ADVIESKAART

# BEN VOORBEREID (op een incident)

Februari 2025

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

Een cybersecurity-probleem kan onverwacht en ingrijpend zijn. Met een goede voorbereiding kun je snel en effectief handelen. Deze advieskaart biedt praktische stappen vóór, tijdens en na een incident.

## 1 > HERKEN HET INCIDENT: WANNEER IS HET EEN CRISIS?

Stel duidelijke criteria vast om te bepalen wanneer een incident als crisis wordt beschouwd. Denk onder andere aan datalekken, ransomware-aanvallen of procesverstoringen. Bedenk daarbij de meest voorkomende scenario's waarin het crisisteam moet worden opgeroepen.

Een crisisteam bestaat uit sleutelpersonen die een incident beheersen en oplossen, vaak vanuit IT, security, communicatie, juridische zaken en management.

## 2 > BELANGRIJKE CONTACTPERSONEN: WIE MOET JE BELLEN?

Maak een overzichtelijke en actuele bellijst met essentiële contactpersonen. Denk onder andere aan:

**Crisisteamleden**: Contactgegevens en rollen binnen het team. **IT- en cloudleveranciers:** 24/7 contactpersonen en escalatielijnen. **Forensisch experts:** Voor onderzoek naar datalekken of cyberaanvallen. **Verzekeraars:** Contactpunten voor het melden van schade. **Autoriteiten:** Zoals het NCSC, de Autoriteit Persoonsgegevens (AP) en de politie. **Werknemers:** Interne contactgroepen, bijvoorbeeld via WhatsApp. **Klanten en toeleveranciers:** Voor communicatie over verstoringen.

## 3 > TEST DE BELLIJST: WEES ZEKER VAN BEREIKBAARHEID

Controleer regelmatig de bereikbaarheid van contactpersonen, zowel tijdens kantooruren als op onvoorspelbare momenten (bijvoorbeeld 's nachts). Houd de bellijst actueel en wijs een verantwoordelijke aan voor het periodiek bijwerken van de bellijst. Zorg dat zowel digitale als fysieke kopieën actueel, veilig en eenvoudig beschikbaar zijn.

## 4 > OEFENINGEN EN SIMULATIES: BEREID JE TEAM VOOR

Organiseer realistische oefeningen waarin een crisis wordt nagebootst om verbeteringen te identificeren. Blijf het oefenen herhalen, bijvoorbeeld eens per jaar. Voer na iedere oefening of werkelijk incident een grondige evaluatie uit en kijk onder andere naar:

- Wat ging goed en waar is verbetering mogelijk?
- Welke processen of contactgegevens moeten worden aangepast?

## 5 > LOGGING TIJDENS INCIDENTEN

Houd een gedetailleerd logboek bij tijdens een incident. Noteer de dagen waarop het incident plaatsvond, welke besluiten en acties op welk tijdstip zijn uitgevoerd. Zorg dat het logboek toegankelijk is en achteraf kan worden geëvalueerd.

*i*

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant