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

1. Zorg voor continuïteit van de belangrijkste dienstverlening. → Lees wat je moet doen in het **Bedrijfscontinuïteitsplan**.
2. Los het incident op en herstel de schade. → Lees in het **Incidentmanagementbeleid** hoe je dit aanpakt.
3. Zorg voor goede interne en externe communicatie. → Werk volgens de aanpak in het **(Crisis)communicatieplan**.

Leveranciers

Noteer hier de contactgegevens van leveranciers en beheerders van de belangrijkste systemen. Zijn zij ook buiten kantoortijden bereikbaar? Zet dit er duidelijk bij.

Omschrijving	Contactgegevens leverancier
ICT-beheerder	
Leerling Adminstratie Systeem (LAS)	
Leerlingvolgsysteem (LVS)	
Cloudprovider (kan zelfde zijn als ICT-beheerder)	
E-mailprovider (kan zelfde zijn als ICT-beheerder)	
Financieel administratiesysteem	
Personeelsbeheersysteem	

Incidentrespons

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

Cybersecurityverzekering *Het is niet noodzakelijk om deze verzekering te hebben. Als je hem hebt, dan werkt de verzekeraar samen met vaste partijen. Bel de verzekeraar daarom snel na het ontdekken van incident.*	
Incidentrespons *Wie kun je bellen en komt je helpen met technische expertise als een incident plaatsvindt?*	
Dataherstel *Wie gaat je organisatie ondersteunen bij het terughalen en herstellen van verloren informatie/data?*	
Digitaal Forensisch Onderzoek *Wie doet technisch onderzoek naar het incident, vooral bij een hack?*	

Belangrijke documenten

Als er een incident plaatsvindt, gebruik je onderstaande documenten voor houvast. Zorg dat er ook papieren versies beschikbaar zijn en dat je weet waar je die kunt vinden (fysieke locatie).

	Datum actuele versie	Fysieke locatie
Bedrijfscontinuïteitsplan		
Incidentmanagementbeleid		
(Crisis)communicatieplan		

Rollen Crisisteam

Als er een incident plaatsvindt, roept de voorzitter of bestuurder het crisisteam bij elkaar.

	Naam	Telefoonnummer
Voorzitter (bijv. bestuurder)		
Secretaris		
Informatiecoördinator		
Adviseur (crisis) communicatie		
Inhoudelijk expert privacy (bijv. voor melden datalek)		
Inhoudelijk expert cybersecurity		
Inhoudelijk expert ... (bijv. financiën)		
(Juridisch advies)		

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. **Informeer** interne organisatie
7. **Documenteer** genomen stappen

ICT uitbesteed? Bel zo snel mogelijk de ICT-beheerder of leverancier en vraag hen de stappen hiernaast te zetten.

Wat doet School-CERT?

School CERT door Kennisnet in samenwerking met SIVON

1. **Telefonische ondersteuning bij incidenten**
   - Advies techniek en proces
   - Ondersteuning communicatie/woordvoering
   - Privacy-advies
2. Online **deelname crisisteam** als adviseur
3. **Schakelpunt** met andere cybersecurity-experts, leveranciers en scholen
4. **Duiding, advies en waarschuwing** (School-CERT Sector Alerts)
5. Hulp bij **evaluatie** en opstellen lessen voor de toekomst

Bel met School-CERT: 0800 321 22 33 (onder kantoortijden)
Of mail naar: support@kennisnet.nl

Aandachtspunten

- Informeer direct de bestuurder bij een incident, die is eindverantwoordelijk.
- Kom bijeen met het crisisteam en zorg dat er één gedeeld beeld is, neem besluiten over de taakverdeling.
- Informeer medewerkers over de situatie en geef direct aan wat ze met ouders, leerlingen etc. kunnen delen.
- Informeer leerlingen en ouders over de situatie en de impact op de continuïteit van onderwijs. Geef ook procesinformatie, wanneer kunnen ze een update verwachten?
- Onderschat de emotionele impact van een incident niet, kijk naar elkaar om en hou in gaten of het te veel wordt voor iemand.

Deze meterkastkaart is onderdeel van het ondersteuningsaanbod bij het Normenkader IBP (versie 1.0).

Bit by Bit – Samen voor digitaal veilig onderwijs

Kennisnet