# Cybercrisismanagement

Voorbereiding en duidelijke rolverdeling maakt uw organisatie weerbaar

Veel organisaties krijgen er vroeg of laat mee te maken: een cyberincident. Hacks en datalekken zijn inmiddels niet meer weg te denken. Denk aan de hack bij Marriott en de ransomware-attack bij aluminiumproducent Hydro. Maar ook tal van datalekken. Ticktetmaster, Nationale Opera, Privacy Zeker (!), allemaal werden ze slachtoffer. En dit is slechts een fractie.

Een cyberincident is een abnormale IT-/dataverstoring met grote gevolgen voor de strategische doelen, continuïteit en reputatie. Of het nou een Ddos-aanval is, uitval van een IT- toepassing, een datalek of -manipulatie, elke organisatie moet zich goed voorbereiden op een cyberincident.

## Cyberincidenten en gevolgen

De impact van een cyberincident kan fors zijn. Bij de ene organisatie is de impact financieel, bij de ander ligt het meer op het vlak van reputatieschade. Onderstaande situaties illustreren de kwestbaarheden.

- Dienstverlenende organisaties met dataverwerking als core business worden heel direct geraakt in hun organisatiecontinuïteit als de ‘schermen op zwart gaan’.
- Organisaties die productielocaties hebben en/of afhankelijk zijn van logistieke operaties voor aan- en aflevering van goederen zijn daardoor kwetsbaar: Wanneer een van de locaties wordt gehackt en stilvalt, kan dat alle locaties beïnvloeden.
- Organisaties die (privacy)gevoelige data beheren kunnen dubbel worden geraakt. Wanneer deze data bij een datalek of hack op straat komen te liggen, heeft dat voor zowel de organisatie als de klant grote impact.

## De belangrijkste cyberrisico's van 2019

**De experts van Aon Cyber Solutions signaleren verscheidene cybersecurityrisico’s voor 2019:**

### Digitale transformaties

Organisaties zijn steeds afhankelijker van digitalisering. Dit brengt risico’s mee, die eerder niet in beeld waren. Dataopslag, e-mail, facturatie, websitebeheer; overal ontstaan risico’s rondom beveiliging en privacy.

### Cyberincidenten

Zodra een ketenorganisatie slachtoffer wordt van een cyberincident, raakt dat heel de keten. Leveringen die niet aankomen, data die op straat liggen, systemen die geinfecteerd worden.

### De Internet of Things

Veel apparatuur is afhankelijk van een internetverbinding. Als die wegvalt kan dat grote impact hebben. Maar de ‘verbondenheid’ zorgt er ook voor dat u kwetsbaar bent. Veel apparaten gebruiken gestandaardiseerde codes en kunnen daardoor gemakkelijk gehacked worden.

## Het crisisteam: gezamenlijke verantwoordelijkheid

In tegenstelling tot wat veel organisaties denken: de cybersecurity en respons na een hack of datalek zijn niet bij IT belegd. Het is een organisatiebrede verantwoordelijkheid, met één team dat de lijnen uitziet en actie onderneemt: het crisisteam. Wanneer de situatie een crisis dreigt te worden die uw strategische doelen en reputatie in gevaar brengt, is dit team aan zet. Het crisisteam houdt overzicht, neemt de regie en maakt besluiten op basis van ervaring en training. Om dit zo goed mogelijk te kunnen doen, is goede voorbereiding dus essentieel.

>>

‘Grote hack bij Marriott, Hydro slachtoffer ransomware. Datalek bij Ticketmaster. Datalek bij Privacy Zeker. In 2018 zijn er maar liefst 20.881 datalekken gemeld.’

## Wilt u meer weten over cybercrisismanagement?

Wilt u meer weten over cybercrisismanagement of meteen aan de slag? Neem dan contact op met:

**Aon Crisismanagement**
crisis_management@aon.nl

Empower Results®

## Actielijst: waar staat u in uw voorbereiding en respons?

Een goede voorbereiding op mogelijke cybercrises begint bij bewustwording en goede monitoring. Dit doet u door inzichtelijk te maken waar de kritieke punten in uw systemen zitten en een duidelijk crisisplan op te stellen. Op die manier kunt u adequaat reageren op een crisis en de gevolgen beperken. Maar hoe zit het met uw voorbereiding en respons? In onderstaand schema laten wij per thema zien wat de belangrijkste acties zijn ten tijde van een crisis.

### Techniek

- bron incident onderzoeken, bron wegnemen, ‘schoonmaken’ en herstellen;

### Communicatie

- medewerkers, klanten en leveranciers informeren en/of waarschuwen;

### Juridisch en financieel

- incident melden bij autoriteit persoonsgegevens, aangifte doen, melden bij verzekeraar, contractuele verplichtingen en compliance oppakken;

### Continuïteit

- website, operatie en productie live houden, klant- en leverancierscontact herstellen/behouden;

### Veiligheid en beveiliging

- wegnemen en beperken van (in)direct gevaar;

### Monitoren en evalueren

- alert blijven op nieuwe incidenten, lessen leren, aanpassingen doorvoeren.

AON
Empower Results®