intermedius

Bevindingen Berenschot

Op basis van het **Bedrijfscontinuïteitsplan Cyber** van de gemeente **Utrechtse Heuvelrug**.

Tijdslijn

Medio 2024 heeft Berenschot een cyberoefening georganiseerd.

Adviezen hieruit voortgekomen voor **BCM-vorming** voor deelnemers.

Gemeenten moeten hun IT-huishouding eind 2026 op orde hebben.

Vanuit de Projectgroep Cyber is o.a. gestart met BCP’s opstellen.

Dit wordt vanuit een vast format gedaan.

Berenschot heeft een **expert review** gedaan op het BCP van de GUH.

Belangrijke punten Berenschot

- **1)** Het BCP is zeer uitgebreid en systematisch opgebouwd en biedt goed inzicht in risico's, effecten en waarborging van kritische bedrijfsprocessen.
  - Review nieuwe en bestaande contracten met **leveranciers** – hoe hebben zij hun **beheersmaatregelen** ingericht?
  - Ontwikkel **herstelstrategieën** per kritisch bedrijfsproces.
- **2)** Het BCP is erg tekstueel ingericht en behoeft meer visuele ondersteuning om tijdens een verstoring echt bruikbaar is.
- **3)** Het BCP hangt goed samen met andere documenten, maar dit benadrukt ook het belang van goed documentenbeheer.
  - Zorg voor **één centraal crisisorganisatieplan**! Verwijs dan vanuit o.a. de BCP's en de Communicatieplannen naar dit centrale plan.

Belangrijke punten Berenschot

- **4)** Het BCP is heel erg IT-gericht, terwijl bedrijfscontinuïteit ook door andere aspecten kan worden beïnvloed.
  - Overweeg ook het schrijven van BCP's voor **andere bedrijfscontinuïteitskwesties**, zoals een pandemie, elektriciteitsuitval, en personeelstekorten.
- **5)** Het is onvoldoende duidelijk of het BCP onderdeel uitmaakt van BCM.
  - Idealiter start je met het **vormgeven van BCM-beleid**. Eerst ambitieniveau beschrijven, eigenaren toewijzen en doelstellingen formuleren. Het BCP hoort vervolgens hier op **voort te bouwen**. Zo is het BCP sterker verankerd binnen BCM.
- **6)** Het BCP hanteert bepaalde criteria om te omschrijven of een bedrijfsproces kritisch is. Maar welke prioritering hanteert een gemeente hierbij zelf?

Conclusie Berenschot

Het BCP bevat in de kern **de meeste ingrediënten** in lijn met de ISO 22301 om in de toekomst **te (gaan) voldoen aan de belangrijkste eisen** uit de Cyberbeveiligingswet en de Wwke. Het plan is **uitgebreid**, gaat uit van een (vooralsnog) impliciete dreigings- en risicoanalyse, benoemt continuïteitsmaatregelen en beschrijft de relatie met de (crisis)organisatie in het geval van situaties die de bedrijfscontinuïteit overschrijden. Daarnaast besteedt het BCP aandacht voor meldprocedures bij verstoringen op de bedrijfscontinuïteit, waarmee invulling wordt gegeven aan de **meldplicht** zoals vereist in beide wetten. Hiermee kan het BCP, met inachtneming van het opvolgen van de genoemde aanbevelingen, **een solide basis** gaan vormen voor compliance met de toekomstige wettelijke kaders.