Cyber Weerbaarheidscentrum Greenport

Uitwijk- en herstelplan

Er zijn verschillende soorten incidenten die invloed kunnen hebben op je bedrijfsvoering. Incidenten kunnen variëren van een defecte printer tot een brand in je kantoorpand met mogelijk ernstige gevolgen. Incidenten zijn onverwacht en vinden helaas vaak op het verkeerde moment plaats.

We spreken van een cyberincident wanneer het incident de beschikbaarheid, integriteit of vertrouwelijkheid van informatiesystemen raakt. Hoe kun je je wapenen tegen cyberincidenten? Met een uitwijk- en herstelplan. Zo'n plan maakt dat je beter voorbereid bent en de schadelijke impact op je bedrijfsvoering kunt beperken.

Disaster Recovery Plan

Een uitwijk- en herstelplan wordt ook wel een "Disaster Recovery Plan" (DRP) genoemd. Een DRP is eigenlijk een soort draaiboek dat stap voor stap beschrijft wie wat moet doen om correct en adequaat te reageren op een calamiteit. Het is ontworpen om duidelijke en efficiënte processen aan te reiken met de bedoeling de IT-storing zo snel mogelijk te herstellen en een aanvaardbaar operationeel niveau te bereiken.

In het document hieronder vind je een template wat je kunt gebruiken om voor jouw organisatie een Disaster Recovery Plan op te zetten.

Download het Template voor een Disaster Recovery Plan

Wees goed voorbereid op een cyberincident

Zorg dat je weet wat je moet doen. Als je systemen niet meer te benaderen zijn, wil je kunnen terugvallen op gegevens waar je wel bij kunt. Bekijk de Toolkit Cyberincidenten om handige hulpmiddelen te vinden.

Toolkit Cyberincidenten

Doordenk enkele scenario's om je oplossingen te valideren

Naast het volgen van een template als hierboven kun je ook praktischer te werk gaan. Brainstorm eens over bepaalde risico's die je hebt geïdentificeerd bij het opstellen van je risicoanalyse. Het doorlopen van een mogelijk scenario kan je inzicht geven in mogelijke problemen waar je tegenaan loopt als een risico leidt tot een cyberincident.

Doordenk het scenario eens dat een cyberincident ervoor zorgt dat je volledig terug moet vallen op een back-up. Doet zich dan één van de volgende problemen voor?

- De back-up is correct versleuteld, maar de decryptiesleutel was digitaal opgeslagen en is nu dus alleen nog in de back-up terug te vinden.
- De back-up is voorhanden, maar het blijkt veel te lang te duren om de systemen te herstellen waardoor het bedrijf te lang stil ligt.
- De back-up bevond zich in het bedrijfspand dat is afgebrand en is dus ook verloren gegaan.

- Door een dergelijk scenario eens goed door te denken, kom je snel tot hele praktische verbeteringen in je uitwijk- en herstelplan. Als je de verbeteringen direct test of doorvoert, voorkom je problemen wanneer de situatie zich echt voordoet.

Dit document is gebaseerd op het document 'Uitwijk- en herstelplan' van het Digital Trust Center. Het originele document is te vinden via https://www.digitaltrustcenter.nl/informatie-advies/uitwijk-en-herstelplan