Een samenwerking tussen de VVSG, Agentschap Binnenlands Bestuur, Audit Vlaanderen en Digitaal Vlaanderen.

In samenspraak met het kabinet Bart Somers, Vlaams minister van Binnenlands Bestuur, Bestuurszaken, Inburgering en Gelijke Kansen

Cyberaanvallen lokale besturen

Infosessie 21 december 2022 | 9u – 10u

Ward VAN HAL | VVSG
Gunter SCHRYVERS | Audit Vlaanderen
Johan SMEKENS | Digitaal Vlaanderen

VVSG AGENTSCHAP BINNENLANDS BESTUUR

AUDIT VLAANDEREN

DIGITAAL VLAANDEREN

Vlaamse overheid

PRAKTISCH

Cyberaanvallen lokale besturen

- Herbekijk de presentatie van de eerste infosessie opnieuw
- Besloten infosessie
- Heb je vragen, stel ze tijdens de sessie in de chat of stuur ze naar cyberresponse@vlaanderen.be

AGENDA

Cyberaanvallen lokale besturen

- Werking van het cyber response team van de Vlaamse overheid
- Vraag en Antwoord

Aanbod Cyber Response Team

(Beknopt)

ORGANISATIE TEAM INFORMATIEVEILIGHEID

Cyber Response Team | Vlaamse overheid (Vo-CRT)

Opstart naar aanleiding van de recente cyber incidenten bij lokale besturen

Bundelen en informeren

- Bronmateriaal:
  - Vragen rond inrichting informatieveiligheid (van lokale besturen)
  - Opvolging en advies uit audit rapporten | Audit Vlaanderen
  - Opvolging en advies uit case findings informatie CCB & CERT

    (Case details vallen onder het geheim van het onderzoek)
- Ondersteuning:
  - Adviezen en documentatie rond TOM's, cyber- & informatieveiligheid via ondersteunende ledenorganisaties (VVSG, V-ICT-OR, …)
  - Proces architectuur en templates cyber response plannen (horen bij BCM)
  - Contact met leveranciers bron informatie:
    - Ondersteunende ledenorganisaties, Audit Vlaanderen, CCB, CERT, commerciële cyber intelligence kanalen
  - Ondersteuning escalaties naar:
    - Cyber defense leveranciers (uit raamcontract Audit Vlaanderen)
    - CCB en CERT
    - Regulatoren GBA en VTC

CYBER & INFORMATION SECURITY INCIDENT MANAGEMENT
(Zal gekoppeld worden aan het 12 stappenplan van het CERT)

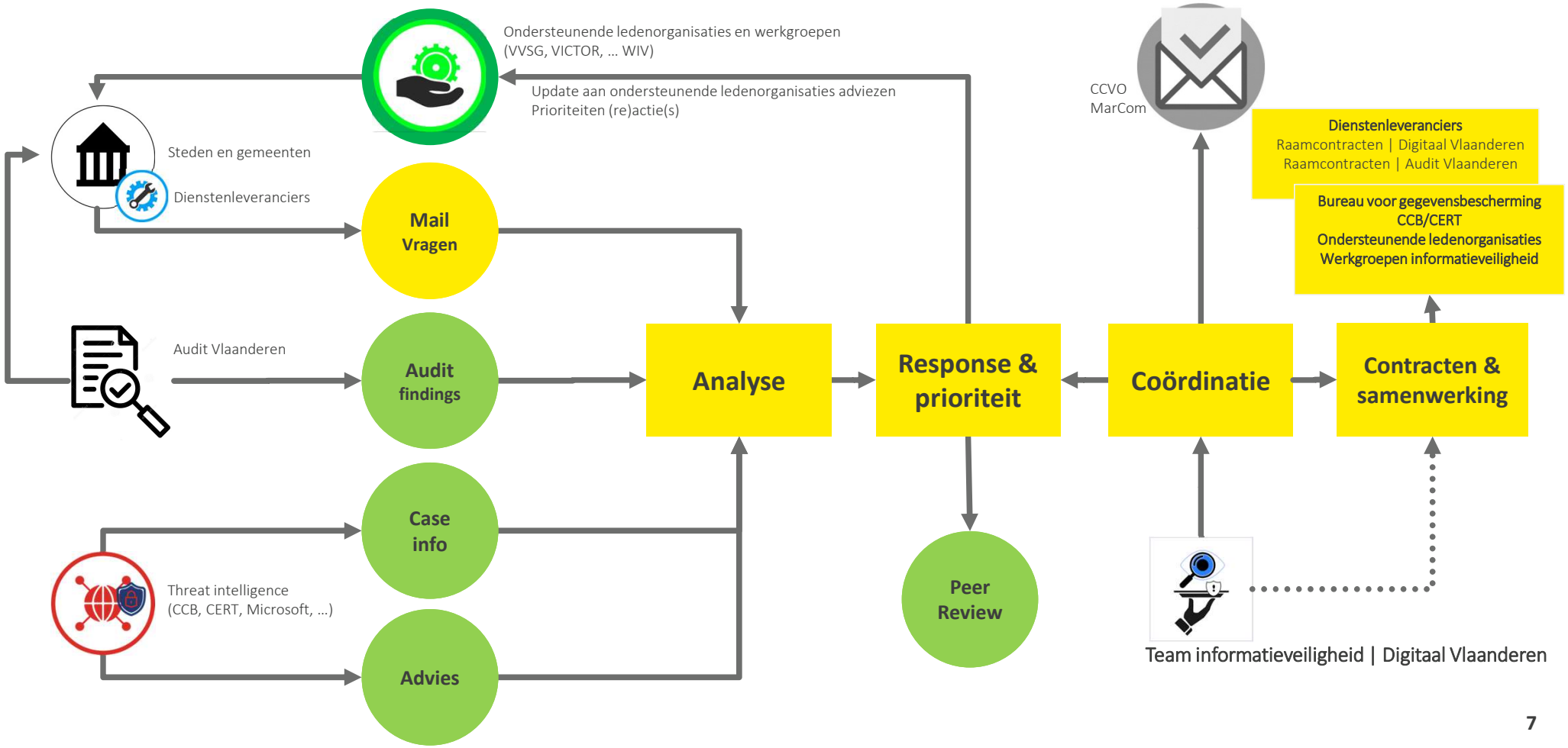
Lokaal bestuur
Dienstenleverancier

Vo-CRT aanbod

Detectie		bevestiging of uitsluiting van een cyberincident
First Response	Reactief	detectie van de getroffen dienstverlening/verwerking > 2de lijn ondersteuning cyber response plan (BCM) > relatiebeheer en uitzetten van ondersteunende opdrachten bij cyber forensische bedrijven binnen de raamcontracten van de Vlaamse overheid
Beperken impact		isolatie van getroffen dienstverlening/verwerking
Analyse		identificatie van de getroffen arena's en systemen lokaliseren van de aanvalsvector, bron en kenmerken
Beoordeling	Reactief	schatting van de omvang van het incident > 2de lijn ondersteuning bij meldingen aan politiediensten, GBA of VTC
Forensisch onderzoek		forensische documentatie en informatieverzameling voor malware-analyse/reverse engineering (indien nodig)
Eliminatie		de aanval stoppen
Herstel		snelle terugkeer (DRP) naar routinematige activiteiten terwijl prioriteit wordt gegeven aan en schade wordt geminimaliseerd
Conclusies	Preventief	> bevindingen formuleren uit onderzoek naar incident en hersteladvies verlenen > geleerde lessen inzetten bij aangepaste adviezen met als doel de impact van toekomstige incidenten maximaal reduceren (VVSG, WIV)

Cyber response team Vlaamse overheid (Vo-CRT)

Organisatie



Ontvangen vragen

(FAQ)

FAQ

Dienstverlening van het Cyber Response Team

Vraag: *Welke diensten biedt het Cyber Response Team (CRT) aan?*

Antwoord: In het Cyber Response Team (CRT) van de Vlaamse overheid wordt expertise gebundeld van Agentschap Binnenlands Bestuur (ABB), Digitaal Vlaanderen, Audit Vlaanderen en de Vlaamse Vereniging van Steden en Gemeenten (VVSG), waardoor de Vlaamse overheid voor een gecoördineerde dienstverlening zorgt naar lokale besturen. Ook het Centrum voor Cybersecurity België (CCB) werkt hieraan mee en stelt zijn kennis en expertise ter beschikking.

De primaire doelstelling van het Cyber Response Team (CRT) is om overheden beter te ondersteunen, te sensibiliseren en te informeren.

FAQ

Dienstverlening van het Cyber Response Team

Vraag: *Biedt het Cyber Response Team (CRT) een 24/7 dienstverlening aan?*

Antwoord: Het Cyber Response Team (CRT) is bereikbaar via cyberresponse@vlaanderen.be. Vragen worden tussen kantooruren (09:00 – 17:00) behandeld.

Binnen het kader van **onze preventieve adviezen** verspreiden we de contact- en proces informatie waarmee u als lokaal bestuur **onmiddellijk mee aan de slag kan gaan.** (Documentatie in opbouw)

> *Bij **een acute noodsituatie**, raden we aan om onmiddellijk contact op te nemen met **het Cyber Emergency Response Team** (CERT) via het online formulier: https://cert.be/nl/een-incident-melden-form.*

Bovenstaande informatie zal op basis van de gestelde vragen verder in detail worden gedocumenteerd. Deze documentatie zal u vervolgens worden aangeboden via de standaard communicatiekanalen van de ondersteunende ledenorganisaties (VVSG, V-ICT-OR, etc.).

FAQ

Dienstverlening van het Cyber Response Team

Vraag: *Moeten cyberveiligheidsincidenten gemeld worden aan Cyber Response Team (CRT)?*

Antwoord: Het Cyber Response Team (CRT)werkt nauw samen met het CCB en het CERT.
Het CERT is het centrale meldpunt voor alle cyberveiligheidsincidenten die zich voordoen in ons land.

Als het onverhoopt mis gaat en u misbruik, inbraak of onbeschikbaarheid vaststelt van de infrastructuur, is het van belang om snel te handelen:

1. Informeer het Cyber Response Team (CRT) via cyberresponse@vlaanderen.be. Het Cyber Response Team (CRT) zal de lokale besturen bijstaan in het samenstellen van de informatie die moet worden aangeleverd aan het CCB/CERT.
   - Er is op heden geen verplichte melding aan het Cyber Response Team (CRT), maar uw informatie en ervaringen kan wel een belangrijke bijdragen leveren aan de veiligheid van alle (lokale) overheden, burgers en bedrijven.
   - Het Cyber Response Team (CRT)kan geen klachten behandelen uit naam van een lokaal bestuur, maar kan jullie wel helpen met het identificeren van prioriteiten en aan te leveren informatie aan het CCB/CERT.
   - Het Cyber Response Team (CRT) zal evalueren of het cyberincident op een adequate manier is opgevangen binnen de voorgestelde processen en aangepast advies en prioriteiten publiceren naar alle (lokale) overheden en hun ondersteunende ledenorganisaties.
2. Contacteer zo snel mogelijk het CERT via het online formulier: https://cert.be/nl/een-incident-melden-form.
3. Neem contact op met de lokale politie die desgevallend de Federal Computer Crime Unit (FCCU) kan inschakelen om de daders te vatten.

FAQ

Dienstverlening van het Cyber Response Team

Vraag: *Wat is de functie van het doorgegeven e-mailadres van de contactpersoon?*

Antwoord: Het doorgegeven e-mailadres zal worden gebruikt indien het Cyber Response Team (CRT) de lokale besturen snel moet kunnen bereiken in geval van een cyberveiligheidsincident of potentiële dreiging.

FAQ

Dienstverlening van het Cyber Response Team

Vraag: *Kunnen lokale besturen beroep doen op raamcontracten indien ondersteuning bij cyberveiligheidsincidenten vereist is?*

Antwoord: De lokale besturen kunnen beroep doen op onze huidige dienstencontracten.

FAQ

Dienstverlening van het Cyber Response Team

Vraag: *Bestaat er een gemeenschappelijke verzekering tegen cyberaanvallen waarop lokale besturen beroep kunnen doen?*

Antwoord: Neen

FAQ

ICT-veiligheidsaudits

Vraag: *Kan er nog beroep worden gedaan op cofinanciering voor ICT-veiligheidsaudits?*

Antwoord: De raamovereenkomst zal blijven lopen. Conform onderstaande vereisten, voorziet Audit Vlaanderen een cofinanciering binnen de grenzen van het beschikbare krediet:

- Voor een basisaudit wordt een cofinanciering van 2/3e van de kostprijs voorzien
- Voor een aanvullende audit wordt een cofinanciering van 1/2e van de kostprijs voorzien

Alle reeds in 2022 lopende bestellingen moeten uiterlijk vóór 31 december 2022 ingediend én opgeleverd zijn om van de cofinanciering te kunnen genieten

Zoals aangekondigd wordt momenteel gewerkt aan een mechanisme om ook in 2023 cofinanciering voor specifieke bestellingen te voorzien. U kan uw interesse hiervoor op voorhand doorgeven door een e-mail te sturen naar ICT-veiligheidsaudits@vlaanderen.be. Concrete informatie over de aangepaste modaliteiten daaromtrent zal zo snel mogelijk gecommuniceerd worden.

Praktisch zal voor de meeste bestellingen pas vanaf januari capaciteit kunnen worden ingezet. Voor vragen met hoogdringendheid kunnen de bedrijven geval per geval bekijken wat qua capaciteitsinzet mogelijk is.

FAQ

ICT-veiligheidsaudits

Vraag: *Kan een basisaudit opnieuw worden uitgevoerd door een andere partij?*

Antwoord: Het periodiek herhalen van de testen in de basisaudit en de aanvullende audit worden sterk aangeraden. In het kader van cofinanciering wordt dergelijke herhaling altijd beschouwd als een aanvullende audit en dus geldt er voor opnieuw uitgevoerde audits een cofinanciering van 1/2e van de kostprijs.

De voorwaarden voor het gebruik van de cascade staan beschreven in het bestek van de raamovereenkomst welke u kunt vinden via deze link:

https://auditvlaanderen.paddlecms.net/sites/default/files/2022-01/bestek%202019-HFB-OP-52630%20%281%29.pdf

FAQ

ICT-veiligheidsaudits

Vraag: *Kan een ICT-veiligheidsaudit worden uitgevoerd bij een dienstenleverancier?*

Antwoord: Elk lokaal bestuur kan bij de gunning van elke overheidsopdracht in het bestek voorwaarden bepalen. Dat kan gaan om het **proactief bieden van bijkomende inzichten** in de gehanteerde aanpak, zoals bv. **via een ISO27001-, ISAE3402-, en/of andere certificatie**. Eveneens kunnen clausules worden voorzien om periodiek verplichte audits te laten uitvoeren en om medewerking aan audits bij of door het lokaal bestuur te verplichten.

Audits die worden georganiseerd door een lokaal bestuur **met het oog op het in kaart brengen en/of verbeteren van de informatieveiligheid kunnen veelal voor cofinanciering in aanmerking komen**, ook wanneer daarbij gebruik wordt gemaakt van dergelijke auditclausules.

FAQ

Paswoordbeleid

Vraag: *Is het nodig om voor gebruikers een paswoordrotatie te voorzien, wanneer er al een 'sterk' wachtwoord wordt afgedwongen in combinatie met multi-factor authenticatie (MFA)?*

Antwoord: Het Cyber Response Team (CRT) wenst blijvend in te zetten op een correct paswoord beleid, zelfs bij vergaande integratie van MFA binnen de dienstverlening. De kwetsbaarheden die vandaag worden gebruikt bij cyberaanvallen geven aan dat cybercriminelen sterk inzetten op het omzeilen van MFA en daar ook steeds weer in slagen. Dit kan omdat niet alle technische MFA oplossingen zonder kwetsbaarheden zijn ingericht.

Een correct beleid is steeds **een combinatie van een correcte technische implementatie en een goede monitoring (van gebruikersaccounts)**. Hierdoor kan verdachte user account activiteit gedetecteerd worden zodat hier efficiënt op gereageerd kan worden (e.g., blokkeren van een account, wachtwoord wijzigen, etc.).

Mocht uw lokaal bestuur niet aan deze implementatie voorwaarden voldoen, dan wordt aangeraden om een **rotatie te voorzien die zo kort mogelijk is.**
Deze maatregel zorgt er voor dat gelekte paswoord informatie slechts voor korte periode van risico blootstelling zorgt.
Paswoord lekken is, naast kwetsbaarheden in de technologie, een van de belangrijkste aanvalsvectoren bij cyberincidenten.

Een correct wachtwoordbeleid voorkomt (onbewust) onveilig gedrag bij uw gebruikers.
Verder wordt het sterk aangeraden om **waar enigszins mogelijk** gebruik te maken van MFA, specifiek voor alle systemen die gevoelige of persoonsgegevens bevatten, of toegang kunnen verschaffen tot het interne netwerk. Dit kan worden gefaciliteerd door Vo-ACM, eID, ItsMe of TOTP, indien gebruik kan worden gemaakt van het Federaal Authenticatie Systeem (FAS).

Gebruik geen identieke paswoordcombinaties bij professioneel en privé activiteiten. Dit is de belangrijkste bron van gelekte paswoorden.

FAQ

Bedrijfscontinuïteit (BCM)

Vraag: *Wat zijn goede praktijken om te communiceren tijdens een noodsituatie wanneer e-mailinfrastructuur geïmpacteerd is?*

Antwoord: Wanneer zich een cyberveiligheidsincident voordoet is **het cruciaal dat medewerkers, partners en instanties snel gecontacteerd kunnen worden.** Door op voorhand na te denken (BCM) over de nodige profielen voor een degelijk crisisbeheer en bijhorende contactgegevens (e.g., e-mailadres, telefoon, mobiel) op te lijsten bespaart u zich heel wat kopzorgen in het heetst van de strijd.

Het is met andere woorden **sterk aangewezen om reeds een contactenlijst met de (belangrijkste) interne en externe belanghebbenden aan te leggen** voordat een crisissituatie zich daadwerkelijk voordoet en deze offline ter beschikking hebt.

Het is aangewezen om **een communicatiekanaal** op te zetten dat kan worden gebruikt bij een cyberveiligheidsincident. Indien het niet mogelijk is om via e-mail te communiceren, is het aangewezen om **alternatieve mogelijkheden** te zoeken. **Zo kan je bijvoorbeeld diensthoofden bellen en hen te vragen om de medewerkers binnen hun diensten verder te contacteren/informeren.**

FAQ

Cyberveiligheid toolkits

Vraag: *Worden de beschikbare toolkits uitgebreid?*

Antwoord: In functie van de noden van de lokale besturen kunnen de beschikbare aangeboden toolkits (e.g., VVSG en Audit Vlaanderen) worden uitgebreid binnen het kader van het project cyberveilige gemeenten.

De huidige documentatie kan via volgende kanalen worden geraadpleegd:

Cybersecurity Toolkit (VVSG)
https://www.vvsg.be/kennisitem/vvsg/cyberveilige-gemeenten

Goede praktijken voor lokale besturen (Audit Vlaanderen)
https://overheid.vlaanderen.be/goede-praktijken-leidraad-organisatiebeheersing

Bedankt voor uw aandacht

Vragen?

cyberresponse@vlaanderen.be

VVSG AGENTSCHAP BINNENLANDS BESTUUR

AUDIT VLAANDEREN

DIGITAAL VLAANDEREN

Vlaamse overheid