Webinar Cyber Response Team

Simulatie
Cyberveiligheidsincident bij
Lokaal Bestuur 'Hackegem'

DIGITAAL VLAANDEREN

Vlaamse overheid

FOCUS VAN DEZE WEBINAR

Wat kunt u verwachten tijdens deze webinar?

- Wat is het Vo-CRT?
- Use-case Cyberveiligheidsincident
  - Simulatie van een cyberincident bij een lokaal bestuur
  - Goede praktijken voor de 5 verschillende fases voor het beheren van een cyberincident
  - Geleerde lessen voor lokale besturen op basis van de use-case
- Doel: lokale besturen informeren op basis van geleerde lessen uit de praktijk

WAT IS HET CYBER RESPONSE TEAM?

PREVENTIEF
- Bundelen van 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
- Adviezen en documentatie rond cyber- & Informatieveiligheid
- Templates en hulpmiddelen (Bv. cyber response plan, security assessment, …)

REACTIEF: REMEDIËRING EN HERSTEL
- Ondersteuning van lokaal bestuur in geval van een cyberaanval
  - Faciliteren escalatie naar:
    - Cyber defense leveranciers (uit raamcontract Audit Vlaanderen, Digitaal Vlaanderen)
    - CCB en CERT
    - Regulatoren GBA en VTC

COMMUNICATIE
- Coördinatie van interne en externe communicatie naar alle belanghebbende doelgroepen

Use-case Cyberveiligheidsincident gemeente Hackegem*

* Gemeente Hackegem is een fictieve gemeente. Het scenario in deze use-case is gebaseerd op geleerde lessen van gehackte Vlaamse lokale besturen.

USE-CASE CYBERVEILIGHEIDSINCIDENT

CONTEXT

- **Gemeente Hackegem** is een gemeente in Vlaanderen met 150.000 inwoners.
- Het is de periode net voor de zomervakantie waardoor het erg druk is bij het lokaal bestuur. Inwoners vernieuwen nog snel hun paspoorten en het vakantiegeld voor het personeel van gemeente Hackegem wordt binnenkort uitbetaald.

CYBERINCIDENT

- Een medewerker van gemeente Hackegem wilt op vrijdagavond nog iets opzoeken op zijn werkcomputer en merkt dat hij geen toegang meer heeft tot bepaalde bestanden. Hij besluit IT een email te sturen en laat het daarbij. Bij gemeente Hackegem wordt er niet in het weekend gewerkt.
- Medewerkers loggen maandagochtend in op hun werkstations en merken dat zij geen toegang meer hebben tot alle computersystemen. Een IT- medewerker heeft hetzelfde probleem en wilt de IT- verantwoordelijke contacteren. Echter, de contactgegevens van het Hoofd IT zijn enkel online beschikbaar. Hierdoor wordt het Hoofd IT pas na 30 minuten gecontacteerd.
- Het Hoofd IT start zijn computer en ziet dat bijna alle servers zijn geëncrypteerd. Op de twee werkende servers staat een boodschap: **You are the victim of a ransomware attack**. Het Hoofd IT ziet deze boodschap en besluit om de centrale stekker eruit te trekken waardoor alle computersystemen meteen uitvallen.

INITIELE IMPACT

- Alle computersystemen werken niet meer waardoor het uitvoeren van werkzaamheden of verlenen van diensten niet mogelijk is voor de 600 medewerkers van de gemeente Hackegem.
- Het departement burgerzaken heeft de komende weken 4000 klanten waarvan de afspraken onzeker zijn.
- De uitbetaling van het loon en vakantiegeld is onzeker omdat de financiële dienstverlening onbeschikbaar is.

FASE 1

Detectie en analyse

SITUATIE

- Bij de gemeente Hackegem wordt de IT dienst na kantooruren via SMS geïnformeerd over verdachte situaties. De medewerker stuurt echter een email op vrijdagavond.
- Hoofd IT trekt onmiddellijk de centrale stekker eruit: alle systemen liggen plat. Hierdoor kan er geen bewijs verzameld worden.

GELEERDE LESSEN USE-CASE

- Gebruik de (meest) geschikte communicatiekanalen om verdachte situaties / incidenten te melden, zowel tijdens als na kantooruren; zorg dat iedereen deze communicatiekanalen kent.
- Overhaast en/of uit emotie handelen leidt niet altijd tot de meest optimale oplossing.

GOEDE PRAKTIJKEN

1. Communiceer direct en escaleer waar nodig

- Zorg voor duidelijke afspraken over notificatie en escalatie van IT-problemen. Verwittig IT via een gepast medium (**niet via email tijdens het weekend of avonduren**) wanneer u iets verdachts opmerkt op uw computersystemen. Bij een cyberincident kan elke minuut een verschil maken.

2. Onderzoek melding en verzamel bewijs

- Onderzoek de melding en check of o.a. de volgende zaken geïmpacteerd zijn: *wijzigingen in configuratiebestanden of bedrijfsgegevens, toeganglogs van systemen, operationele logs van systemen, firewall-logs, netwerkverkeer, meldingen uit endpointbeveiliging, onbeschikbare data.* **Vergeet niet om het beschikbare bewijsmateriaal te documenteren**. Deze inventaris is nodig om de reikwijdte van het cyberincident te kunnen vaststellen en te communiceren.

3. Communiceer intern en plan een crisisvergadering

- Bij het geval van een cyberincident is het zaak om **zo snel mogelijk intern te communiceren** zodat elke belangrijke stakeholder op de hoogte is. Een crisisteam bestaat op zijn minst uit de volgende rollen: *burgermeester, algemeen directeur en andere leidende ambtenaren, ICT-dienst, DPO en/of CISO, communicatiedienst.*

4. Maak een initieel plan van aanpak en schakel externe hulp in

- Tijdens de crisisvergadering bepaal je de initiële aanpak van het cyberincident. De initiële aanpak helpt om snel te handelen en om een overzicht te bewaren van de te nemen acties. Informeer zo snel mogelijk de lokale politie, het CERT, het Vo-CRT voor bijstand. Schakel indien nodig bijkomende technische expertise in via dienstenleveranciers. In geval van gelekte persoonsgegevens dient u ook het VTC/GBA tijdig in te lichten.

FASE 2

Schadebeperking en bestrijding

SITUATIE

- Het Hoofd IT kent een leverancier die nieuwe hardware kan leveren tegen een scherpe prijs. Het crisisteam gaat akkoord. Bij levering blijkt dat de machines eerst twee dagen geconfigureerd moeten worden.
- Interne medewerkers kunnen niet worden ingelicht omdat er geen fysieke contactlijst beschikbaar is.

GELEERDE LESSEN USE-CASE

- Neem de tijd om nieuwe hardware en systemen aan te kopen.
- Neem niet enkel levertijden, maar ook duur voor de configuratie van hardware en systemen mee in de verwachte hersteltijden.
- Zorg voor offline of fysieke versies van belangrijke documenten.

GOEDE PRAKTIJKEN

1. **Zet een structuur op voor crisiswerking**
   - Creëer een werkbare structuur voor een crisiswerking. **Stel het crisisteam definitief samen** (voeg bijv. politie of andere externe stakeholders toe aan de originele crisisgroep), maak afspraken over overlegmomenten en spreek af wat en naar wie mag gecommuniceerd worden.
2. **Rust het crisisteam uit en maximaliseer de capaciteit**
   - Voor het oplossen van het cyberincident zijn er ‘schone’ en veilige computers nodig met een netwerkverbinding en eventueel tijdelijk emailaccounts. **Zorg ervoor dat de nieuwe hardware gemakkelijk aan te sluiten is op uw bestaande systemen.** Indien dit niet het geval is, bestaat het risico dat u kostbare tijd verliest door de nodige configuraties.
   - Schakel waar nodig externe experts in en schaal de ‘normale’ werkzaamheden van uw IT- personeel waar mogelijk af. Zij focussen zich het best op het oplossen van het cyberincident.
3. **Start de crisiscommunicatie op**
   - Idealiter heeft uw lokaal bestuur een fysiek crisiscommunicatieplan klaar liggen met daarin contactlijsten en een overzicht van alternatieve communicatiekanalen.
   - Breng eerst uw interne medewerkers op de hoogte van het cyberincident zodat zij weten wat er aan de hand is en wijs contactpersonen aan voor hun vragen.
   - Breng hierna externen op de hoogte. Het wordt aangeraden om op een open manier met externen te communiceren. Dit is belangrijk om hevige reputatie schade en/of foutieve communicatie over het incident te voorkomen. Maak eventueel een FAQ om internen en externen in te lichten.
4. **Neem de nodige technische maatregelen**
   - Na de analyse van het cyberincident is het belangrijk om de getroffen systemen los te koppelen en geïmpacteerde of kwetsbare functionaliteiten stil te leggen. Bij een volledige encryptie van uw systemen kan dit leiden tot het stilleggen van uw volledige digitale infrastructuur.

FASE 3

Remediering en herstel

SITUATIE

- Gemeente Hackegem heeft geen BIA uitgevoerd en BCP opgemaakt omdat dit teveel geld kostte.
- Gemeente Hackegem schakelt een externe partij in om de BIA en heropstart te begeleiden.
- De hele infrastructuur inclusief back-ups zijn beschadigd en gemeente Hackegem moet de omgeving van nul heropbouwen.

GELEERDE LESSEN USE-CASE

- Investeer vooraf in een BIA en BCP.
- Denk in oplossingen (bijv. betrek buurgemeentes bij het opstellen van continuïteitsmaatregelen).
- Zorg voor veilige back-ups.

GOEDE PRAKTIJKEN

1. **Breng de impact in kaart en bereid kritieke processen voor**
   - Idealiter heeft **een bedrijfscontinuïteitplan (BCP)** uitgewerkt. Een BIA helpt om de belangrijkste processen/diensten binnen uw lokaal bestuur te identificeren en een BCP helpt om deze processen/diensten in de juiste volgorde en met de juiste middelen en capaciteit op te starten.
2. **Stel prioriteiten voor heropstart**
   - Wanneer uw lokaal bestuur reeds een **Business Impact Assessment (BIA) heeft uitgevoerd en** een BCP voor handen heeft, kunt u de stappen en volgorde van herstel volgen die daar beschreven staan. Indien deze plannen niet aanwezig zijn, zal het crisisteam **op basis van impactclustering** moeten bepalen welke processen wanneer opgestart moeten worden. Om de impact van het uitvallen van processen in te schatten, kunt u de volgende indicatoren gebruiken: m*enselijke impact, financiële impact, juridische impact, impact op reputatie, impact op dienstverlening*.
3. **Bedenk (alternatieve) oplossingen voor processen**
   - Zodra de prioritaire rangorde voor de heropstart van processen vaststaat, moet er gekeken worden hoe deze processen heropgestart moeten worden. Bij een cyberincident is het vaak niet mogelijk om de processen op de ‘normale’ manier operationeel te krijgen. Het is dus belangrijk om **out-of-the-box te denken en met alternatieve oplossingen** te komen.
   - Eenmaal dat er oplossingen zijn bedacht voor processen is het belangrijk om de juiste mensen, hardware, gegevens en werkplekken te verzamelen voor het uitvoeren van de heropstart.
4. **Herstel de benodigde systemen**
   - Voor het opstarten van uw dienstverlening heeft u zondermeer computersystemen nodig. Voor het herstel van systemen bestaan drie verschillende methodes: 1) Kwaadaardige artefacten schoonmaken en de aangetaste bestanden vervangen door schone versies 2) Herstellen vanaf een back-up 3) Systemen of omgeving vanaf nul heropbouwen.
   - Welk methode het best is voor uw lokaal bestuur hangt af van het cyberincident. **Laat u zich vooral bijstaan door een Cyber Emergency Response Team bij het maken van een herstelstrategie**.

FASE 4

Kennisgeving

Hackegem

SITUATIE

- Bij het cyberincident is er veel (gevoelige) data gelekt.
- De burgermeester vindt het verschrikkelijk voor de slachtoffers en stuurt een bericht uit naar de slachtoffers waarin hij schrijft dat de geïmpacteerden financieel gecompenseerd zullen worden voor de schade.

GELEERDE LESSEN USE-CASE

- Win juridisch advies in voordat u slachtoffers van een datalek informeert.
- Zorg dat communicatie naar de belanghebbenden (bijv. burgers, pers, enz.) op voorhand bepaald is.

GOEDE PRAKTIJKEN

1. Meld het cyberincident bij de juiste instanties

- Het beste meldt en registreert u een cyberincident bij de juiste instanties tijdens de Detect & Analyse fase. Indien u dat nog niet gedaan heeft, dan is dit het moment om dat alsnog te doen. Meld het incident bij het **VTC en GBA (binnen 72 uur)** en rapporteer het incident aan **het Cyber Response Team voor lokale overheden (Vo-CRT) en bij het CERT.** Als u een klacht wilt indienen tegen dader(s) is het ook vereist om aangifte te doen bij **de politie**.

2. Informeer de slachtoffers van datalekken

- Indien het cyberveiligheidsincident gepaard gaat met een datalek met een hoog risico voor de slachtoffers**, bent u als lokaal bestuur verplicht om hen te informeren.** Voordat u de slachtoffers informeert, wordt het aangeraden om **juridisch advies in te winnen**. Indien ook bankgegevens zijn blootgesteld, verwittigt u ook het beste banken of creditcard firma's.
- Kies een geschikt communicatiemiddel om de slachtoffers te informeren. Dit hangt vooral af van de hoeveelheid slachtoffers en de impact van de gelekte data op deze slachtoffers**. De kennisgeving dient zeker de volgende informatie te bevatten**: n*aam van de verantwoordelijke voor de gegevensverwerking, contactgegevens voor bijkomende informatie, samenvatting van het incident, aard van de betrokken gegevens, mogelijke gevolgen voor betrokkenen, genomen maatregelen om het lek te verhelpen en mogelijke schade te beperken*.

3. Registreer de gedane meldingen

- Aangezien het melden van een cyberincident onderhevig is aan **wetgeving en regels**, is het belangrijk om de gedane meldingen bij te houden in een meldingsregister (onderdeel van het logboek voor crisisbeheer). Hiermee kunt u in een oogopslag zien of alle relevante instanties gecontacteerd werden.

FASE 5

Afsluiten incident en opvolging

SITUATIE

- Het crisisteam evalueert het cyberincident en concludeert dat er een aantal minder optimale keuzes zijn gemaakt.
- De algemeen directeur beslist dat deze ‘fouten’ niet openbaar gemaakt mogen worden en verbiedt daarom het delen van de geleerde lessen.

GELEERDE LESSEN USE-CASE

- Deel altijd de geleerde lessen: de cyberveiligheid van lokale besturen is iets waar we samen aan moeten werken!

GOEDE PRAKTIJKEN

1. **Archiveer bewijsmateriaal en breng de impact in kaart**
   - Nadat het cyberincident grotendeels is afgehandeld, is het belangrijk om bestaande documentatie te archiveren en bijkomende informatie op te vragen die de gevolgen van het incident in kaart brengen (juridisch of financieel belang).
   - Zorg tenminste dat de volgende informatie gearchiveerd wordt: forensisch bewijsmateriaal, relevante incidentinformatie en communicatiegegevens, logboek, financiële gegevens (bijv. onvoorziene kosten).
2. **Evalueer de crisisaanpak en implementeer oplossingen en maatregelen uit evaluatie**
   - Enige tijd nadat de crisiswerking is afgebouwd, is het belangrijk om met het crisisteam de genomen crisisacties te evalueren. Het beste doet u dit door gezamenlijk door het logboek te gaan. Naast een evaluatie met het crisisteam wordt het ook aangeraden om medewerkers (en andere geïmpacteerde) te bevragen.
   - Tijdens de evaluatie zullen waarschijnlijk oplossingen en maatregelen naar boven komen die een herhaling van het cyberincident kunnen voorkomen in de toekomst. **Vertaal deze geleerde lessen naar de praktijk** en leg ze vast in de processen en procedures van uw lokaal bestuur.
3. **Plan afsluitende communicatie**
   - Nadat het cyberincident is afgesloten, kunt u belanghebbenden hierover informeren. Waak erover dat u niet te voorbarig bent met uw communicatie: er bestaat altijd een kans dat iets over het hoofd is gezien en een herhaling van het incident mogelijk is.
4. **Deel de geleerde lessen**
   - Voor het opstarten van uw dienstverlening heeft u zonder meer computersystemen nodig. Het wordt ten zeerste aanbevolen om de geleerde lessen te delen met andere lokale besturen, organisaties en overheden. Op deze manier kunnen toekomstige incidenten mogelijk vermeden worden en gaat waardevolle rapportering niet verloren. Contacteer ook zeker het Cyber Response Team voor Lokale Overheden (Vo-CRT) voor het delen van de geleerde lessen. Zij zorgen er dan voor dat de beschikbare informatie via een centraal platform gedistribueerd wordt.

Samenvatting van de 5 fases: een cybercrime draaiboek

	FASE 1 DETECTIE EN ANALYSE	FASE 2 SCHADEBEPERKING EN BESTRIJDING	FASE 3 REMEDIERING EN HERSTEL	FASE 4 KENNISGEVING	FASE 5 AFSLUITEN INCIDENT EN OPVOLGING
GOEDE PRAKTIJKEN	• Communiceer direct en escaleer waar nodig • Onderzoek melding en verzamel bewijs • Communiceer intern en plan een crisisvergadering • Maak een initieel plan van aanpak en schakel externe hulp in	• Zet een structuur op voor crisiswerking • Rust het crisisteam uit en maximaliseer de capaciteit • Start de crisiscommunicatie op • Neem de nodige technische maatregelen	• Breng de impact in kaart en bereid kritieke processen voor • Stel prioriteiten voor heropstart • Bedenk (alternatieve) oplossingen voor processen • Herstel de benodigde systemen	• Meld het cyberincident bij de juiste instanties • Informeer de slachtoffers van datalekken • Registreer de gedane meldingen	• Archiveer bewijsmateriaal en breng de impact in kaart • Evalueer de crisisaanpak en implementeer oplossingen en maatregelen uit evaluatie • Plan afsluitende communicatie • Deel de geleerde lessen
GELEERDE LESSEN USE-CASE	• Gebruik de (meest) geschikte communicatiekanalen om verdachte situaties en incidenten te melden, zowel tijdens als na de kantooruren en zorg dat iedereen deze communicatiekanalen kent • Overhaast of uit emotie handelen leidt niet altijd tot de meest optimale oplossing	• Neem de tijd om nieuwe hardware en systemen aan te kopen. • Neem niet enkel levertijden, maar ook duur voor de configuratie van hardware en systemen mee in de verwachte hersteltijden • Zorg voor offline en fysieke versies van belangrijke documenten	• Investeer vooraf in een BIA en BCP • Denk in oplossingen (bijv. betrek buurgemeentes bij het opstellen van continuïteitsmaatregelen) • Zorg voor veilige back-ups	• Win juridisch advies in voordat u de slachtoffers van een datalek informeert • Zorg dat communicatie naar de belanghebbenden (bijv. burgers, pers, enz.) op voorhand bepaald zijn	• Deel altijd de geleerde lessen: de cyberveiligheid van lokale besturen is iets waar we samen aan moeten werken!

Kennisartikelen om te helpen bij (de voorbereiding op) cyberveiligheidsincidenten

- Een goede voorbereiding is **essentieel om snel te kunnen handelen** als er zich een cyberveiligheidsincident voordoet. Hieronder vindt u documentatie die u kan helpen bij deze voorbereiding.

- **Relevante kennisdelingsartikelen op** Cyber Response Team - Digitaal Vlaanderen
  - Asset- en configuratiebeheer
  - Crisiscommunicatie voor lokale besturen
  - Kwetsbaarhedenbeheer
  - Security Information Event Management (SIEM)
  - Wachtwoordbeleid
  - Authenticatiebeleid
  - Autorisatiebeleid
- **Vlaamse cyber diensteninventarisatie**
- **Toolkit Cyber Incident Response Plan**

Bedankt voor uw aandacht

Vragen?

cyberresponse@vlaanderen.be

DIGITAAL VLAANDEREN

Vlaamse overheid