Ministerie van Economische Zaken

Bellijst cyberincident

Als je door een cyberincident niet meer bij je bestanden kunt komen, wie moet je dan bellen? Hoe bereik je je IT-support, applicatiebeheerder of webhost? En wie moeten er van de situatie op de hoogte worden gesteld? Belangrijke leveranciers, opdrachtgevers of een cyberverzekeraar? Maak je eigen bellijst voor noodsituaties en print hem uit.

Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Bedrijfsnaam		Referentie	
Contactpersoon		Notities	
Telefoon			

Belangrijke websites en bijv. back-up locaties	

digital trust center.

Ministerie van Economische Zaken

Tips voor optimaal gebruik van de bellijst

Tip 1 Noteer ook contract- of supportnummers

Het kan zijn dat je bedrijfssystemen niet beschikbaar zijn en het is daarom handig om alle benodigde informatie bij een cyberincident al van tevoren op de bellijst te schrijven. Dit kunnen contract- of supportnummers zijn, of technische informatie zoals versienummers. Weet je niet zeker welke informatie nodig is? Neem even contact op met de hulptroepen op je bellijst (IT-support, applicatiebeheerder of webhost) en spreek de procedure door.

Tip 2 Noteer ook ketenpartners

Op de bellijst kun je ook de contactgegevens van andere bedrijven of organisaties noteren die op de hoogte moeten zijn van je IT-verstoring. Denk bijvoorbeeld aan (keten)leveranciers, grote afnemers of belangrijke klanten en een cyberverzekeraar.

Tip 3 Print en plaats de bellijst

Een duidelijke afgesproken plek zorgt ervoor dat de bellijst tijdens een cyberincident snel gebruikt kan worden. Als je een uitwijklocatie hebt, vergeet dan niet om de bellijst ook daar beschikbaar te hebben. Hang de bellijst aan de muur of plak hem aan de binnenkant van een kast.

Tip 4 Maak interne afspraken

Zorg dat alle betrokkenen binnen je bedrijf op de hoogte zijn welke stappen gezet moeten worden bij een cyberaanval of -incident. Dit kun je doen door te oefenen.

Tip 5 Stem af met je IT-dienstverleners

Zorg dat alle betrokkenen binnen je bedrijf op de hoogte zijn welke stappen gezet moeten worden bij een cyberaanval of -incident. Dit kun je doen door te oefenen.

Tip 6 Update de bellijst jaarlijks

Agendeer dat je tenminste één keer per jaar de bellijst controleert. Bekijk hierbij of de lijst nog de juiste persoonsgegevens en contract- of supportnummers bevat. Zijn er systemen of applicaties bij gekomen? Update de bellijst indien nodig. Bij grote veranderingen in IT-dienstverlening van je bedrijf is het aan te raden om de bellijst meteen te updaten.

Waar kun je terecht na een cyberincident?

Doe aangifte bij de Politie
0900 8844
politie.nl/aangifte-of-melding-doen

Meld fraude bij de Fraudehelpdesk
088 786 73 72
fraudehelpdesk.nl

Rapporteer je datalek bij AP
088 180 52 55
datalekken.autoriteitpersoonsgegevens.nl

Vind algemene informatie bij het DTC
digitaltrustcenter.nl