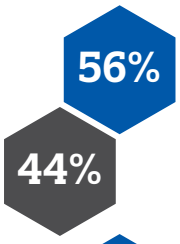
In 4 stappen voorbereid op een cyberincident

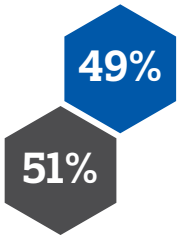
Gebruik onze checklist en blijf een crisis de baas

Hacks, datalekken en andere cyberincidenten zijn een dagelijkse realiteit. Hoe we met dit risico omgaan varieert sterk. Stel er vindt een cyberaanval plaats binnen uw bedrijf. Wat doet u tijdens een cybercrisis? Om de gevolgen te beperken, is het belangrijk dat vooraf helder is hoe u met de belangrijkste dilemma's omgaat.

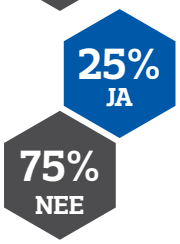
Uit ons **onderzoek** blijkt dat de meningen van professionals verdeeld zijn. Verdeeldheid over dit soort beslissingen kan tijdens een crisis cruciaal zijn.



56% van de respondenten besluit direct alle systemen stop te zetten. Daarentegen vindt **44%** het verstandiger eerst nader onderzoek te laten doen door specialisten.



Ook op het gebied van communicatie zien we verdeeldheid: **49%** geeft aan klanten en leveranciers direct op de hoogte te stellen, terwijl **51%** besluit dit pas te doen wanneer dit echt niet anders kan.



25% betaalt ransom om toegang tot de eigen data terug te krijgen. **75%** betaalt niet.

Niet improviseren maar voorbereiden

We zien in de praktijk dat er tijdens een incident veel wordt geïmproviseerd. Vooral bij het samenbrengen van experts en het bepalen van een aanpak. Een herkenbare aanpak geeft houvast bij een incident. Om schade te beperken betrekt u tijdig de juiste mensen, doorziet u de te nemen stappen en voert u de mogelijke maatregelen uit. Voorbereiding loont: u versnelt hiermee uw respons en verkleint uw achterstand.

Vier stappen voor een gedegen aanpak

1. **Koers bepalen:** hoe willen wij omgaan met uitdagingen in een crisis?
2. **Crisisplan opstellen:** sleutelbesluiten identificeren en verantwoordelijkheden bepalen
3. **Organiseren:** formeren van een crisisteam, aansluiten van benodigde expertise en koppelen de disciplines
4. **Voorbereiden:** trainen en oefenen

Wij helpen u graag succesvol te ondernemen

Wij ondersteunen u graag met:

- Het ontwikkelen van een responsplan of crisisplan op basis van interactieve workshops
- Een workshop voor het crisisteam / directie met:
  - bespreking bijzonderheden van een cybercrisis,
  - reflectie op de eigen voorbereiding,
  - meerdere mogelijke scenario's / inzet van onze **serious game**.
- Een interactieve oefening van het crisisteam en eventuele andere aangesloten teams (communicatie, IT / CERT of een operationeel team).

Voorbereiding loont: u versnelt uw respons op een incident en verkleint uw achterstand.

Wilt u meer weten? Neem contact met ons op.

Neem contact op met:

Marco Zannoni
Specialist cybercrisismanagement
+31 (0)6 535 766 37

aon.nl/cybercrisismanagement

Empower Results®

Checklist

Blijf een cybercrisis de baas

Veiligheid en beveiliging

- Wegnemen en beperken van (in)direct gevaar voor mensen en bezittingen als gevolg van het incident.

IT

- Inschakelen aanvullende expertise
- Onderzoeken van de bron van het incident
- Wegnemen van de bron van het incident
- Duiding van de aanval: is het een gerichte aanval of worden zwakheden uitgebuit? Dreigt er een vervolg?
- 'Schoonmaken' van uw systemen en data
- Herstellen van de schade

Communicatie

- Uitwerken scenario's
- Informeren van medewerkers en bieden van handelingsperspectief
- Informeren en/of waarschuwen van uw klanten en leveranciers
- Informeren van alle belanghebbenden
- Informeren van en contacten met media
- Monitoren van en omgaan met sociale media

Juridisch en financieel

- Betrekken privacy officer en melden incident bij autoriteit persoonsgegevens
- Aangifte doen bij de politie
- Schade melden bij verzekeraar
- Controleren van contractuele verplichtingen en compliance
- Inzet gespecialiseerde advocaat
- Vastleggen overwegingen en besluiten

Continuïteit

- Inzichtelijk maken van mogelijke alternatieve werkwijzen (benutten bestaande BCM-voorbereiding)
- Bereikbaarheid en functionaliteit website herstellen
- Live houden van de operatie en productie
- Herstellen/behouden klant- en leverancierscontact
- Bepalen of er verantwoord kan worden opgestart

Monitoren en evalueren

- Alert blijven op nieuwe incidenten
- Monitoren: wat zijn verwachte en onverwachte effecten van de verstoring en/of de getroffen maatregelen?
- Lessen leren van het incident
- Aanpassingen doorvoeren in cyberaanpak en crisisplan

19.0019.01-cyb-incid_checklistV4-zndemail

AON
Empower Results®