netwerk brandweer

Webinar Bedrijfscontinuïteit

Theoretische benadering

David Matthys – Deskundige ICT – Hulpverleningszone Meetjesland

Netwerk Brandweer

- Samenwerkingsverband tussen Vlaamse hulpverleningszones en VVSG als adviseur brandweerzorg voor lokale besturen
- Actieve deelname aan de taskforce Cyberveilige Gemeenten (o.a. rond deliverables bedrijfscontinuïteit en draaiboek cybercrime)
- Geleerde lessen meenemen naar de specifieke werking van de brandweer

netwerk brandweer

Wat is bedrijfscontinuïteit?

- Elke organisatie (in ons geval lokale overheid) is opgericht om zekere strategische en operationele doelstellingen te realiseren. Daartoe ontwerpt zij een bepaalde structuur en werking:
  - taken, activiteiten en processen
  - functies en rollen (menselijke expertise)
  - gebouwen en gereedschappen (o.a. voertuigen)
  - technologie (hier: alles dat elektrisch/elektronisch word aangestuurd)

Wat is bedrijfscontinuïteit?

- Bedrijfscontinuïteit is een maat voor het vermogen van een lokale overheid om haar bedrijfs-kritische activiteiten overeind te houden ingeval van een onverwachte gebeurtenis

- We richten ons m.a.w. op processen die we vooraf en/of op het moment zelf als vitaal kenmerken

netwerk brandweer

Wat is [digitale] bedrijfscontinuïteit?

- Onverwachte gebeurtenis: we spitsen ons hier toe op “cyberincident”
  - toeval (bv. stroompanne door noodweer)
  - ongeluk (bv. netwerkkabel beschadigd door graafwerken)
  - opzet (bv. doelbewuste hacking om criminele of geopolitieke redenen)

- Er werd reeds gewerkt aan bedrijfscontinuïteit n.a.v. de pandemie

netwerk brandweer

Waarom bedrijfscontinuïteit?

- Verkleinen van de gevolgen van incident voor diverse stakeholders
  - eigen medewerkers en personeel
  - burgers en bedrijven (ook toeleveranciers!)
  - partnerinstellingen (andere overheidsdiensten)

- Fysieke en/of emotionele schade, besmeurd imago, politiek-bestuurlijke impact, financiële schadeclaims, (straf)rechterlijk onderzoek

- Belang van BESCHIKBAARHEID = BETROUWBAARHEID!

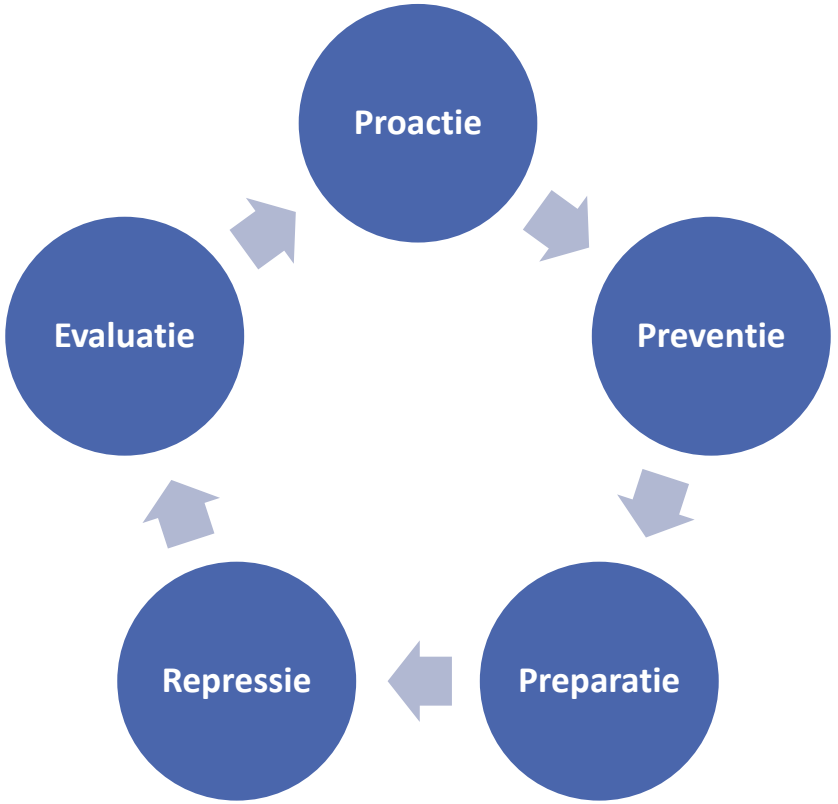
netwerk brandweer

Wie is betrokken bij bedrijfscontinuïteit?

- Ingeval van cyber: ZEKER NIET ALLEEN de ICT-dienst!!! Effectgebied kan de hele organisatie bevatten en zelfs overschrijden
- Voor instandhouding van bedrijfs-kritische activiteiten: proceseigenaren
- Voor een snelle en goede respons: mensen met beslissingsbevoegdheid
- Vaak vergeten: beheren van de communicatie bij een incident of crisis

netwerk brandweer

Hoe pakken we bedrijfscontinuïteit aan?



netwerk brandweer

Veiligheidsketen – proactie

- **DEFINITIE**: wegnemen van structurele oorzaken van onveiligheid

- **TOEPASSING**: uitvoeren van een Business Impact Analyse (BIA) op de bedrijfsprocessen in uw organisatie
  - wat zijn de gevolgen wanneer uitvoering wordt onderbroken of stilvalt?
  - hoe snel moet het proces terug operationeel zijn (RTO)?
  - welke minimale dienstverlening willen we in nood kunnen aanbieden (RPO)?
  - concreet voorbeeld in praktijkdeel webinar

Veiligheidsketen – preventie

- **DEFINITIE**: treffen van maatregelen om noodsituatie te voorkomen of vroegtijdig te stoppen en daarmee ongewenste gevolgen te beperken

- **TOEPASSING**:
  - opstellen van een (informatie)veiligheidsplan
  - treffen van organisatorische en technologische maatregelen
  - sensibiliseren van medewerkers

Veiligheidsketen – preparatie

- **DEFINITIE**: nemen van voorzorgen die een goede reactie op een ramp of crisis mogelijk maken

- **TOEPASSING**:
  - opmaken van crisisplannen en draaiboeken (alternatieve dienstverlening)
  - ontwikkelen van oefenscenario's voor cyberincidenten (1ste keer = nulmeting)
    - ransomware of wiperware op servers met kritieke applicaties en/of data
    - uitschakelen communicatiekanalen door gedistribueerde netwerkaanval

Veiligheidsketen – repressie

- **DEFINITIE**: daadwerkelijk bestrijden van ramp of crisis

- **AANDACHTSPUNTEN**:
  - Gouden “uur”: periode onmiddellijk na het optreden van een incident waarin geboden hulpverlening de grootste invloed heeft op de uitkomst voor een slachtoffer => durf voldoende snel alarmeren en opschalen!
  - Stealing Thunder: zorg dat je als eerste het slechte nieuws bekend maakt aan de buitenwereld

Veiligheidsketen – repressie

- Mogelijke samenstelling van een CMT (Crisis Management Team)
  - IT: schoonmaken en repareren van systemen en applicaties
  - Communicatie: informeren intern, voorlichten extern
  - Operaties: vrijwaren en hernemen van dienstverlening
  - Management: coördinatie en nemen van strategische besluiten
  - Bijkomende sleutelfuncties: functionaris gegevensbescherming (DPO), ambtenaar noodplanning, preventie-adviseur, diensthoofd financiën, diensthoofd facilitair beheer (logistiek)

Veiligheidsketen – evaluatie

- **DEFINITIE**: afwikkelen van de naweeën van een crisis en terugkeren naar de normale modus operandi

- **AANDACHTSPUNTEN**:
  - Wees voorbereid op een lange herstelperiode
  - Heb oog voor de soms traumatische impact van dergelijke gebeurtenissen op uw medewerkers
  - Organiseer een officiële debriefing voor alle betrokkenen. Wat ging er goed? Waar kunnen we nog winst op boeken?

netwerk brandweer

Wat hebben wij hier zelf uit gehaald?

- Begin met een (sterk) beperkte set van processen om de complexiteit in het begin onder controle te houden
- Werken in sprints of iteraties is zeker aanbevolen
- Kennisnetwerken vormen de ware kracht om te komen tot weerbare organisaties