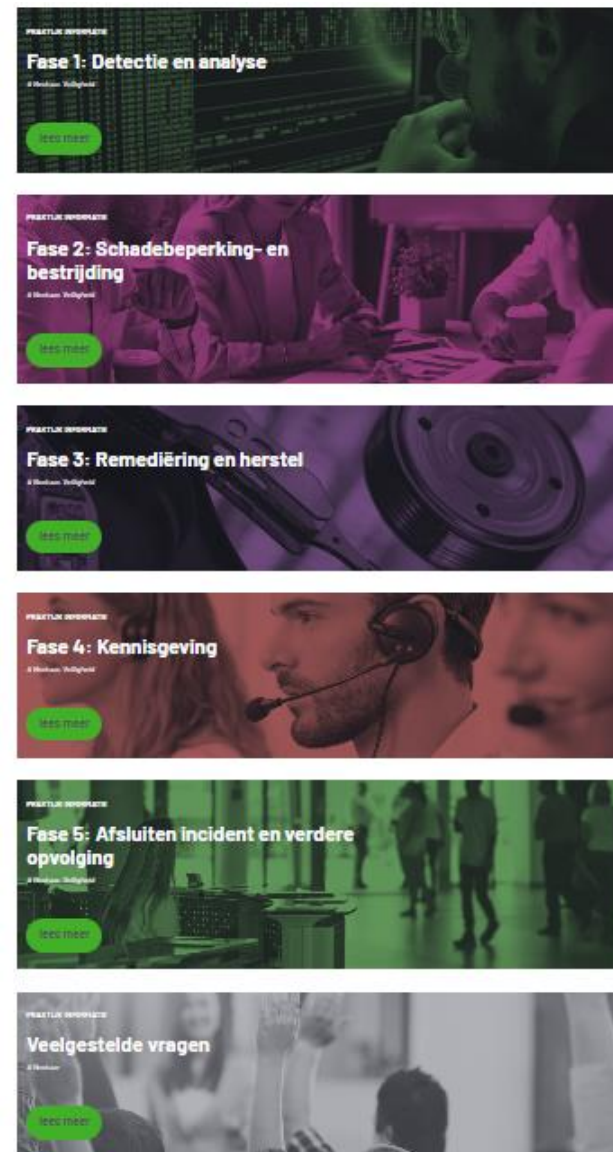
Procedure melding cyberincidenten

Draaiboek Cybercrime



Draaiboek Cybercrime

- Het draaiboek cybercrime geeft een omvattende en pragmatische aanpak weer voor het bestrijden van cyberveiligheidsincidenten.
- De beschreven stappen kunnen gebruikt worden als inspiratiebron voor een eigen incident response plan of draaiboek.



Crisiscommunicatieplan

- Sjabloon
- Een crisiscommunicatieplan legt vast op welke manier je als organisatie of lokaal bestuur ervoor zal zorgen dat de communicatie tijdens een crisissituatie coherent kan verlopen en dat deze het imago, de legitimiteit en de vertrouwensrelaties met stakeholders waarborgt.



Crisiscommunicatieplan

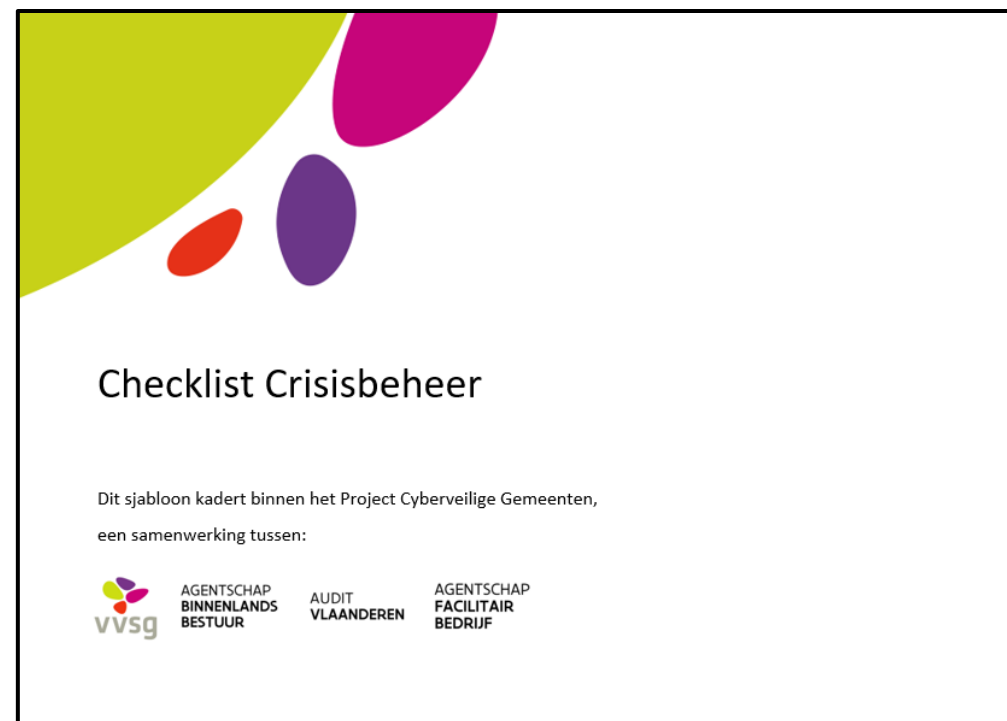


Checklist crisisbeheer

- Sjabloon
- Wanneer je lokaal bestuur geconfronteerd wordt met een cyberaanval of ander IT-gerelateerd incident, dienen op korte termijn diverse maatregelen genomen te worden om de situatie onder controle te krijgen en terug te keren naar de gewone werking.
- Proactief nadenken over de te nemen stappen faciliteert het crisisbeheer bij grootschalige incidenten.



Checklist crisisbeheer



Register voor cyberincidenten



Register voor
cyberincidenten

- Sjabloon
- Een incidentenregister is een waardevolle tool om het zicht te behouden op de informatie- en cyberveiligheidsincidenten die zich voordoen in je lokaal bestuur en welke opvolging hier concreet aan werd gegeven.
- Daarnaast kan het ook een belangrijke inspiratiebron voor beleidskeuzes zijn, aangezien het classificeren van incidenten zicht geeft op mogelijke pijnpunten binnen de organisatie of IT-omgeving.

Interne en externe contactlijsten

- Sjabloon
- Wanneer zich een cyber- of informatieveiligheidsincident voordoet is het cruciaal dat medewerkers, partners en instanties snel gecontacteerd kunnen worden.
- Door op voorhand na te denken over de nodige profielen voor een degelijk crisisbeheer en bijhorende contactgegevens op te lijsten bespaar je je heel wat kopzorgen in het heetst van de strijd.

Interne en externe contactlijsten voor informatieveiligheidsincidenten en datalekken

VVSG

Naam	Functie	Lid Informatie- veiligheids- commissie	Telefoon	E-mail
Naam Consulent	Functionaris voor gegevensbescherming (DPO)	ja	XXX XXXXX	privacy@organisatie.be
Naam Consulent	Back-up functionaris voor gegevensbescherming	nee	XXX XXXXX	privacy@organisatie.be
Organisatie	Permanentiedienst	nee	XXX XXXXX	emailadres@organisatie.be
Naam Voornaam	Algemeen directeur (AD)	nee	XXX XXXXX	emailadres@bestuur.be
Naam Voornaam	IT-medewerker	ja	XXX XXXXX	emailadres@bestuur.be
Naam Voornaam	IT-medewerker	ja	XXX XXXXX	emailadres@bestuur.be
Naam Voornaam	Diensthooft interne zaken	ja	XXX XXXXX	emailadres@bestuur.be
Naam Voornaam	Diensthooft burgerzaken	ja	XXX XXXXX	emailadres@bestuur.be
Naam Voornaam	Diensthooft personeel	ja	XXX XXXXX	emailadres@bestuur.be
...	...			
Naam Voornaam	Burgemeester	nee	XXX XXXXX	emailadres@bestuur.be
Naam Voornaam	Schepen voor informatica	nee	XXX XXXXX	emailadres@bestuur.be

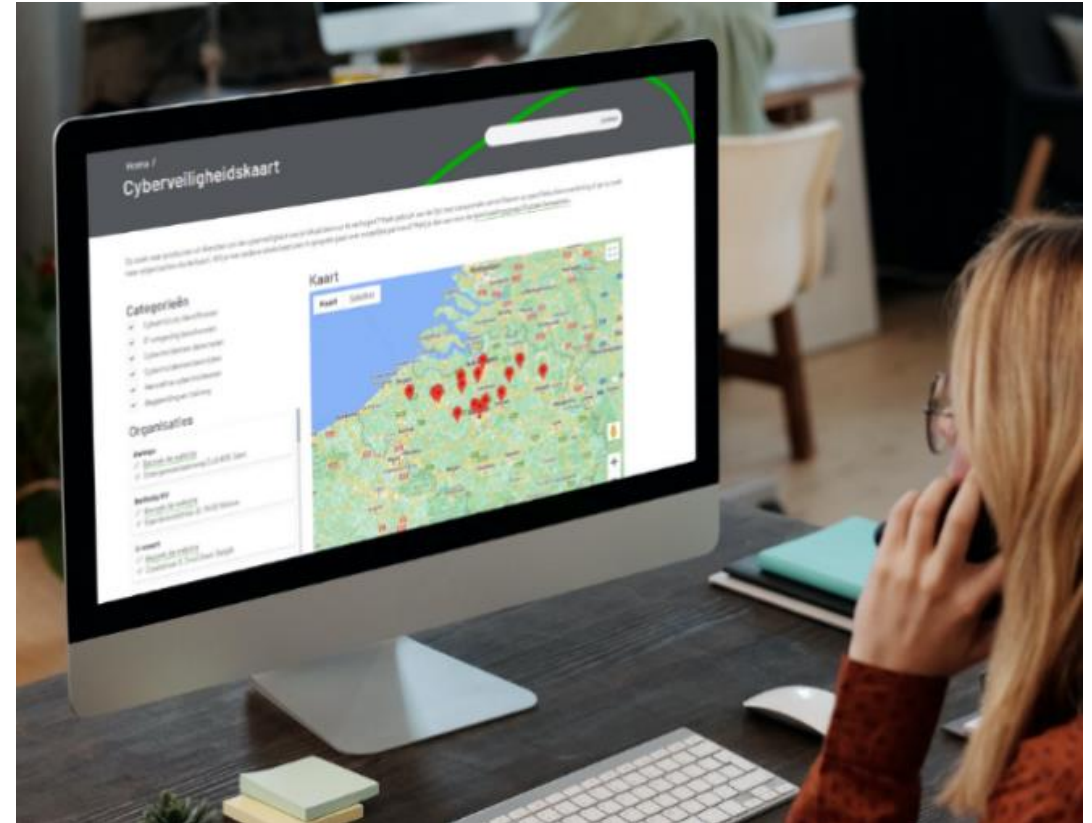
Procedure melding cyberincidenten

- Sjabloon
- Wie moet intern op de hoogte zijn van een informatieveiligheids- of cyberincident? Welke externa instanties dienen betrokken te worden? De interne en externe meldingsprocedure brengt deze processen in kaart.



Cyberveiligheidskaart

- Een interactieve cyberveiligheidskaart ontwikkeld die lokale besturen de weg wijst naar organisaties, bedrijven en kennisinstellingen met een interessant aanbod op maat van lokale besturen.



Project Cyberveilige Gemeenten

- Projectpagina cyberveiligheid via het VVSG-kennisnetwerk
- Vragen, opmerkingen of suggesties?
 - Cyberveiligheid@vvsg.be

Webinar 08.12.2022

Toelichting crisiscommunicatie bij een (cyber)incident

Mieke De Meester
Coördinator crisiscommunicatie bij het
Crisiscentrum van de Vlaamse overheid

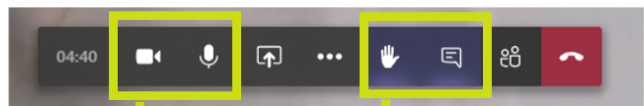
vvsg



Webinar 08.12.2022

Q&A

Stel je vraag via de chat



Zet uw micro en video aan
Nadien zet u ze weer uit

Vraag het woord via
de chat of klik op
het handje

VVSG



Na het webinar

Je ontvangt uiterlijk morgen een evaluatieformulier met de link naar:

- de opname van het webinar
- de presentatie

Vraag niet behandeld tijdens het webinar?

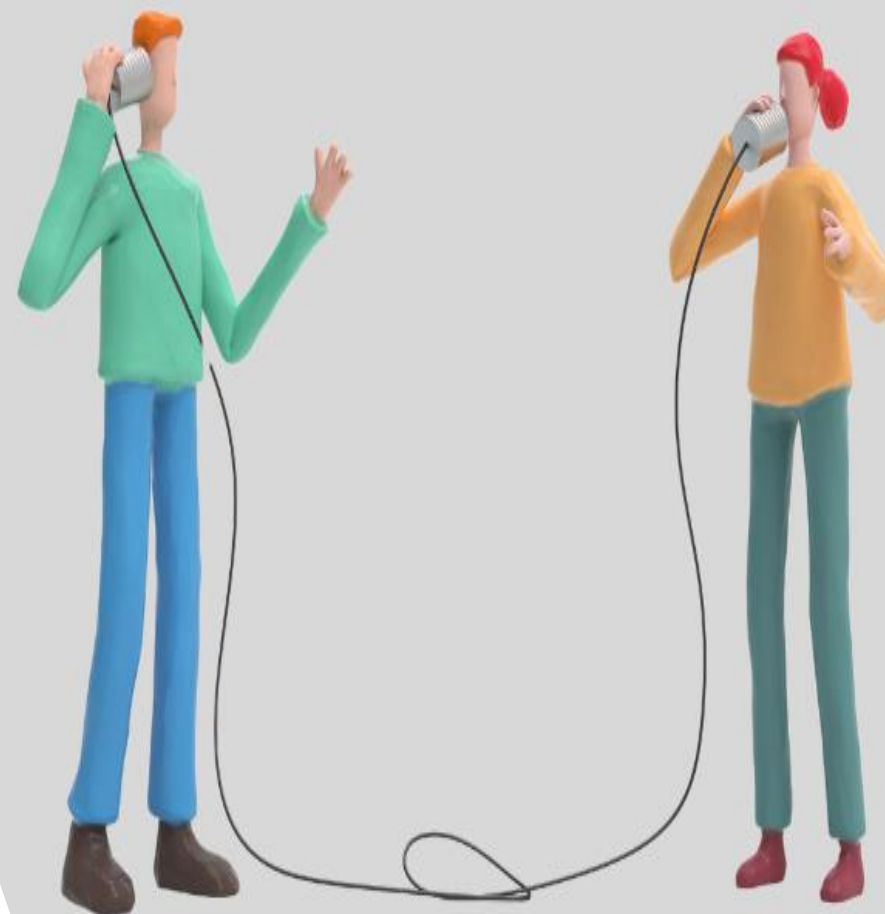
- Wij bundelen de vragen en plaatsen deze achteraf op de projectpagina cyberveiligheid via het VVSG-kennisnetwerk.

Webinar 08.12.2022

Bedankt voor de aandacht

Vragen, opmerkingen of suggesties
i.v.m. cyberveiligheid?

- cyberveiligheid@vvsg.be



vvsg