



Spinware Solutions B.V.
veilig werken met de cloud

Bedrijfscontinuïteits plan

Versie: september 2024



Inhoudsopgave

1. Inleiding.....	3
2. Het bedrijfscontinuïteitsplan	4
2.1. Risicoanalyse en bedreigingen	4
2.2. Kritieke bedrijfsfuncties	6
2.3. Noodhulpteam en verantwoordelijkheden	6
2.4. Herstelstrategieën	7
2.4.1. IT-systemen en datacenter	7
2.4.2. Cyberaanvallen	7
2.4.3. Stroomuitval	7
2.4.4. Klantcommunicatie	7
2.5. Communicatieplan	8
2.6. Test- en opleidingsprogramma.....	8
2.7. Herstel na een ramp.....	8
3. Conclusie.....	9

1. Inleiding

Dit bedrijfscontinuïteitsplan (BCP) is opgesteld om ervoor te zorgen dat Spinware Solutions B.V. in geval van een crisis of onderbreking van de bedrijfsvoering, zijn essentiële diensten en producten kan blijven leveren aan klanten. Dit document beschrijft de procedures, processen en verantwoordelijkheden die in werking treden om de impact van een noodsituatie te minimaliseren.

Het doel van dit bedrijfscontinuïteitsplan is om te verzekeren dat Spinware Solutions B.V. in staat is om snel en effectief te reageren op verstoringen van de normale bedrijfsvoering en om zo snel mogelijk terug te keren naar de normale dienstverlening. Dit plan dekt rampen zoals IT-storingen, cyberaanvallen, stroomuitval, natuurrampen en menselijke fouten.

2. Het bedrijfscontinuïteitsplan

Dit plan omvat alle kritieke systemen, processen en afdelingen van Spinware Solutions B.V., inclusief IT-infrastructuur, datacenterbeheer (Smartdc datacenter i3D.net), netwerkbeheer, klantondersteuning, en communicatie. Het richt zich met name op het waarborgen van de continuïteit van cruciale ICT-diensten en de beschikbaarheid van klantgegevens.

2.1. Risicoanalyse en bedreigingen

De belangrijkste bedreigingen voor de continuïteit van het bedrijf worden geïdentificeerd en geanalyseerd op basis van hun waarschijnlijkheid en impact. De risico's voor Spinware Solutions B.V. kunnen onder andere zijn:

- Cyberaanvallen (bijv. ransomware, DDoS-aanvallen)
- Stroomuitval
- Hardware-uitval (bijv. servers, datacenter, internet, netwerkapparatuur)
- Softwarefouten
- Menselijke fouten
- Natuurrampen (bijv. brand, overstromingen)
- Pandemieën

Deze risico's worden beoordeeld op basis van hun waarschijnlijkheid en de impact op de bedrijfsvoering. Prioriteit wordt gegeven aan de risico's met de hoogste impact.

Spinware Solutions B.V. heeft een uitgebreide risicoanalyse uitgevoerd om de bedreigingen te identificeren die de continuïteit van de bedrijfsvoering kunnen verstoren. Deze analyse omvat de beoordeling van risico's op basis van hun impact en de waarschijnlijkheid dat ze zich voordoen. Hieronder volgen de belangrijkste risico's waar Spinware Solutions B.V. rekening mee moet houden.

	Risico	Concreet voorbeeld	Impact	Waarschijnlijkheid
Cyberaanvallen	Cyberaanvallen, (ransomware en DDoS-aanvallen) kunnen de systemen ernstig verstoren. Aangezien de IT-infrastructuur en klantdata belangrijke assets zijn, vormen aanvallen op deze systemen een significant risico.	Een ransomware-aanval kan klantgegevens en bedrijfsgegevens versleutelen, waardoor Spinware Solutions B.V. geen toegang meer heeft tot essentiële data totdat er losgeld wordt betaald. Een DDoS-aanval kan de netwerkprestaties lamleggen, waardoor klanten geen toegang hebben tot online diensten.	Zeer hoog, met mogelijke reputatieschade, financiële verliezen en verlies van klantenvertrouwen.	Gemiddeld tot hoog, gezien de toenemende cyberdreigingen in de ICT-sector.
Stroomuitval datacenter	Een langdurige stroomuitval kan het datacenter stilleggen, wat invloed heeft op de beschikbaarheid van alle ICT-diensten.	Een regionale stroomstoring die de back-up generatoren van het datacenter overbelast, kan ertoe leiden dat servers niet meer toegankelijk zijn, wat resulteert in uitval van klantendiensten.	Hoog, aangezien het verlies van toegang tot het datacenter betekent dat klantdata en systemen onbeschikbaar zijn.	Laag tot gemiddeld, gezien de redundante systemen en back-up stroomvoorzieningen van het datacenter, maar het risico blijft aanwezig bij langdurige uitval.
Hardware-uitval	Het falen van essentiële hardwarecomponenten, zoals servers of netwerkapparatuur, kan leiden tot onderbreking van diensten.	Uitval van een server die klantendatabases host, waardoor klanten tijdelijk geen toegang hebben tot hun gegevens. Hoewel er redundantie is, kan de vervangingsperiode van hardware tijdrovend zijn.	Middelhoog, afhankelijk van de snelheid van herstel en de beschikbaarheid van back-upsystemen.	Gemiddeld, aangezien hardware altijd een kans op falen heeft, ondanks preventief onderhoud.
Softwarefouten	Fouten of onvoorziene gevolgen van software-updates kunnen leiden tot verstoring van services of toegang tot klantgegevens.	Na een grote software-update van de beheersystemen bij Spinware Solutions B.V. kan een bug optreden die de toegang tot klantportalen tijdelijk onmogelijk maakt.	Middelhoog, aangezien bugs vaak snel kunnen worden geïdentificeerd en hersteld, maar klantvertrouwen kan tijdelijk worden geschaad.	Gemiddeld, vooral na grote systeemupdates of migraties.
Natuurrampen	Extreme weersomstandigheden of brand kunnen de fysieke infrastructuur van het datacenter en de kantoorlocaties van Spinware Solutions B.V. bedreigen.	Een brand in het datacenter of in de kantoren van Spinware Solutions B.V. kan leiden tot dataverlies of onderbreking van de fysieke bedrijfsvoering.	Zeer hoog, vooral als belangrijke infrastructuur verloren gaat of langdurige onderbreking van de dienstverlening veroorzaakt wordt.	Laag, maar niet uit te sluiten. Het datacenter heeft waarschijnlijk brand- en noodplannen, maar natuurrampen zoals overstromingen blijven een risico in laaggelegen gebieden zoals Nederland.

	Risico	Concreet voorbeeld	Impact	Waarschijnlijkheid
Menselijke fouten	Menselijke fouten, zoals configuratiefouten of onbedoelde verwijdering van data, kunnen aanzienlijke schade aanrichten.	Een systeembeheerder voert per ongeluk een verkeerde configuratie door op een cruciaal netwerkkapparaat, waardoor bepaalde diensten onbeschikbaar worden voor klanten.	Middelhoog, afhankelijk van de omvang van de fout en de snelheid van herstel.	Gemiddeld tot hoog, omdat menselijke fouten een constante factor blijven in elke organisatie, ondanks de genomen voorzorgsmaatregelen.
Pandemieën	Een pandemie of gezondheids crisis kan de beschikbaarheid van personeel beïnvloeden, waardoor de operationele capaciteit van Spinware Solutions B.V. wordt beperkt.	Tijdens een nieuwe pandemie is een groot deel van het personeel ziek, waardoor de dienstverlening vertraagd raakt en klanten langer moeten wachten op ondersteuning.	Middelmatig, aangezien werk op afstand voor de meeste ICT-functies mogelijk is, maar de efficiëntie kan afnemen.	Laag, maar de ervaring met COVID-19 toont aan dat het risico niet genegeerd mag worden.

Deze concrete risicoanalyse geeft Spinware Solutions B.V. inzicht in de specifieke bedreigingen die de continuïteit van hun bedrijfsvoering kunnen beïnvloeden, met een focus op het Smartdc datacenters en de klantgerichte diensten. Elk risico wordt continu gemonitord en er worden passende maatregelen genomen om zowel de waarschijnlijkheid als de impact te minimaliseren.

2.2. Kritieke bedrijfsfuncties

Voor Spinware Solutions B.V. zijn de volgende functies cruciaal voor de bedrijfsvoering en moeten deze te allen tijde beschikbaar blijven:

1. **Datacenterbeheer** (Smartdc datacenter): Het beheren en onderhouden van de servers en databases die essentieel zijn voor de werking van applicaties en diensten.
2. **Klantondersteuning**: Communicatie met klanten om technische problemen op te lossen en productondersteuning te bieden.
3. **Netwerkbeheer**: Het onderhouden van netwerkconnectiviteit voor interne en externe gebruikers.
4. **Beveiliging**: Het beschermen van klantgegevens en bedrijfsinformatie tegen cyberaanvallen.
5. **Applicatie- en softwareondersteuning**: Onderhoud en updates van bedrijfs- en klantsoftware.

2.3. Noodhulpteam en verantwoordelijkheden

Bij een onderbreking treedt het noodhulpteam (BCP-team) in werking. Dit team bestaat uit vertegenwoordigers van verschillende afdelingen en is verantwoordelijk voor het uitvoeren van de noodzakelijke stappen om de continuïteit te waarborgen. Het team bestaat uit:

- BCP-coördinator: Heeft de algemene leiding over de uitvoering van het continuïteitsplan.
- IT-beheerder: Verantwoordelijk voor IT-systemen en herstel van hardware en software.
- Communicatieverantwoordelijke: Verzorgt de interne en externe communicatie tijdens de crisis.

Verantwoordelijkheden van het BCP-team:

- Snelle beoordeling van de situatie en bepalen van de actievereisten.
- Implementatie van het herstelplan.
- Communicatie met medewerkers, klanten en andere stakeholders.

2.4. Herstelstrategieën

Om de continuïteit te waarborgen, worden er per kritieke functie herstelstrategieën opgesteld.

2.4.1. IT-systemen en datacenter

- **Back-up en herstel:** Dagelijkse back-ups van gegevens worden opgeslagen in een externe cloudomgeving. Bij een storing kan het Smartdc datacenter binnen 24 uur worden hersteld vanuit deze back-ups.
- **Failover-systemen:** Er zijn redundante servers aanwezig die automatisch de taken van defecte servers overnemen.
- **Cloud-opslag:** Kritieke gegevens worden tevens opgeslagen in de cloud voor directe toegang bij serveruitval.

2.4.2. Cyberaanvallen

- **Firewall en antivirus:** Actieve monitoring van netwerkverkeer en implementatie van geavanceerde firewall- en antivirusoplossingen.
- **Incident Response Plan:** In geval van een cyberaanval treedt een incidentenbeleid in werking, waarbij specifieke stappen worden genomen om de aanval te identificeren, te isoleren en te verhelpen.
- **Training:** Regelmatige beveiligingstraining voor medewerkers om bewustwording van bedreigingen te vergroten en menselijke fouten te beperken.

2.4.3. Stroomuitval

- **Noodstroomvoorziening:** Het Smartdc datacenter is modulair opgebouwd en bestaat uit meerdere suites. Elke suite is een autonoom mini-datacenter met een eigen redundante stroomvoorziening en koelapparatuur. Elke suite heeft zijn eigen glasvezelverbindingen, biometrische toegangscontrole, rookdetectie en brandpreventiesystemen. Hierdoor blijft het datacenter operationeel, zelfs bij langdurige stroomonderbrekingen.
- **Werk op afstand:** Medewerkers kunnen, indien nodig, vanuit huis werken via VPN en cloudsysteem.

2.4.4. Klantcommunicatie

- **Telefonische ondersteuning:** Bij storingen kunnen klanten blijven bellen via een back-up telefoonlijn die losstaat van het interne netwerk.
- **E-mailsupport:** E-mail blijft beschikbaar via cloudsysteem, zelfs bij storingen in de fysieke infrastructuur.

2.5. Communicatieplan

Goede communicatie is van cruciaal belang tijdens een noodsituatie. Het incidentenbeleid van Spinware Solutions B.V. bevat procedures voor interne en externe communicatie:

- **Intern:** Het BCP-team communiceert snel en effectief met alle medewerkers via een combinatie van telefoon, e-mail, SMS en de communicatieplatformen Microsoft Teams en Slack.
- **Extern:** Klanten worden op de hoogte gehouden via e-mail, bedrijfswebsite en SMS-berichten.

2.6. Test- en opleidingsprogramma

Om te verzekeren dat het bedrijfscontinuïteitsplan effectief is, zal het plan regelmatig worden getest en bijgewerkt. Dit omvat:

- **Jaarlijkse testen:** Volledige simulaties van noodszenario's om ervoor te zorgen dat alle betrokkenen hun verantwoordelijkheden begrijpen.
- **Evaluatie en updates:** Het plan wordt na elke test geëvalueerd en indien nodig aangepast aan veranderende omstandigheden, zoals nieuwe bedreigingen of technologische ontwikkelingen.
- **Training van personeel:** Alle medewerkers ontvangen periodieke trainingen over hun rol in het bedrijfscontinuïteitsplan.

2.7. Herstel na een ramp

Na een ramp worden de volgende stappen ondernomen om terug te keren naar een normale bedrijfsvoering:

1. **Schadebeoordeling:** Een uitgebreide evaluatie van de schade aan IT-systemen, gebouwen en personeel.
2. **Herstel van systemen:** Prioriteit wordt gegeven aan het herstellen van kritieke systemen zoals het datacenter en klantendatabases.
3. **Evaluatie en rapportage:** Een grondige evaluatie van de respons en uitvoering van het bedrijfscontinuïteitsplan wordt opgesteld, en verbeteringen worden geïdentificeerd voor toekomstige incidenten.
4. **Herstart normale operatie:** Zodra alle systemen weer operationeel zijn, worden alle diensten volledig hervat en wordt een rapport van de incidentafhandeling gecommuniceerd naar de belanghebbenden.

3. Conclusie

Het bedrijfscontinuïteitsplan van Spinware Solutions B.V. is opgesteld om ervoor te zorgen dat het bedrijf in staat is snel en effectief te reageren op noodsituaties, de continuïteit van de dienstverlening te waarborgen, en het vertrouwen van klanten te behouden. Regelmatige evaluaties en trainingen zullen helpen om dit plan up-to-date te houden en klaar voor gebruik in elke noodsituatie.

Voor verdere vragen of meldingen van incidenten kunt u contact met ons opnemen met Rudolf Philipse via 070 3115400. Wij staan altijd klaar om u te ondersteunen en te zorgen voor een snelle en effectieve oplossing van eventuele problemen.