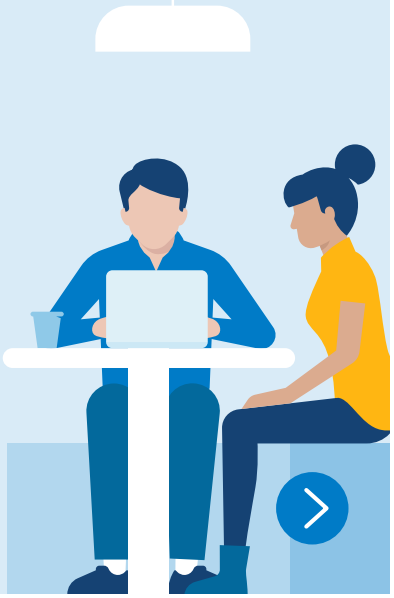
Ministerie van Economische Zaken

Digitale veiligheid
Voorkomen en reageren

Elk bedrijf kan te maken krijgen met een cyberincident. Of je nu een cyberaanval moet afweren of betere afspraken wil maken over je digitale veiligheid, een goed plan is cruciaal. Duidelijke communicatie met je dienstverleners speelt hierbij een grote rol. Deze praatplaat helpt je om samen met je IT-dienstverlener de juiste afspraken te maken. Hieronder vind je twee belangrijke onderdelen die jouw bedrijf weerbaarder maken tegen cyberdreigingen:

Voorkomen: Maak duidelijke afspraken met je IT-dienstverlener over digitale veiligheid en krijg inzicht in:

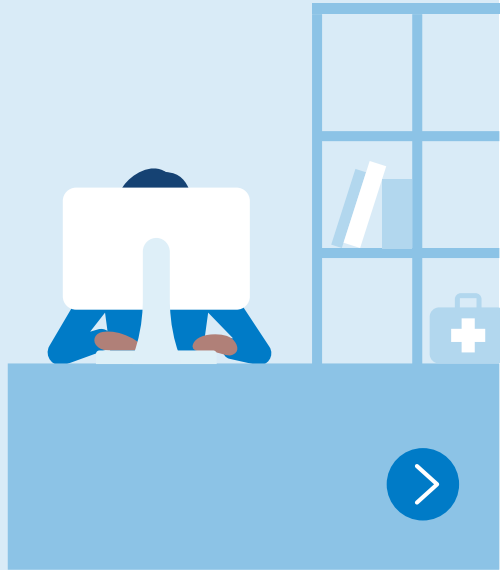
- Afspraken over rollen en verantwoordelijkheden
- De volledigheid van de IT-dienstverlening
- Aanpassingen die gemaakt moeten worden
- Dreigingen en risico's voor jouw bedrijf



In dit document lees je meer over onderwerpen die als leidraad kunnen dienen in het gesprek.

Reageren: Leer in 4 fasen hoe je een cyberincident herkent, aanpakt en herstelt.

1. Voorbereiding
2. Incidentrespons
3. Herstel
4. Evaluatie en oefenen



Lees hier meer over elke fase.

digital trust center.

Bespreek digitale veiligheid
met je IT-dienstverlener

Maatregelen tegen digitale dreigingen

De benodigde digitale veiligheidsmaatregelen kunnen per bedrijf verschillen. Vraag je IT-dienstverlener welke maatregelen zij nemen en waarom. Bespreek in elk geval:

- ☐ **Back-ups: Hoe worden deze beheerd en getest?**
  Een back-up is je laatste redmiddel bij een incident. Zorg ervoor dat deze automatisch wordt gemaakt, veilig wordt opgeslagen (digitaal én fysiek), en snel kan worden hersteld.
- ☐ **Updates: Hoe zorgt je IT-dienstverlener voor tijdige updates?**
  Het tijdig installeren van beveiligingsupdates is belangrijk voor de veiligheid en werking van je software. Bespreek met je IT-dienstverlener hoe zij ervoor zorgen dat alle systemen up-to-date en goed beveiligd blijven.
- ☐ **Wachtwoordbeleid: Welke richtlijnen gelden en is tweefactor-authenticatie ingesteld?**
  Sterke wachtwoorden en tweefactorauthenticatie helpen ongeautoriseerde toegang te voorkomen. Bespreek hoe toegang tot systemen wordt beheerd, ook bij in- en uitdiensttreding van personeel.
- ☐ **Antivirus: Hoe voorkomt je IT-dienstverlener dat computers besmet raken met virussen?**
  Bescherming tegen schadelijke software, zoals malware en ransomware, is essentieel. Bespreek met je IT-dienstverlener welke maatregelen zij nemen en hoe ze dit monitoren.

Resultaat: Basismaatregelen

Inventariseren verantwoordelijkheid

Zorg voor duidelijkheid over wie wat doet en of extra maatregelen nodig zijn.

Breng in kaart:
- ☐ Wat de dienstverlening omvat.
- ☐ Welke verantwoordelijkheden er bij jou liggen en welke bij je IT-dienstverlener.
- ☐ Of de afspraken voldoende zijn om je bedrijf digitaal veilig te houden.

Resultaat: Dienstverlening en verantwoordelijkheden

Rapportage

Vraag je IT-dienstverlener regelmatig om een rapportage van de dienstverlening.

- ☐ Hoe vaak ontvang je een rapportage?
- ☐ Welke maatregelen (back-ups, updates etc.) zijn genomen?
- ☐ Wat is het effect hiervan over tijd?

Deze rapportages helpen je om controle te houden, bij te sturen en beter voorbereid te zijn op toekomstige gesprekken.

Resultaat: Controle en verantwoording

Belangen van jouw bedrijf

Bepaal welke data en bedrijfsprocessen cruciaal zijn.

- ☐ Welke processen en data moeten beschermd worden?
- ☐ Welke risico's zijn hieraan verbonden?

Bespreek dit met je IT-dienstverlener om mogelijke dreigingen in kaart te brengen.

Resultaat: Gezamenlijk beeld van digitale dreigingen

1. Voorbereiding op een incident
Duidelijke afspraken voorkomen chaos

Met je IT-dienstverlener

- ☐ **Controleer de schriftelijke overeenkomst:** Zijn alle punten uit de vorige pagina gedekt?
- ☐ **Maak afspraken ter voorbereiding:** Wie is waarvoor verantwoordelijk tijdens en na een incident?
- ☐ **Bespreek aanvullende diensten:** Heb je extra ondersteuning nodig bij het voorkomen van incidenten, hulp tijdens een incident of begeleiding bij herstel? Bespreek dit met je IT-dienstverlener.

Wees voorbereid! Download en print de bellijst, vul de contact-gegevens in en houd hem bij elke stap binnen handbereik.

Hulp nodig? Bekijk de handreiking voor een incident responsplan.

Rollen en verantwoordelijkheden

- ☐ **Bepaal wie de crisismanager is:** De crisismanager bepaalt het opschalen naar crisisniveau en coördineert de reactie op de crisis.
- ☐ **Bepaal de overige rollen:** Verdeel taken op het gebied van organisatie, techniek en interne -en externe communicatie (klanten, media, belanghebbenden).
- ☐ **Beleg de rollen:** Wijs de rollen toe aan medewerkers binnen het bedrijf.

1

2. Incidentrespons
Herken een incident en handel snel

Stap 1: Interne controle
Hoe herken je een mogelijk incident? Let op ongebruikelijke activiteiten die jij of je collega's opmerken.

- ☐ **Noteer de signalen:** Beschrijf objectief wat ongebruikelijk is.
- ☐ **Vat kort samen:** Leg schriftelijk vast welke signalen erop wijzen dat iets niet klopt.
- ☐ **Gebruik deze bevindingen:** Deze samenvatting helpt bij het gesprek met je IT-dienstverlener.

⚠ *Houd er rekening mee dat een signaal ook van buiten je organisatie kan komen.*

Stap 2: Extern verifiëren
Neem contact op met de IT-dienstverlener die verantwoordelijk is voor de getroffen systemen.

- ☐ **Deel de signalen:** Geef door wat je hebt vastgesteld.
- ☐ **Vraag om advies:** Wat moet je wél en vooral níet doen met je IT-middelen?
- ☐ **Classificeer het incident:** Bepaal samen de impact.
- ☐ **Bepaal de locatie**: Vindt het incident intern of extern (bij een leverancier) plaats?

⚠ *Analyseer samen met je IT-dienstverlener in **welke systemen** deze signalen worden waargenomen (binnen de organisatie, of erbuiten?).*

Stap 3: Zelf in actie komen
Je hebt nu vastgesteld dat er sprake is van een incident, wat ga je nu doen?

- ☐ **Gebruik de voorheen opgestelde rolverdeling:** Wie doet wat?
- ☐ **Alternatieven zoeken:** Kun je bepaalde IT-middelen niet gebruiken? Vind een veilig alternatief.
- ☐ **Communiceren:** Informeer interne en externe betrokkenen.
- ☐ **Melden bij toezichthouders:** Is er een datalek? Meld het direct bij de AP (Autoriteit Persoonsgegevens).

⚠ *Beperk schade. Stop met wat je niet meer kan doen, en bespreek wat wél verantwoord is om door te laten gaan.*

→

3

4

1 2 4

3. Herstel
Blijf in contact bij elke stap

Stap 1: Onder controle
De crisismanager bespreekt met de relevante dienstverleners wanneer het herstel kan beginnen.

- ☐ Ontvang bevestiging dat het incident onder controle is.

Stap 2: Veiligheid voorop
Herstel is belangrijk, maar om veilig te herstellen is het essentieel om te voorkomen dat het incident zich kan herhalen.

- ☐ Overleg of het veilig is om back-ups terug te zetten of dat het veiliger en/of goedkoper is om opnieuw te beginnen.

⚠ *Let op! Hoe oud je back-up is bepaalt hoeveel werk je kwijt bent.*

⚠ *Test je back-ups vóór dat je ze nodig hebt, via de DTC back-up test.*

Stap 3: Stem af
Blijf in contact met je IT-dienstverlener.

- ☐ Stel een herstelplan op waarin staat wanneer en hoe je weer terugkeert naar de normale bedrijfsvoering. Doe dit altijd in overleg met je IT-dienstverlener.

→

1 2 3

4. Evaluatie en oefenen
Blijf verbeteren

Evalueren
Evalueer alle voorgaande punten en kijk na wat je beter kunt inrichten. Herhaal deze cyclus regelmatig in de vorm van een oefening om deze stappen te blijven toetsen.

⚠ *Ga naar de oefenpagina van DTC om te bekijken welke vorm van oefenen bij je organisatie past. Oefen deze oefening met je crisisteam dat je samengesteld hebt. Oefen regelmatig met elkaar om goed op elkaar ingespeeld te zijn.*

Leren van elkaar en het delen van best practices
Deel je ervaringen met anderen en leer van elkaar, bijvoorbeeld binnen je branche of sector, of binnen de keten. Hieronder vind je hulpmiddelen die je kunt gebruiken bij het oefenen en evalueren.

- De DTC website als verzamelplaats van handelingsperspectief.
- De keurmerken van het CCV helpen je bij het kiezen van de juiste cybersecurity producten en diensten.
- De CCRC crisiskaart helpt je op een laagdrempelige wijze bij het voorbereiden op een cybercrisis.