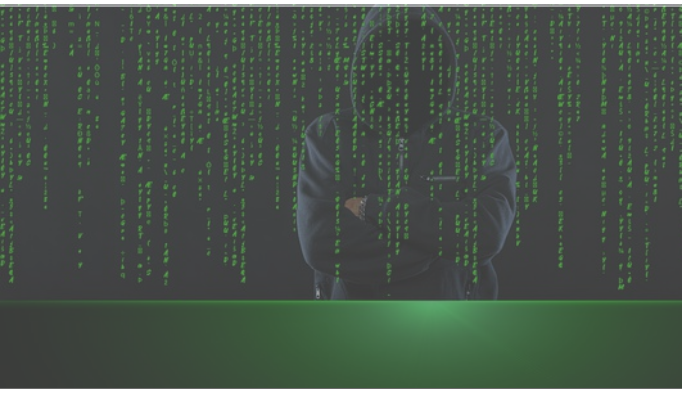
Gids
Crisisteamoefening Cyberaanval

controllit
Business Continuity Management

Inhoudsopgave

Inleiding



Koppen als "Cybercriminaliteit", "2 miljoen klantgegevens gelekt", "Hackersaanval legt bedrijf wekenlang lam" verschijnen herhaaldelijk in de media. Ondanks alle risicobeperkende maatregelen en bedrijfsvoorzorgsmaatregelen doet dit scenario zich ook in Duitsland meerdere malen per jaar voor, met schadebedragen die in de miljoenen lopen.

Is uw bedrijf op dit scenario voorbereid?

In deze gids voor een crisisteamoefening cyberaanval willen wij de essentiële themagebieden voor een succesvolle aanpak van een dergelijke crisis presenteren. Daarbij besteden wij bijzondere aandacht aan de klassieke doelstellingen van crisisbeheersing:

- **Bescherming van mensenlevens**/schade aan mens en milieu
- **Beperking van de schad Vermijding**/beperking van economische schade, vermijding van imagoschade, vrijwaring van (tijd)kritische bedrijfsprocessen
- **Bescherming van de normale werking** van niet-beïnvloede delen van de installatie

Een ander aandachtspunt is de effectieve en efficiënte samenwerking van de leden van uw crisisteam op basis van de **basistaken van een crisisteam**:

- Identificatie en analyse van crisissituaties
- Vaststelling van een strategie voor crisisbeheersing
- Ontwikkeling van opties voor actie
- Beoordeling van de kansen op succes, risico's en mogelijkheden
- Prioriteiten stellen en beslissingen nemen
- Informatie over genomen maatregelen
- Delegatie en controle van acties
- Evaluatie en herbeoordeling

Preventieve maatregelen

Crisisbeheersing is een reactief proces, maar natuurlijk bereidt u uw crisisbeheersingsorganisatie ook op haar taken voor met preventieve maatregelen.

Hier vatten wij de belangrijkste maatregelen samen vanuit het perspectief van het scenario van de "cyberaanval":

Ga na of alle verantwoordelijke leden van uw crisisorganisatie in staat zijn op te treden en klaar zijn om in actie te komen (bijvoorbeeld door regelmatige opleiding, vergaderstructuur, regelmatige uitwisseling van informatie, bewustmakingsmaatregelen):

- Leden van de crisiseenheid, met inbegrip van hun plaatsvervangers
- Deelnemers op tactisch niveau (afdelingshoofden, enz.)
- Uitvoerders op operationeel niveau (werknemers in de gespecialiseerde diensten)

Maak gebruik van uw systeem voor bedrijfscontinuïteitsbeheer (BCM) wanneer dat is geïmplementeerd:

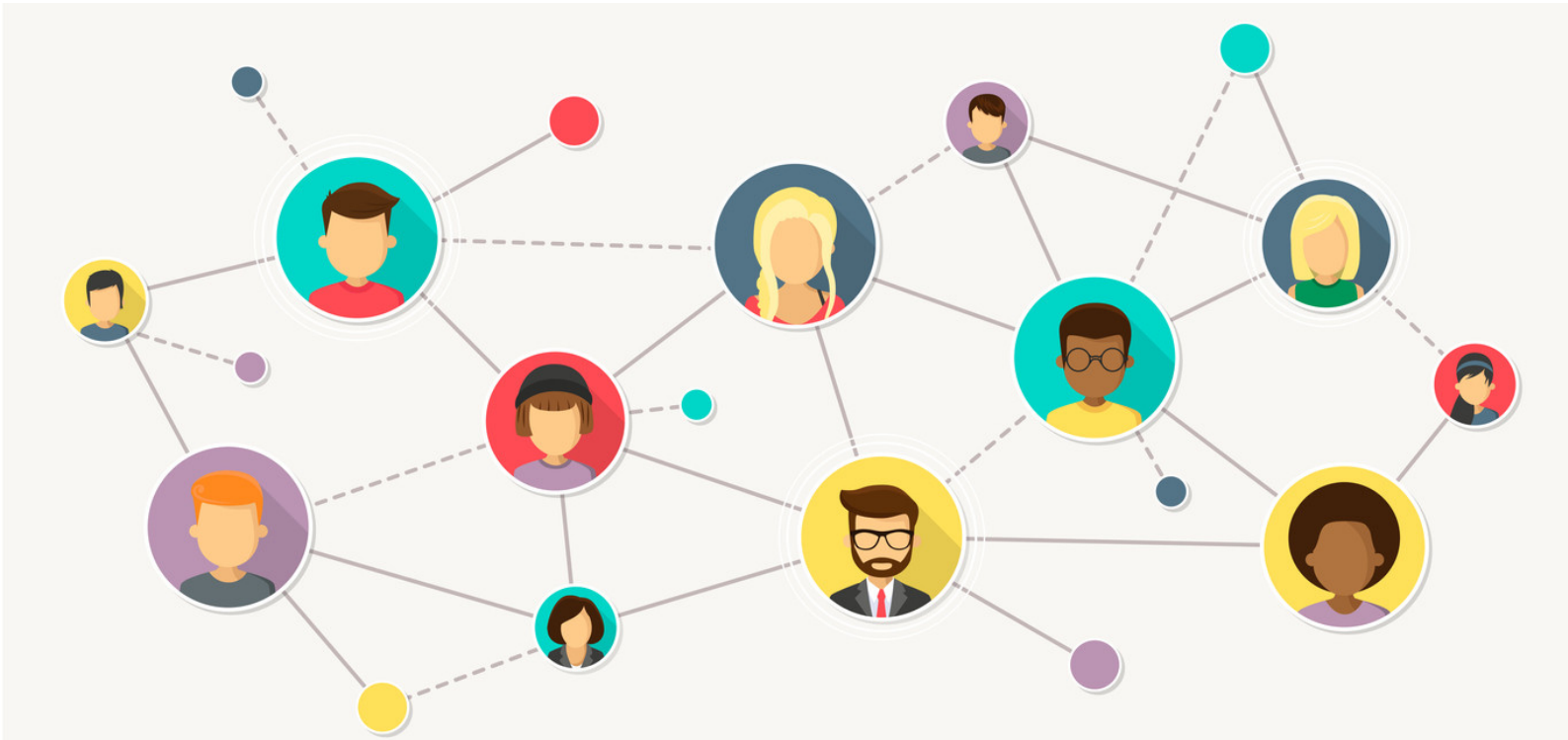
- Beoordelen van de tijdigheid en doeltreffendheid van bedrijfscontinuïteitsplannen voor het scenario van een IT-storing:
  - → Zijn de gebruikte oplossingsopties in staat om bij een IT-storing een storing in een bedrijfsproces tijdelijk te compenseren (met name wat betreft de geïmplementeerde workarounds)?
  - → Zijn uw backupmaatregelen, zoals warm naar koud stand-by enz. doeltreffend en toepasbaar?
- Als u geen BCMS hebt ingevoerd, controleer dan uw operationele capaciteit aan de hand van de volgende onderwerpen

Maak gebruik van uw IT Service Continuity Management System (ITSCM) en Information Security Management System (ISMS) wanneer deze zijn geïmplementeerd:

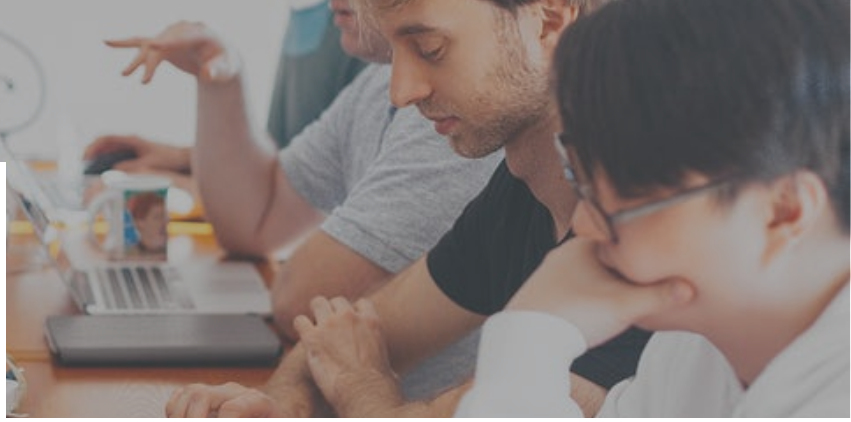
- Zijn de gebruikte oplossingsopties in geval van een IT-storing in staat een storing in een bedrijfsproces tijdelijk te compenseren?
- Kunnen uw IT-doelstellingen, zoals Recovery Time Actual (RTA) en Recovery Point Actual (RPA), worden gehaald?
- Is de beschikbaarheid van IT-diensten voldoende gewaarborgd vanuit het oogpunt van het ITSCM?
- Is het herstel van middelen na een aanval afdoende gewaarborgd in het ITSCM?
- Zijn de beschermingsdoelstellingen van de ISM adequaat gewaarborgd?
- Als u ITSCM en/of ISM nog niet hebt geïmplementeerd, ga dan na of u er klaar voor bent aan de hand van de onderstaande onderwerpen.

Preventieve maatregelen

Gebruik maken van het opzetten en onderhouden door de crisismanager van externe interfaces (hier met name autoriteiten zoals de rijksrecherche (Staatsdienst voor Crimineel Onderzoek, Federale financiële toezichthoudende autoriteit, enz.)



Zorgen voor begrip en bewustmaking en voor procedurele veiligheid met betrekking tot het onderwerp (bewustmakingsmaatregelen)



Reactieve maatregelen

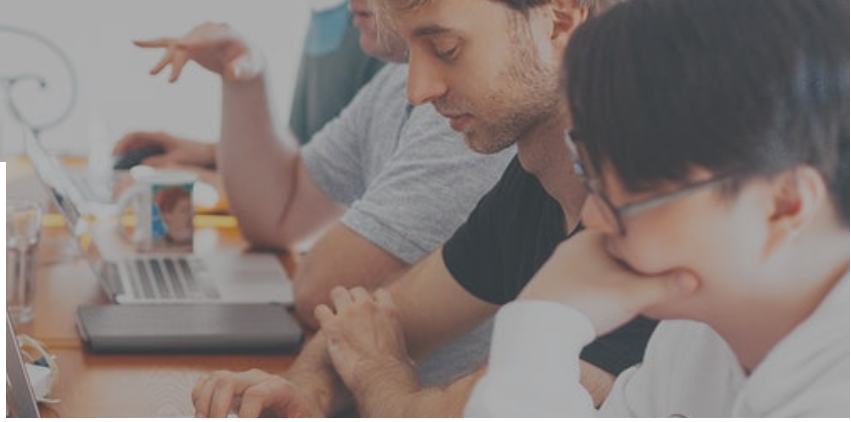
Bij een crisisbeheersingsoefening staan de reactieve maatregelen in geval van een incident op de voorgrond (maar ook als het incident zich daadwerkelijk voordoet). Dit impliceert een ordelijke start van het werk van uw crisisteam, ondersteund door een algemeen overzicht van onderwerpen. De eerste stappen alsmede gedetailleerde punten voor individuele leden van het crisisteam worden hieronder gepresenteerd.

Algemeen overzicht van onderwerpen

In geval van een cyberaanval worden de eerste maatregelen genomen met betrokkenheid van het ITSCM/ISM en, indien nodig, met inschakeling van externe instanties: De nadruk ligt onmiddellijk op schadebeperking en beveiligingsmaatregelen.

Daarnaast zijn de volgende maatregelen en overwegingen van essentieel belang:

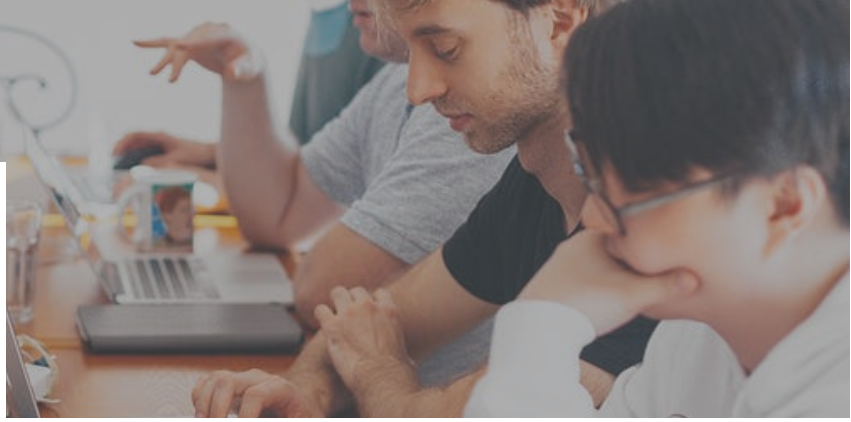
- Neem de volgende punten in acht bij het waarschuwen en het samenstellen van het crisisbeheerteam:
  - → Crisisteamkamer bruikbaar (eventueel gebruik van de alternatieve crisisteamkamer)?
    - Kan uw crisisruimte zelfvoorzienend worden gebruikt met betrekking tot individuele of meerdere IT-componenten?
    - Virtuele instrumenten met verbinding met het bedrijfssysteem zijn waarschijnlijk niet beschikbaar!
  - → Inventarisatie van beschikbare IT-systemen en software (van telefoon tot website tot noodlaptops)
  - → Snelle interne - externe communicatie
    - Eerste info: Bevestiging van het evenement op basis van vooraf vast-gestelde formuleringen (idealiter binnen tien minuten)
    - Bijzondere aandacht moet worden besteed aan de positionering van de onderneming en de externe communicatiestrategie (verantwoordelijk-heid, dader/slachtoffer, enz.).
  - → Vaststelling en afbakening van de huidige en potentiële omvang van de schade (interface ITSCM/IT)
  - → Activering van de BCP's en het IT-herstelplan (indien beschikbaar)
  - → Verkrijgen van goedkeuring van de begroting (indien nodig)



Reactieve maatregelen

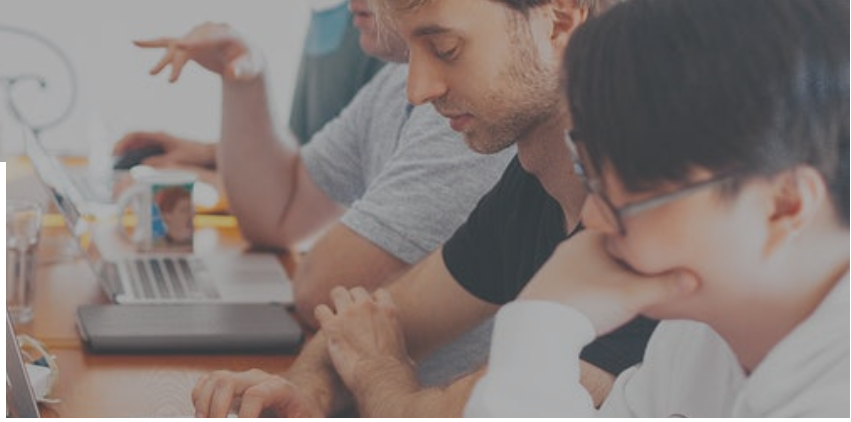
- Let op een dynamische effectcascade (dit is zeer waarschijnlijk): Gewoonlijk ontstaat er een domino-effect binnen IT-systemen.
- Let op het extreem hoge initiële momentum en de waarschijnlijke druk (door de algemene hoge IT-afhankelijkheid) van de chaosfase, vooral in termen van informatie (overvloed en schaarste).
- Uitvoeren van de kerntaken van het initialiseren en waarborgen van noodoperaties.
- Gebruik uw organisatievorm: Is er een bijstands- en serviceteam (AST), een communicatieteam of zijn leden van het crisisteam verantwoordelijk voor een gestructureerde verbinding van de afdelingen?
  - → Wat zijn de rapportage- en informatiekanalen?
  - → Hoe integreert u de interface vertegenwoordigers BCM, ITSCM en ISM in de crisisteam?
- Gebruik de verbinding van de diensten met het bijstands- en serviceteam of het crisisteam voor het bepalen van de situatie::
  - → Welke afdelingen zijn betrokken?
  - → Welke afdelingen kunnen wel/niet werken?
  - → Welke IT-diensten worden beïnvloed?
  - → Van welke IT-diensten kan gebruik worden gemaakt?
  - → Zijn de gegevens van werknemers en/of klanten aangetast?
  - → Welke voorzorgsmaatregelen zijn succesvol/mogen prioriteit krijgen?

- Zorgen voor de informatiestroom en de gecoördineerde verbinding met externe interfaces (bv. autoriteiten zoals Staatsdienst voor Crimineel Onderzoek, Federale financiële toezichthoudende autoriteit), alsook voor de tijdige uitvoering van rapportageverplichtingen:
  - → Indien nodig, integratie van Staatsdienst voor Crimineel Onderzoek of externe deskundigen (bv. IT-forensisch onderzoek) in het crisisteam
  - → Naleving van de rapporteringstermijnen in overeenstemming met de bedrijfs- en sectorvereisten



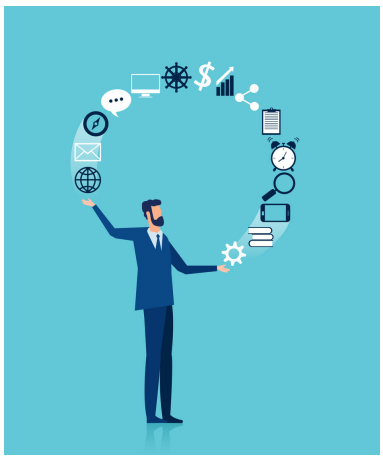
Reactieve maatregelen

- Controle geavanceerde situationeel bewustzijn: gebruik visualisatie voor overzicht!
  - → Interne en externe omvang van de schade: Welke IT-diensten worden getroffen? Welke RTA en RPA zijn momenteel realistisch? Welke gegevens zijn aangetast?
  - → Welke afdelingen zijn betrokken? In het bijzonder: Welke tijdkritische bedrijfsprocessen en welke RTO bestaan er?
  - → Welke afdelingen zijn werkbaar/niet werkbaar? Zijn er bedrijfsherstelopties beschikbaar?
  - → Welke IT-diensten zijn nodig in noodsituaties en zijn bruikbaar/herstelbaar? Prioritering op de tijdlijn?
  - → Verantwoordelijkheid voor de gebeurtenis: eigen schuld/externe schuld/ eerbiediging van de zorgplicht
  - → Overzicht van de maatregelen en statuscontrole
  - → Vaststelling van de oorzaak voor een optimale beperking van de schade (bv. via IT-forensisch onderzoek)
- Gebruik je drempels!
  - → Zijn er drempels vastgesteld en welke drempels worden overschreden? Drempelwaarde mogelijk overschreden voor:
    - IT-storing
    - Mislukte IT-dienstverlener
    - Indien van toepassing, drempelwaarden ITSCM (indien beschikbaar)
- Let op de implicaties voor thuiswerken en werken op afstand
  - → VPN-verbindingen kunnen ook gevolgen hebben voor de privéapparatuur van werknemers (bring-your-own-device).
- Beoordeel de vooruitzichten voor uw crisisteam.
  - → In geval van een IT-storing zal de KS waarschijnlijk langere tijd worden gebruikt (afhankelijk van het type cyberaanval en de wijze waarop deze is afgehandeld)
- Start het herstelproces parallel met de noodoperatie (IT-herstel).
- Controleer uw verzekeringsdekking en meldingsplicht (bv. bedrijfsonderbrekingsverzekering).
- Besteed bijzondere aandacht aan de ondersteuning van de hotlines.
  - → Als de telefonie nog werkt, kan een hoog extra volume worden verwacht (vragen van klanten en media)



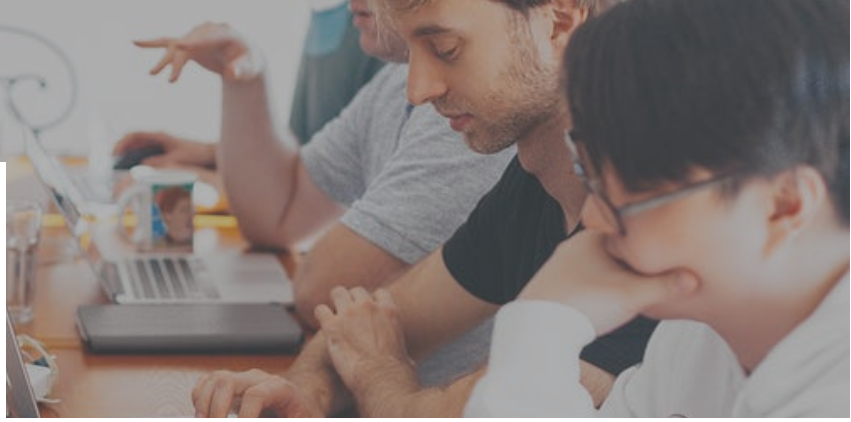
Reactieve maatregelen

Specifieke taken van de leden van de crisiseenheid



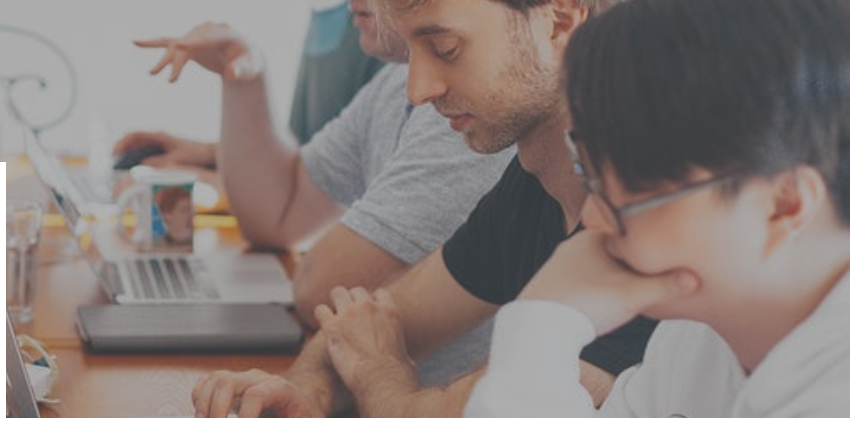
Sommige leden van uw crisisteam kunnen hun taken volgens de checklist in het "cyber attack" scenario verwerken (bijvoorbeeld de functiehouders moderatie, logboekbeheer, visuali-satie, bijstand, juridisch en financieel). In het onder-staande worden de bijzonderheden van de functiehouders met het oog op het scenario "cyberaanval" gepresenteerd:

- **Crisisteamleider:**
  - → Zorgen voor de werkcapaciteit van de crisiseenheid (initieel en periodiek)
    - Integratie van relevante functies en rollen
    - Beschikbaarheid van voldoende middelen (technisch, ruimtelijk, enz.)
  - → Totstandbrenging van een functionerend kader voor samenwerking
    - Schema, briefings, documentatie
  - → Naleven van de rapportageverplichtingen in het kader van de onderneming (zo nodig samenwerken met Legal).
  - → De samenwerking met de autoriteiten actief beheren (indien nodig, integratie van personeel van het Staatsbureau voor Crimineel Onderzoek, IT-forensisch onderzoek).
    - Integratie van leden van de autoriteiten in het crisisteam (indien mogelijk!)
  - → Indien nodig en operationeel beperkt: consolideer de prioritering naar operaties en belanghebbenden
    - Kernactiviteiten/kernprocessen
    - Wat is mogelijk met welke middelen (trefwoord IT beschikbaarheid)?
  - → Controleer of het verstandig is een beroep te doen op deskundigen en dienstverleners
  - → Proactieve informatie verstrekken aan het management/de besluitvormings-autoriteit (DMA) en comités
    - Coördinatie van de informatieverstrekking vóór optredens in de pers (in samenwerking met de voor communicatie verantwoordelijke persoon)
  - → Naleving van FORDEC
  - → Zorg ervoor dat u de actie controleert en een effectiviteitscontrole uitvoert
  - → Houd een oogje op de begroting en de financiële controle
  - → Actief beheren van informatie
  - → Oefen actieve zorg (ook dit scenario kan stressvol zijn).



Reactieve maatregelen

- **Verantwoordelijkheidsgebied Communicatie:**
  - → Nagaan welke media beschikbaar zijn in de huidige situatie (initieel en in de loop van de crisis)
    - Gebruik de beschikbare media (intern, extern, sociale media)
    - Gebruik uw dienstverleners voor communicatie indien nodig
  - → Besteed aandacht aan de consistentie en betrouwbaarheid van uw externe en interne communicatie
    - Eerste info: Bevestiging van het evenement op basis van vooraf bepaalde formuleringen (idealiter binnen de eerste tien minuten).
    - Passende communicatiestrategie (dader/slachtoffer, verantwoordingsplicht, openheid, enz.)
    - Snelle uitbreiding van de communicatie tot alle belanghebbenden
    - Coördinatie binnen crisisteam, met name met IT betreffende verwachte tijdslijnen (actief beheren van interne/externe verwachtingen)
  - → Let op de grote belangstelling voor de verantwoording van het evenement
  - → FAQ's gebruiken en maken (voor interne en externe behoeften)
    - Actief informatiebeheer met de relevante interfaces
  - → Ondersteun uw hotlines (en dienstverleners, indien van toepassing) met formuleringssjablonen om consistente externe communicatie te garanderen



Reactieve maatregelen

- **Verantwoordelijk voor personeelszaken (HR):**
  - → Coördinatie van mogelijke personeelstekorten en -overschotten (flexibele personeelsbezetting):
    - Welke afdelingen hebben behoefte aan personeel?
    - Welke afdelingen kunnen personeel leveren?
    - Over welke vaardigheden beschikken werknemers/hebben ze behoefte aan (actief beheer van vaardigheden)?
  - → Coördinatie van gegevenscontrole en toegangsrechten
  - → Ervoor zorgen dat personeelsdossiers indien nodig beschikbaar zijn voor de crisisteam en anders worden afgesloten (bv. voor interne overtreders).
  - → Coördinatie van het informatiebeheer over de ondernemingsraad/personeelsraad
  - → Advies over overuren en arbeidsrecht indien nodig (handmatige workarounds voor IT-storingen vereisen gewoonlijk meer tijd en personeel)
  - → Betalingsverplichtingen controleren
  - → Gebruik de middelen van uw dienstverleners
  - → Coördineer indien nodig verzoeken om personeelsdiensten
  - → Actief beheren van informatie

- **Verantwoordelijkheidsgebied IT:**
  - → Informeer uw dienstverleners (incl. datacenters)
  - → Verduidelijking van de verantwoordelijkheden binnen IT
    - Gebruik van het IT-noodhandboek
  - → Onderzoek en geef een raming van de omvang van de IT-storing (zie hierboven voor de omvang van de schade).
  - → Ontwikkel een prognose voor de verspreiding van de schade
  - → Opties tonen voor IT-tijdlijnen en herstel
    - Prioriteringsvoorstellen van de kant van IT
    - Let op de prioritering door de crisisteam
    - Prioriteiten van de BCM/ITSCM in acht nemen
    - Integreren van tijd en economische aspecten (haalbaarheid)
  - → Het initiatief nemen tot de uitvoering om de IT-diensten te herstellen
  - → Identificeren en coördineren van redelijke IT-dienstverleners/experts (incl. IT-forensisch onderzoek)
    - voor noodbediening
    - voor herstel
  - → Voer een actief interfacebeheer met ISM, gegevensbeschermingsfunctionarissen
  - → Actief beheren van informatie

Reactieve maatregelen

- **Verantwoordelijkheidsgebied afdeling:**
  - → Controleer de omvang van de schade in uw gebied
  - → Consolideer en communiceer de vereisten in uw gebied (met betrekking tot IT en extra personeel indien nodig)
  - → Herzie en gebruik uw prioritering met betrekking tot de kerntaken
  - → Gebruik en test de functionaliteit en doeltreffendheid van uw overbruggings-maatregelen
  - → Gebruik uw expertise om flexibel en creatief oplossingsmogelijkheden toe te passen
  - → Actief beheren van informatie
    - Richting crisisteam
    - Samenwerking met andere diensten

- **Verantwoordelijkheidsgebied ISM en gegevensbescherming :**
  - → Controleren of beveiligingsdoelen van de ISM worden beïnvloed
  - → de doeltreffendheid van ISM-maatregelen te controleren en deze aan te passen aan de behoeften en in overeenstemming met de wet
  - → Voldoen aan de rapportagevoorschriften op het gebied waarvoor u verantwoordelijk bent en actief informatie beheren met de relevante autoriteiten.
  - → Actief beheren van interfaces met ITSCM, BCM en gegevensbeschermings-functionarissen
  - → Actief beheren van informatie
    - incl. het adviseren van het crisisteam over alle ISM- en gegevensbescher-mingsvraagstukken

Terugkeer naar normale werking en opvolging

De terugkeer naar de normale gang van zaken na de actieve inzet van de crisiseenheid zal de gebruikelijke geplande maatregelen vereisen:

- **Zorg voor terugkeer naar normale werking volgens uw herstelproces.**
  - → Zorgen voor de basisfunctionaliteit van IT-diensten
    - Organisatie van de beveiligde en misschien nog niet volledig beschikbare IT-diensten (b.v. omgaan met prestaties, functie, gebruikersbeperkingen
  - → Gecoördineerde overdracht van werkpakketten aan de gespecialiseerde diensten
  - → Organisatie van de verwerking van de achterstand
  - → ordelijke afwikkeling van de werkzaamheden van de crisiseenheid (met inbegrip van overdracht, informatielijnen, veiligstelling van documenten en dossiers

- **Zorgen voor een gestructureerde follow-up of herwaardering van de gebeurtenissen (lering trekken uit het proces/post-mortem analyse)**

Controllit AG
Kühnehöfe 20
22761 Hamburg
Duitsland
www.controll-it.de

Status: Oktober 2021

Controllit AG is uw partner voor Business Continuity Management (BCM). Sinds onze oprichting ontwikkelen wij integratieve concepten en producten voor Business Continuity Management, IT Service Continuity Management en Crisis Management. Wij helpen u met strategische, organisatorische en technische concepten om uw bedrijfsprocessen te beveiligen tegen bedreigingen en om te voorzien in noodgevallen.

De inhoud van dit document is bedoeld om informatie te verstrekken over virtuele crisisorganisatie. Latere veranderingen mogelijk zijn.

Foto credits: S. 4: iStock.com/alphaspirit; S. 5: iStock.com/alphaspirit; iStock.com/Maike Hildebrandt; iStock.com/tudmeak; S. 7: iStock.com/SurfUpVector; S. 9: iStock.com/Feodora Chiosea; S. 10: iStock.com/ipuwadol

© Copyright Controllit AG