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 16 december 2022 | 9u – 10u

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

VVSG AGENTSCHAP BINNENLANDS BESTUUR

AUDIT VLAANDEREN

DIGITAAL VLAANDEREN

Vlaamse overheid

Deze sessie zal worden opgenomen

PRAKTISCH

Cyberaanvallen lokale besturen

- Open infosessie – opname binnenkort beschikbaar
- Heb je vragen, noteer ze en stuur ze naar cyberresponse@vlaanderen.be
- Tweede infosessie (besloten) op woensdag 21 december 2022 (9u-10u)
  - Feedback op de gestelde vragen
- In deze presentatie gaan we niet in detail in op de specifieke feiten uit deze incidenten. Deze zijn onderworpen aan geheimhouding.

AGENDA

Cyberaanvallen lokale besturen

- Context bij de recente cyberaanvallen
- Aanbevelingen : Snelle verbeterpunten om het risico op een cyber aanval te reduceren
- Oproep tot actie !
- Ondersteuningsinitiatieven voor lokale besturen
  - VVSG toolkit Cybersecurity
  - Cofinancieringsaanbod ICT-veiligheidsaudits
  - Cyber response team Vlaamse overheid (Nieuw)

CONTEXT

Cyberaanvallen lokale besturen

- Cyberdreigingen vormen in toenemende mate een risico voor overheden op alle niveaus
  Recent: cyberincidenten in Zwijndrecht, Antwerpen en Diest

- Sinds enkele weken zien overheden in Vlaanderen het aantal aanvallen op hun ICT-infrastructuur sterk stijgen

  Waarom nu?
  - **Alertheid** van personen: focus op afsluiten van het jaar, druk, verlof in het achterhoofd, cadeautjes en koopjes (phishing)
  - **Beschikbaarheid** van weerbare sleutelfiguren: verlof, op vakantie

- Aanval kan leiden tot
  - Verliezen van vertrouwen bij burgers en bedrijven
  - Onbeschikbaarheid/verlies van data waaronder ook persoonsgegevens (AVG)
  - Toegang tot data door onbevoegden, waaronder persoonsgegevens (AVG)
  - Onderbrekingen in de dienstverlening aan burgers en bedrijven
  - Onbeschikbaarheid van ICT-systemen

Checklist om het risico op een cyber aanval te reduceren

6 prioriteiten op basis van geleerde lessen

Checklist om het risico op een cyber aanval te reduceren

01 Beheer en patch kwetsbaarheden

Patch kwetsbaarheden:

- IT infrastructuur:
  - ✓ VPN gateways
  - ✓ Webservers
  - ✓ Mail infrastructuur
  - ✓ Firewall configuraties (bv. Fortinet)
- Pc, smartphone, tablets, ...
- Software:
  Zorg voor ondersteuning zodat u toegang hebt tot herstelsoftware (patches)
- Vervang verouderde toestellen

De VVSG heeft een opvolgingsplan ontwikkeld om de opvolging van het cyber veiligheidsplan te faciliteren.

In dit plan identificeert u het eigenaarschap en verantwoordelijkheden, bovenop een duidelijke planning wat betreft identificatie van kwetsbaarheden en een correct herstelplan.

https://www.vvsg.be/kennisitem/vvsg/sjabloon-veiligheids-en-opvolgingsplan

Checklist om het risico op een cyber aanval te reduceren

02 Beheer accounts en wachtwoorden

- Reset de wachtwoorden van alle accounts binnen uw netwerk (inclusief beheeraccounts) op regelmatige basis
- Valideer de blootstelling van uw domeinen en accounts via bijv. *HaveIBeenPwned*
- Zet in op Multi-Factor Authenticatie (Vo-ACM)
  - Stel een wachtwoordbeleid op, voor toepassingen waarop geen mogelijkheid is tot MFA
  - Wijs een verantwoordelijke aan die instaat voor een regelmatige vernieuwing van de wachtwoorden
- Maak gebruik van Windows LAPS of een PAM oplossing om geprivilegieerde accounts beter te beveiligen

De VVSG heeft richtlijnen opgesteld voor cyberveiligheid voor de volgende domeinen: identificeren, beveiligen, detecteren en herstellen. In het hoofdstuk 'beveiligen' (p.6-9) staan zeer bruikbare richtlijnen voor het verbeteren van jouw Identity Threat Protection.

https://www.vvsg.be/kennisitem/vvsg/richtlijnen-organisatiebeheersing

Checklist om het risico op een cyber aanval te reduceren

03 Gebruikers awareness

- Phishing is een zeer populair entry-point voor aanvallers
- Zorg voor opleiding en awareness bij de gebruikers hoe ze phishing kunnen herkennen en melden
- Voer regelmatig phishing campagnes uit om de waakzaamheid te stimuleren

In het kader van het project Cyberveilige Gemeenten werkte de VVSG een video en poster uit over phishing. U kan deze gebruiken om de medewerkers uit uw lokaal bestuur in te lichten over de gevaren van phishing.

https://www.vvsg.be/kennisitem/vvsg/help-is-dit-phishing

https://www.vlaanderen.be/nieuwsberichten/pas-op-voor-fraude-met-valse-e-mails-sms-phishing

Digitaal Vlaanderen heeft een aanbod met phishing campagnes en training Die u kunnen helpen om de bewust-wording bij uw gebruikers te stimuleren

04 Beheer en monitor uw IT infrastructuur

- Ken uw infrastructuur en breng de risico's in kaart
  - Ken het normale gedrag van uw infrastructuur
- Uitgaande communicatie
  - Blokkeer gekende risicovolle IP adressen
  - Ban datastromen uit geopolitiek gevoelige locaties
  - Laat enkel datastromen toe die echt nodig zijn
  - Beperk datastromen tot de minimale functionele behoefte
- Zorg voor monitoring op alle inkomende en uitgaande datastromen
  - IDS (Detectie van inbraken en misbruik)
  - IPS (Voorkom inbraken en misbruik)

In het kader van de ontwikkeling van een Security Operations Center (SOC) in de stad Geel, heeft de VVSG tips en tricks opgesteld voor het monitoren van een IT landschap. Je kunt deze gebruiken om jouw lokaal bestuur in te lichten over IT architecturen en hoe deze het best opgesteld en gemonitord kunnen worden.

https://www.vvsg.be/kennisitem/vvsg/kies-voor-een-structurele-aanpak-met-periodieke-opvolging-stad-geel

Geopolitieke risico's

https://crisiscentrum.be/nl/risicos-belgie/veiligheidsrisicos/geopolitieke-risicos

Checklist om het risico op een cyber aanval te reduceren

05 Bedrijfscontinuïteit

- Bepaal de prioriteit: identificeer kritische processen, gevoelige gegevens en kroonjuwelen
- Stel een bedrijfcontinuïteitsplan (BCM) op, implementeer het en test het
  - Dit laat toe om tijdelijk manueel verder te werken en een minimale dienstverlening te garanderen
  - Zorg voor een disaster recovery plan en een aangepaste set van maatregelen
    - Offline backup
      (bijv. een cloud oplossing met aparte keys)

Het VVSG heeft een Business Continuity Plan (BCP) sjabloon opgesteld die gebruikt kan worden om een op maat gemaakt BCP op te stellen of een reeds bestaand plan verder uit te werken.

https://www.vvsg.be/kennisitem/vvsg/sjabloon-business-continuiteitsplan

Checklist om het risico op een cyber aanval te reduceren

06 Versterk de weerbaarheid

- Beveilig je gevoelige gegevens tegen inzage door derden
  - Encryptie van media
    - Bitlocker, Azure key Vault, AWS Key management services.
- Beveilig je infrastructuur tegen ongewenste toegangen
  - Beperk de toegang tot het functionele minimum
  - Segmenteer uw netwerk, toepassingen en infrastructuur zodat een dreiging zich moeilijker kan verspreiden (0-trust)
    - Functioneel geminimaliseerde informatiestromen tussen deze segmenten
  - Zorg voor beheer van- kwetsbaarheden, patch management

Het VVSG heeft een Business Continuity Plan (BCP) sjabloon opgesteld die gebruikt kan worden om een op maat gemaakt BCP op te stellen of een reeds bestaand plan verder uit te werken.

https://www.vvsg.be/kennisitem/vvsg/sjabloon-business-continuiteitsplan

07

Bij twijfel…

- Contacteer het Cyber Response Team van de Vlaamse overheid of het CBB/CERT
- Zorg ervoor dat de juiste contactgegevens achtergelaten worden

Cyber Response Team

cyberresponse@vlaanderen.be

Centrum voor Cybersecurity België

info@ccb.belgium.be

Cyber Emergency Response Team

https://www.cert.be/nl/een-incident-melden-form

Checklist om het risico op een cyber aanval te reduceren

01 02 03 04 05 06 07

1. Beheer en patch kwetsbaarheden
2. Beheer accounts en wachtwoorden
3. Gebruikers awareness
4. Beheer en monitor uw IT infrastructuur
5. Bedrijfscontinuïteit
6. Versterk de weerbaarheid

Cyber Response Team

cyberresponse@vlaanderen.be

Centrum voor Cybersecurity België

info@ccb.belgium.be

Cyber Emergency Response Team

https://www.cert.be/nl/een-incident-melden-form

ICT-veiligheidsaudits met cofinanciering

https://www.auditvlaanderen.be/ict-veiligheidsaudits

Project Cyberveilige Gemeenten

https://www.vvsg.be/kennisitem/vvsg/cyberveiligheid

Oproep tot actie !

OPROEP TOT ACTIE!

Typische fenomenen bij een aanval en hoe ze te herkennen:

- Kijk na of er recent **accounts** werden toegevoegd op uw werkstations, servers
  - **Typisch fenomeen bij een aanval**
  - Inventariseer alle accounts (ook lokaal op machines) en valideer of er een gekende reden is om deze te hebben, zo niet, verwijder deze accounts
- Kijk na of er recent **geplande taken** werden aangemaakt op uw werkstations en servers
  - **Typisch fenomeen bij een aanval**
  - Inventariseer geplande taken en valideer of er een gekende reden is om deze te hebben, zo niet, beëindig deze taken
- Kijk na of alle accounts in **administrator rollen**, zowel lokaal als in AD gekend zijn, zo niet, beëindig deze accounts
  - **Typisch fenomeen bij een aanval**
- Kijk na of er recent **GPO**'s werden aangepast of toegevoegd op uw AD infrastructuur, wees kritisch
  - **Typisch fenomeen bij een aanval**
- **Neem alsnog deel aan de ICT-veiligheidsaudit!**

De VVSG heeft richtlijnen opgesteld voor cyberveiligheid voor de volgende domeinen: identificeren, beveiligen, detecteren en herstellen. De richtlijnen in dit document kunnen als leidraad dienen voor het uitvoeren van generieke cyber acties.

https://www.vvsg.be/kennisitem/vvsg/richtlijnen-organisatiebeheersing

Overleg deze acties met uw leveranciers!

Wat zijn de ondersteunings-initiatieven voor lokale besturen

Ondersteuningsinitiatieven voor lokale besturen

BESTAAND INITIATIEF: PROJECT CYBERVEILIGE GEMEENTEN

- Toolkit Cybersecurity
  12 tools om aan de slag te gaan rond cyberveiligheid
- Draaiboek cybercrime
  Het belang van regelmatig back-ups te maken
- Inspirerende webinars (her)bekijken via de projectpagina cyberveiligheid
- Traject Ethisch Hacken in samenwerking met Howest
  - In combinatie met een ICT-veiligheidsaudit met cofinanciering via Audit Vlaanderen
- Vragen, opmerkingen en suggesties over het project cyberveilige gemeenten?
  Raadpleeg onze website, contacteer ons via cyberveiligheid@vvsg.be

Ondersteuningsinitiatieven voor lokale besturen

BESTAAND INITIATIEF: COFINANCIERING ICT-VEILIGHEIDSAUDITS

- Bestelbaar op basis van raamovereenkomst → contacteer gerust de firma's rechtstreeks,

  eerst Deloitte Consulting & Advisory en indien nodig kan in cascade vervolgens contact opgenomen worden met Ernst & Young Special Business Services

- Basisaudit :

  interne en externe intrusietesten op minimum 3 systemen + zwakke wachtwoordentest
  Vast basispakket met optionele zesde dag (Vlaamse overheid draagt 2/3e van de kost)

- Aanvullende audit:

  inhoud kan op maat uitgewerkt worden in functie van de noden van het lokaal bestuur
  (50% cofinanciering)

- Vergemakkelijkt de inzet van gespecialiseerde ICT-auditoren
  om kwetsbaarheden te detecteren en om aan de slag te gaan met de remediëring daarvan

- Vragen, opmerkingen en suggesties m.b.t. cofinanciering ICT-veiligheidsaudits?
  Contacteer ons via ict-veiligheidsaudits@vlaanderen.be

Wat kan u verwachten van het cyber response team van de Vlaamse overheid ?

CYBER & INFORMATION SECURITY INCIDENT MANAGEMENT

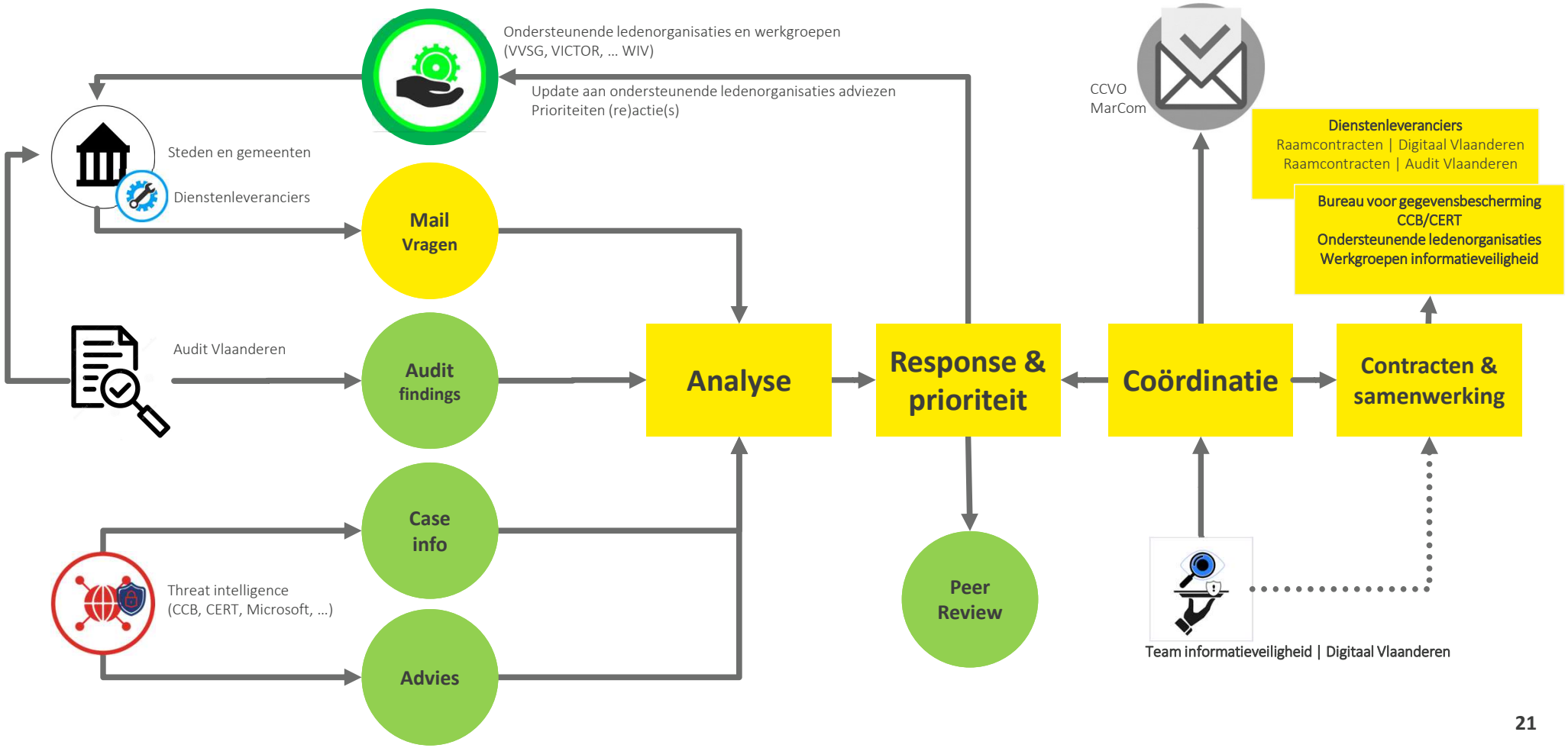
(Zal gekoppeld worden aan het 12 stappenplan van het CERT)

Vo-CRT aanbod

Detectie	bevestiging of uitsluiting van een cyberincident
First Response	detectie van de getroffen dienstverlening/verwerking > 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	schatting van de omvang van het incident > 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	> 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



Basis principes
Beschikbare ondersteunende documentatie

We gebruiken de bestaande basis elementen die reeds aanwezig zijn:

- Informatie cyberveilige gemeenten (VVSG)
- Audit rapporten (Audit Vlaanderen)
- Case info uit gekende incidenten (Zwijndrecht, Antwerpen, Diest)
- Adviezen CCB, CERT, Cyber threat intelligence

Bedankt voor uw aandacht

Vragen?

cyberresponse@vlaanderen.be

VVSG AGENTSCHAP BINNENLANDS BESTUUR

AUDIT VLAANDEREN

DIGITAAL VLAANDEREN

Vlaamse overheid