PVO / Limburg

Back on track Inventarisatie:

Snel (weer) doordraaien in het geval van een cyber / IT calamiteit

1 **Welke IT-systemen en/of software zijn essentieel?**

2 **Welke risico's loop je als deze (langdurig) niet beschikbaar zijn?**

3 **Welke afdeling(en) en/of personen zijn hiervoor verantwoordelijk?**

4 **Wat ga je doen als het (toch) misgaat? ***

*Je kunt je niet op alle specifieke scenario's voorbereiden, bekijk op de volgende pagina een aantal zaken die wel preventief kunnen worden opgepakt.

Zaken die preventief kunnen worden opgepakt

1. Bewustwording onder het voltallige personeel, inclusief directie!
2. Laten uitvoeren van de PVO-cyberscan.
3. Vullen van het PVO Back on Track Recoverplan
4. Zorgen voor een veilige meldcultuur, zodat je kan leren van incidenten.
5. Regelmatig oefenen en alle info actualiseren

Back on track: hulp en uitleg bij het invullen van het werkblad.

- **Welke IT-systemen en/of software zijn essentieel?**
  Als je niet weet wat je aan hard- en software in huis hebt, dan wordt het ook moeilijk om te beslissen wat je wil beschermen en wat je minimaal nodig hebt om toch (enigszins) door te kunnen draaien in het geval van een calamiteit.

  Om dit blok in te vullen kan het helpen om te denken in een 'wat als scenario'.
  Voorbeeld: wat als mijn Cloud omgeving niet bereikbaar is (office 365)... Heb ik dan een offline back-up waarop ik kan terugvallen, zodat ik gegevens heb om door te werken?

  Of: kan ik in sommige situaties terugvallen op reservesystemen of 'pen en papier' (analoog) om door te draaien. Denk aan een fysiopraktijk met een computerstoring, maar die wel patiënten wil kunnen behandelen. Of een garagist die zijn werkplaats wil door laten draaien.

- **Welke risico's loop je als deze (langdurig) niet beschikbaar zijn?**
  De risico's die je loopt, verschillen heel erg per organisatie. De ene zal relatief weinig risico lopen en toch wel doordraaien, terwijl de andere meteen moet gaan nadenken over zaken als reputatieschade, financiële schade, verlies van data etc. Hoe meer risico's je in kaart weet te brengen, des te meer oplossingen je kunt toepassen.

- **Welke afdeling(en) en/of personen zijn hiervoor verantwoordelijk?**
  Misschien ligt het voor de hand om alle kwesties rondom informatiebeveiliging bij IT neer te leggen. Dat is echter niet realistisch, want informatiebeveiliging is meer dan alleen IT. Voorbeeld: het voldoen aan geldende wet- en regelgeving en/of internationaal geaccepteerde standaarden (NIS2/ ISO) vereist misschien ook een blik van een juridisch medewerker en/of beleidsmedewerkers etc. Wie bepaalt de budgetten etc.?

  Als taken, verantwoordelijkheden en bevoegdheden (TBV's) niet duidelijk zijn, kun je elkaar ook niet aanspreken op het nemen van (of gebrek aan) verantwoordelijkheid en de acties die daarbij horen. Voorkom dat mensen in een crisissituatie vooral naar elkaar wijzen met als gevolg dat actie uitblijft, of dat genomen actief niet effectief zijn.

- **Wat ga je doen als het (toch) misgaat?**
  Een ongeluk overkomt je altijd op het moment dat je deze het minste kan gebruiken. Het laatste wat je dan wil is dan pas gaan nadenken over 'Wat nu?!' Natuurlijk ga je IT bellen, maar dan ben je er nog niet. Hoe informeer je medewerkers en klanten? Wat vertel je wel en niet? Wat doe je als de pers je vragen gaat stellen? Heb je een lijst van belangrijke nummers uitgeprint?

  Alles wat je hier opschrijft kun je uiteindelijk gaan verwerken in het calamiteitenplan en het recoverplan.