

CYBERNOODPLAN:

Eerste stappen na een cyberaanval

Dit noodplan helpt bij de eerste stappen na een cyberincident.

Hang het zichtbaar op en oefen het periodiek. Zorg ervoor dat er binnen jouw onderneming een aanspreekpunt is voor IT-incidenten.

1. **BLIJF ALTIJD KALM**
2. **ZOEK HULP EN NEEM DIRECT CONTACT OP MET JE ICT-AFDELING OF INTERNE AANSPEEKPUNT VOOR IT-INCIDENTEN.**



1. Isoleer de geïnfecteerde apparaten.

- ✓ Koppel het apparaat direct los van het wifi netwerk. Trek de internetkabel eruit of zet de Wifi verbinding uit. Het doel is om geen connectie meer te hebben met het netwerk en het internet.
- ✓ Let op: Schakel de stroom niet uit! Laat de computer dus aanstaan! Zonder stroom verlies je mogelijk nuttig bewijsmateriaal.
- ✓ Verwijder externe harde schijven en USB-opslagmedia.



2. Meld z.s.m. het incident intern.



3. Betaal geen losgeld. Betalen lost het probleem nooit direct op en stimuleert computercriminelen om meer aanvallen uit te voeren.

- ✓ Aan de IT-afdeling of interne aanspreekpunt voor IT-incidenten
- ✓ Informeer relevante medewerkers en managers.
- ✓ Noteer datum, tijdstip en activiteit.
- ✓ Maak een foto of screenshot van de melding.
- ✓ En bewaar deze informatie voor politie-aangifte die later gedaan moet worden.



4. Laat het melden aan externen over aan de IT-afdeling of aan andere afgesproken personen. Die nemen contact op met:

- ✓ Jullie IT-bedrijf of cybersecuritybedrijf.
- ✓ Politie voor aangifte.
- ✓ Digital Trust Center (DTC) voor algemene cyberincidentinformatie.
- ✓ Vitale aanbieders moeten inbreuken en incidenten melden aan het Nationaal Cyber Security Centrum (NCSC) en hun toezicht-houder. Kijk bij meldplicht op www.ncsc.nl



5. DE IT-afdeling kijkt of er een decryptietool beschikbaar is.



6. Laat een cyberbeveiligingsspecialist de systemen onderzoeken.

- ✓ Bezoek de website No More Ransom en check of er een oplossing is voor de ransomware-variant.
- ✓ Let op: gebruik alleen tools van betrouwbare bronnen.
- ✓ Herstel systemen alleen met schone back-ups.

WAAR KAN IK TERECHT NA EEN CYBERINCIDENT?

Belangrijke contactpersonen

(Voeg hier specifieke interne nummers toe)

- IT-afdeling: (0165) 582 999

.....
• IT-leverancier: Jetron ICT

.....
• (Cyber)verzekeraar:

.....
• Cybersecurityspecialist:

Belangrijke externe contacten

- Politie (aangifte cybercrime): **0800-8844**
- NCSC (voor vitale aanbieders en overheden): **075-751 55 55**
- DTC (voor alle bedrijven die geen aanbieder zijn, incl. zzp'ers) op: **www.digitaltrustcenter.nl**
- Vertrouwenslijn Afpersing: **0800-2800 200**

** Begin 2026 - wanneer het DTC en het NCSC zijn gefuseerd en er nieuwe cyberwetgeving van kracht is - volgt een update van dit plan.*