Back On Track – Recoverplan

Een cyberaanval is geen pretje en kan veel schade veroorzaken.

Adequaat handelen helpt om dit te beperken. Daarom deze gids. Vul de gevraagde gegevens in en bewaar dit op een veilige plek. Het liefst digitaal en op papier, zodat je crisisteam er mee aan de slag kan als het nodig is. LET OP: Hou er rekening mee dat de aanvaller anticipeert op de verdediging en dat de crisis langer kan duren. Hou je team dus fit. De situatie is bijna altijd vertrouwelijk en wordt in het geheim afgehandeld. Dit maakt communicatie uitdagend. Stoppen van de aanval is belangrijker dan de dienstverlening herstellen. Het helpt om regelmatig een crisissituatie na te bootsen en te oefenen.

1. Samenstelling Crisisteam (naam en telefoonnummer):

Voorzitter: .....

Logger: .....

Security Officer: .....

Communicatie: .....

Waar nodig aan te vullen met: IT Manager, Jurist, HR Manager, Privacy Officer, Facility Manager. Houd het team zo klein mogelijk!

2. Veilig Stellen:

- Verbreek de internetverbinding (ontkoppel netwerkstekkers en schakel wifi uit)
- Stel de back-ups veilig (bij voorkeur losgekoppeld van het netwerk)
- Zet automatische back-ups uit (om verdere verspreiding van de besmetting te voorkomen)
- Stel alle logfiles veilig (van cruciaal belang voor onderzoek)

3. Communicatie:

Communiceer proactief en blijf beeldvorming de baas.

- Zorg vanuit het crisisteam voor een communicatie expert die integraal verantwoordelijk is voor alle communicatie rondom de crisis
- Forceer alle communicatie in relatie tot de crisis via het crisisteam
- Informeer je medewerkers zodat ze op vragen kunnen reageren
- Zorg voor heldere informatie naar klanten
- Het crisisteam zal intensief samenwerken. Spreek een protocol af en gebruik tools als Signal, Threema of Whatsapp
- Informeer openbare media en voorkom dat ze hun eigen interpretaties geven
- Regelmatige communicatie is essentieel, zelfs zonder ontwikkelingen

4. Externe Hulp:

Er zijn bedrijven die gespecialiseerd zijn in het begeleiden van een cybercrisis. Noteer hieronder de gegevens van een geselecteerd bedrijf. Het is raadzaam vooraf afspraken te maken. Veel cyberverzekeraars hebben overigens al afspraken met dergelijke bedrijven.

Bedrijf: .....

Alarmnummer: .....

E-mail: .....

Uurtarief: .....

Responstijd: .....

! Belangrijke Informatie

Kritische Bedrijfsprocessen:

Bedrijfsproces: Verantwoordelijke:

Telefoon: Betrokken essentiële leveranciers:

Bedrijfsproces: Verantwoordelijke:

Telefoon: Betrokken essentiële leveranciers:

Bedrijfsproces: Verantwoordelijke:

Telefoon: Betrokken essentiële leveranciers:

(Denk aan verkoop, productie, HR, etc)

Essentiële Leveranciers:

Bedrijfsnaam: Levert:

Contract eigenaar: Telefoon:

Bedrijfsnaam: Levert:

Contract eigenaar: Telefoon:

Bedrijfsnaam: Levert:

Contract eigenaar: Telefoon:

Belangrijke Documenten:

Naam document: Waar te vinden:

Naam document: Waar te vinden:

Naam document: Waar te vinden:

(Denk aan bedrijfscontinuïteitsplan, incidentmanagementplan, communicatieplan)

5. Scenario's:

Stel 3 scenario's op en werk deze jaarlijks bij.

- **Positief scenario** (de dienstverlening komt weer terug zonder al te veel impact en de kosten blijven beperkt)
- **Gemiddeld scenario** (er is flinke impact en de duur van de crisis is enkele dagen tot weken. Uiteindelijk kan alles hersteld worden ondanks de hoge kosten)
- **Slechtste scenario** (de impact is zo groot dat herstel niet meer mogelijk is door verlies van kritische data en de dienstverlening ligt vele weken stil)

6. Verzekering:

Er zijn verzekeringen die de kosten van een cybercrisis dekken. Overweeg of dit zinvol is voor je. Zo ja, noteer hieronder de gegevens:

Naam verzekeraar: .....

Alarmnummer: ..... E-mail contactpersoon: .....

Eigen Risico: ..... Externe hulp: ..... NEE / JA (vul dan gegevens in onder 4)

7. Melding Incident:

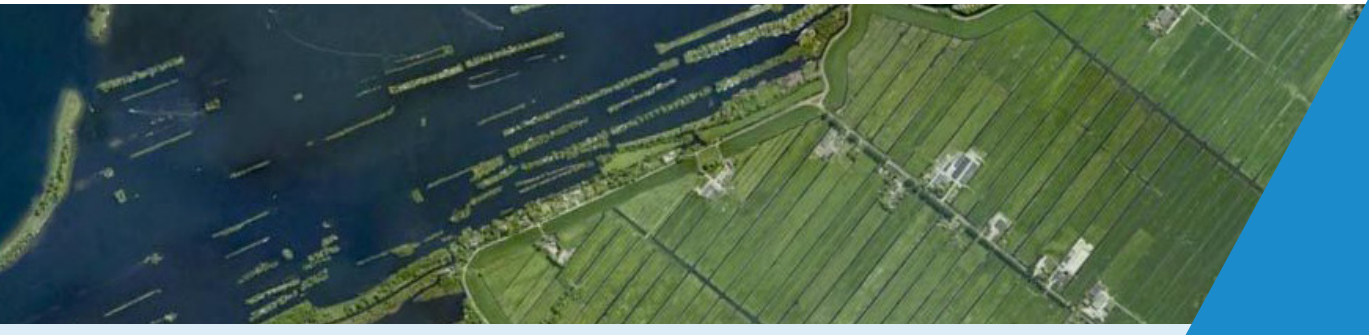
Vanuit verschillende wetten is het verplicht een privacy of cyberincident te melden. Vul aan waar nodig:

- Datalek (moet binnen 72 uur na ontdekken): www.autoriteitpersoonsgegevens.nl/datalek-melden
- Cyberincident (voor vitale organisaties, zo snel mogelijk): www.ncsc.nl/wbni-melding-doen
-
-

8. Vastlegging:

Tijdens een crisis gebeurt er veel in korte tijd. Het vastleggen van beslissingen, acties en andere zaken helpt. Enkele tips:

- **Wijs een logger aan** (is primair verantwoordelijk voor de vastlegging en bewaakt meestal ook acties en regelt overleggen)
- **Gebruik een centraal logboek** (een centraal logboek verhoogt de efficiëntie. Alle leden hebben toegang en zo is er maar 1 waarheid en ook een log van acties en voortgang. Kan digitaal of fysiek)
- **Feiten vastlegging** (leg elke relevant feit vast, hoe klein ook. Zet er het tijdstip van vastlegging bij)
- **SMART acties** (de logger zorgt er voor dat acties specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden worden vastgelegd)
- **Maak een tijdslijn** (zorgt ervoor dat het verloop van de crisis chronologisch te volgen is)



Tot slot:

Altijd doen:

- Kom op vaste tijden bij elkaar
- Gebruik een vaste agenda (zie hierna)
- Hanteer de BOB-methodiek (beeldvorming, oordeelsvorming, besluitvorming)
- Onderhoud de scenario's (zie 5) ook gedurende de ontwikkeling van de crisis

Belangrijke besluiten:

- Wel of niet uitzetten van niet besmette systemen
- Wel of niet ingaan op de eisen
- Wanneer starten met herstel

Voor de crisismanager:

- Hoe is de crisis ontdekt?
- Is al bekend wat voor aanval het betreft? (aanval op ketenpartij, DDoS, Datadiefstal, Malware, Ransomware, Cyberaanval)
- Wat is het vermoedelijke motief? (hacktivisme, financieel gewin, diefstal vertrouwelijke data, ontwrichting maatschappij)
- Is er impact op de dienstverlening of wordt die verwacht?
- Zijn er andere issues die tegelijkertijd spelen?
- Wie is er al op de hoogte? (medewerkers, toezichthouder, klanten, leveranciers, media)
- Zijn er andere partijen (zoals ketenpartners) betrokken bij de crisis?
- Hebben andere organisaties ook last van de crisis?

Voorbeeld Crisisagenda:

1. Opening
- aanwezigen/ vergaderafspraken
- agenda
- telefoons op stil en laptop dicht

2. Acties
- vorig overleg/ status

3. Beeldvorming
- belangrijke mededelingen per lid
  > gebeurtenissen en genomen maatregelen
  > reacties via (social) media
  > andere actieve teams

4. Oordeelsvorming
- analyse van de situatie (acute situaties, extra teamleden nodig)
  > crisisdiagnose
  > doelstellingen en uitgangspunten

5. Besluitvorming
- vaststelling
- acties

6. Communicatie
- intern en extern

7. Sluiting
- vaststelling tijd volgende vergadering