Disaster Recovery Plan

Disclaimer - *Dit document kan gebruikt worden als template voor het opzetten van een Disaster Recovery Plan (DRP) binnen jouw organisatie. De content van dit document bevat een aantal uitgangspunten die je zou kunnen opnemen in je eigen (DRP). Niet alle uitgangspunten zullen van toepassing zijn, maak daarom een eigen afweging om bepaalde uitgangspunten wel of niet op te nemen. Naast de handreikingen in dit document is het belangrijk input te verzamelen van de verschillende afdelingen binnen je organisatie.*

Disaster Recovery Plan

Disaster Recovery Plan definitie: Plan waarin staat hoe het digitale systeem moet herstellen na een grote storing (Cybersecurity Woordenboek).

Doel: een DRP beschrijft een gestructureerde aanpak die gehanteerd wordt:

- wanneer een onvoorzien incident zich voordoet dat de bedrijfscontinuïteit in gevaar brengt,
- om de kans op en de impact van zo'n incident zoveel mogelijk te beperken.

Een DRP is 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.

Disaster Recovery **Plan**

Stap 1: Projectmanagement

De eerste stap in het opstellen van een DRP is projectmanagement.
In deze fase moeten de volgende activiteiten plaatsvinden:

- Support verkrijgen van senior management;
- Project scope definiëren en bijbehorende doelstellingen formuleren;
- Inschatting maken van benodigde resources en capaciteit;
- Opstellen van een planning voor de belangrijkste doelstellingen van het project.

Stap 2: Scope en planning

Het is belangrijk om de scope en doelstellingen van het DRP helder te formuleren. Is het plan alleen van toepassing op de IT onderdelen van een organisatie of is het van toepassing op de gehele organisatie? Gaat het bijvoorbeeld alleen om de technologie in het datacenter of gaat het om de algehele technologie van een organisatie? Daarnaast is een bijbehorende planning onmisbaar.

Een risicoanalyse kan helpen bij het bepalen van je scope. Tijdens een risicoanalyse ga je na wat de impact zou zijn op de business wanneer bepaalde bedrijf kritische applicaties of diensten niet meer geleverd kunnen worden. Om dit te kunnen doen, is het cruciaal om exact te weten welke applicaties en diensten op welke onderdelen van uw ICT-infrastructuur draaien en waar deze zich bevinden.

Stap 3: Uitvoeren Business Impact Analyses

Bij een Business Impact Analyse (BIA) wordt bekeken hoe de verschillende business units werken, welke bedrijfskritische processen afhankelijk zijn van IT en welke gevolgen bepaalde risico's zouden kunnen hebben voor dat specifieke proces maar ook voor de andere bedrijfsactiviteiten.

De risico's die je ziet, rangschik je op prioriteit. Hoe groot is de impact op het bedrijf als risico zich voltrekt? Zo zullen sommige risico's impact hebben op de hele organisatie en andere slechts een klein onderdeel raken. Soms zullen de operationele en financiële verliezen groot zijn, soms is het minder gemakkelijk om de impact te kwantificeren, zoals bij reputatieschade.

Na zo'n BIA-analyse heb je een duidelijk beeld van alle mogelijke gevolgen van een incident voor een bedrijf, zowel de praktische problemen als de mogelijke kosten ervan. Het doel is om te bepalen hoe (in)tolerant de bedrijfskritische applicaties en -diensten zijn voor een mogelijke storing en wat de maximaal aanvaardbare downtime ervan mag zijn.

Daarna kun je de mogelijke opties evalueren om hun resistentie te verhogen en het risico op onderbreking te reduceren.
Dit natuurlijk met de bedoeling om de dienstverlening binnen een aanvaardbare tijdsspanne te kunnen herstellen.

Stap 3: Uitvoeren Business Impact Analyses

Er zijn twee belangrijke berekeningen die gedaan moeten worden bij het opstellen van een BIA.

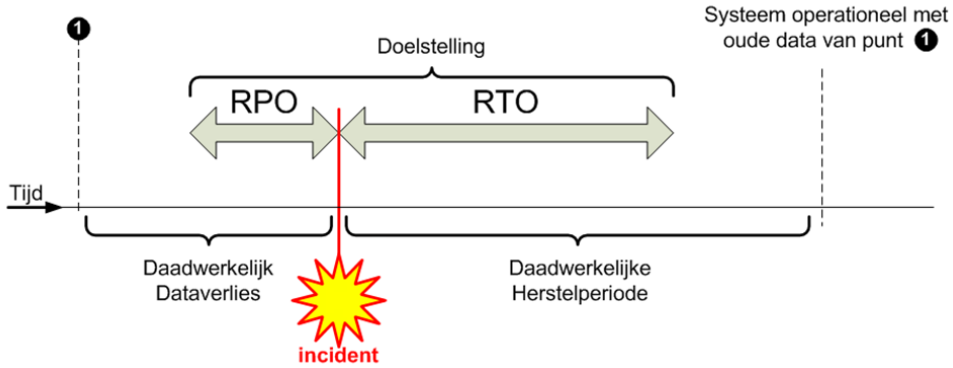
1 Het bepalen van de Recovery Time Objective (RTO)

Recovery Time Objective is de streeftijd waarbinnen een bepaalde functie, proces of dienst opnieuw operationeel moet zijn na een storing, om onaanvaardbare gevolgen voor de bedrijfsactiviteiten te vermijden.

Hierbij is het dus van belang om te berekenen hoe snel je organisatie zich moet kunnen herstellen, en op basis daarvan bepaal je welke maatregelen en budgetten nodig zijn om de bedrijfscontinuïteit zo goed mogelijk te verzekeren.

2 Het bepalen van Recovery Point Objective (RPO)

Recovery Point Objective beschrijft het tijdsinterval dat mag voorbijgaan zonder dat de hoeveelheid verloren data de maximum toelaatbare drempel overschrijdt. De RPO wordt bepaald op basis van de tijd tussen 2 back-ups en de hoeveelheid gegevens die tussen die 2 back-ups verloren zouden kunnen gaan.



Stap 4: Opstellen van een Disaster Recovery Strategie

Na de risicoanalyse, de BIA, het bepalen van de RTO en RPO en het in kaart brengen van het ICT landschap, kun je beginnen om concrete acties en procedures op te stellen waarop je kunt terugvallen wanneer een incident zich voordoet. De belangrijkste elementen die je hierin opneemt, lichten we toe.

1 Rollen en verantwoordelijkheden

Allereerst moet duidelijk opgesteld worden wie wat móet en màg doen in geval van een calamiteit. Dit kun je eenvoudig weergeven in een tabel met:

- De contactgegevens van de verschillende leden van het Disaster Recovery Team;
- De bijbehorende rollen en verantwoordelijkheden per teamlid;
- De beperkingen van hun autoriteit in geval van een incident;
- Uitgavelimieten (bijvoorbeeld als er materialen aangekocht moeten worden).

2 Reageren op een incident

Het DRP legt vast wie van van het Disaster Recovery Team de ernst van de situatie in eerste instantie zal evalueren, het incident onder controle zal proberen krijgen en de nodige contactpersonen op de hoogte zal brengen.

Stap 4: Opstellen van een Disaster Recovery Strategie

3 Activatieplan

Aan de hand van de incidentevaluatie wordt besloten om het DRP (of onderdelen daarvan) te activeren. Het DRP beschrijft gedetailleerd en stap voor stap hoe gehandeld moet worden om het geraakte bedrijfsproces of netwerkelement zo snel en efficiënt mogelijk te herstellen of de taken ervan door een ander systeem te laten overnemen, zodat een normaal operationeel niveau bereikt kan worden.

4 Documentatie

Een DRP bevat naast bovenstaande informatie ook onderstaande elementen:

- Contactgegevens van leveranciers,
- Gekende herstelprocedures beschreven door deze leveranciers,
- Systeem- en applicatie-inventarissen,
- Netwerkbeschrijvingen en -schema's,
- Contracten en Service Level Agreements.

Stap 5: Testen en evalueren

Evenals andere plannen is het belangrijk je DRP regelmatig te testen en te evalueren daar waar nodig. Dit kan bijvoorbeeld het geval zijn wanneer je vaststelt dat de gedefinieerde procedures niet de gewenste resultaten opleveren of de afgesproken RTO en RPO overschrijden.

Naast testen is het jaarlijks updaten van je DRP ook belangrijk. Een DRP met verouderde contact- en contractinformatie is schadelijk omdat er kostbare tijd verloren zal gaan op cruciale momenten. Updaten is ook van belang wanneer je nieuwe activiteiten of diensten aan je organisatie toevoegt. Het loont dan om af te wegen welke impact deze nieuwe activiteiten en of diensten op je DRP hebben en in welke mate het DRP aangepast moet worden.