

Wat te doen bij een **hack of ransomware?**

- 1** Zorg voor continuïteit van de belangrijkste dienstverlening. → Lees wat u moet doen in uw *bedrijfscontinuïteitsplan*.
- 2** Los het incident op en herstel de schade. → Lees in uw *Incidentmanagementplan* hoe u dit aanpakt.
- 3** Zorg voor goede interne en externe communicatie. → Werk volgens de aanpak in uw *crisiscommunicatieplan*.

Leveranciers

Leveranciers

Noteer hier de locatie van contactgegevens van en afspraken met de security-contactpersonen van uw leveranciers & dienstverleners.

Netwerk & Storage	Locatie documenten
Burgerzaken	
Website / Hosting	
Zaaksysteem	
Databases	

Incident Response

Noteer hier de contactgegevens van de partijen die u nodig heeft bij de bestrijding van een incident. Noteer ook de afspraken over reactietijden en kosten of geef de locatie aan van het overzicht.

Incident Response		
Data Recovery		
Digitaal Forensisch Onderzoek		

Rollen Crisisteam

	Naam	Telefoonnummer
Voorzitter		
Vastleggen acties / Notulen		
Technisch advies		
Beveiligingsadvies		
Privacyadvies		
Communicatie / Woordvoering		
Aansturing ICT-intern		
Aansturing Leveranciers		
Juridisch advies		
Overig: oa domeinadvies		

Zorg voor een *app-groep* met de belangrijkste stakeholders

Belangrijke documenten

	Datum actuele versie	Fysieke locatie
Bedrijfscontinuïteitsplan(en)		
Incidentmanagementplan		
ICT Crisiscommunicatieplan		



De 7 gouden regels

1. Zet de apparatuur **niet** uit
2. **Verbreek** de netwerkverbinding
3. Stel de **back-ups** veilig
4. Zet de automatische back-ups **uit**
5. Stel **logfiles** veilig
6. **Informeert** interne organisatie
7. **Documenteer** genomen stappen



Let op: nieuw telefoonnummer IBD
070 204 55 11

Wat doet de IBD?

1. **Telefonische ondersteuning**
 - Advies techniek en proces
 - ondersteuning communicatie/woordvoering
 - privacyadvies
2. Online **deelname crisisteam** als adviseur
3. **Schakelpunt** met rijksoverheid, leveranciers en gemeenten
 - advies en waarschuwing
 - inzet netwerk VNG(-bestuurders)
4. **Bemiddeling** capaciteit en steun andere gemeenten (gemeentelijk responsnetwerk)
5. **Second opinion** op adviezen en voorstellen derden
6. Hulp bij **evaluatie** en opstellen lessen voor de toekomst

Aandachtspunten

- Maak afspraken over **opschaling/afschaling** en over het **informeren** van bestuurders
- Maak gebruik van de kennis en kunde van de **veiligheidsregio** bij crisismanagement
- Sluit aan bij de **faciliteiten van de reguliere crisisstructuur**. Denk aan ICT-middelen, aflossingsprotocollen, catering
- Aarzel niet om de **hulp van andere gemeenten** in te roepen, de IBD kan hierin bemiddelen

Rol directie (koude fase)

- Bewaakt ieder halfjaar **paraatheid** organisatie
- Bewaakt ieder kwartaal **preventieve maatregelen**
- Bewaakt ieder kwartaal **impactbeperkende maatregelen**
- **Rapporteert** aan bestuur

Mindmaps

Voor mindmaps over essentiële maatregelen en processen kijkt u op: www.informatiebeveiligingsdienst.nl/vdw