Guide til BCDR:
Bliv klogere på Business Continuity og Disaster Receovery

COMBY

BCDR
BUSINESS
CONTINUITY
DISASTER
RECOVERY

COMBY

Intro til BCDR?

Guide til Forretningskontinuitet og katastrofehåndtering (Business Continuity and Disaster Recovery)

Forretningskontinuitet (BC) og katastrofehåndtering (DR) er to tæt forbundne elementer, der understøtter en organisations evne til at forblive operationel efter og under en krisesituation.

BCDR har til formål at begrænse konsekvenserne af potentielle og kritiske afbrydelser eller forstyrrelser i forretningens drift. BCDR gør det muligt for en organisation hurtigt at komme tilbage på benene efter en krisesituation. Dette reducerer risikoen for datatab og skader på organisationens omdømme samtidig med at risikoen for yderligere kritiske situationer mindskes.

Vi har sammensat denne guide, som gør dig klogere på, hvad en opdateret BCDR-praksis kan gøre for din organisation.

Indhold

Forretningskontinuitet (BC) og katastrofehåndtering (DR) er to tæt forbundne praksisser, der understøtter en organisations evne til at forblive operationel efter en krisesituation.

Hvem er Comby?

Comby er en IT-virksomhed, der blev stiftet i år 2000 med et ønske om at udfordre det eksisterende og gøre det bedre. Siden vi startede, har vi boet på Grønland og leveret IT-løsninger til både private og erhvervskunder. Og nu slår vi også vores folder i Danmark, hvor vi servicerer danske erhvervskunder.

Hvad er BCDR?

Forretningskontinuitet (BC) og katastrofehåndtering (DR) er to tæt forbundne praksisser, der understøtter en organisations evne til at forblive operationel efter og under en krisesituation har ramt organisationen.

En særdeles vigtig egenskab for en organisation er dens modstandsdygtighed, hvis den står over for trusler i form af alt fra naturkatastrofer til cyberangreb.

BCDR er i takt med digitaliseringen blevet vigtigere end nogensinde før. Alle virksomheder, små som store, er i stigende grad afhængige af digitale teknologier for at kunne skabe indtægter, yde services og supportere deres kunder – og kunderne har samtidig en forventning om, at applikationer og data altid er tilgængelige.

"Missionskritiske data må helst ikke opleve nedetid," siger direktør i Comby A/S, Brian Torp. "Selv når ikke-kritiske data er nede, har kunderne en meget lille tolerance."

Sådanne udfald er ikke kun til gene for kunderne.

AK TECHOTEL

Den 9. juni blev AK Techotel angrebet af en hackergruppe med ransomware, som krypterede væsentlige IT funktioner. AK Techotel driver bookingsystemer på hoteller primært i Norden og alle hotellernes reservationer var blevet krypteret.

AK Techotel betaler "et betydeligt beløb" i bitcoins for at få låst reservationerne op. Men så enkelt var det ikke, så AK Techotel måtte ligeledes anvende dyre specialister udefra for at få systemerne op at køre igen.

Jyske Banks Anders Dam, hvis hotel og konferencecenter anvender AK Techotel, kender til flere situationer, som ikke har vværet fremme i offentlighedens lys.

Kilder: techotel.dk & Avisen Danmark

En brand, en oversvømmelse, ransomware-angreb eller andre uventede nødsituationer kan resultere i økonomiske tab, skade en virksomheds brand og i værste fald lukke en virksomhed permanent.

Internationale undersøgelser viser, at mange organisationer i løbet af det seneste år har været under en negativ påvirkning af en eller anden form for problem med den digitale infrastruktur. Og for nogle af disse er omkostningerne løbet op i store million beløb.

"Sådanne udfald kan i dag strække sig over mange datacentre, og ifølge 'best practices' bør man løbende foretage omfattende evalueringer af modstandsdygtigheden hos både tredjeparts og virksomhedsejede digitale infrastrukturer.

Bauhaus hårdt ramt af hackere

Bauhaus i Norden blev midt i juni 2021 ramt af et voldsomt hackerangreb, som lukkede kæden ude af sine egne IT systemer. Dette betød, at Bauhaus ikke kunne servicere sine erhvervskunder eller kunne modtage click-and-collect ordrer.

Hos Bauhaus får selskabets egen IT-afdeling assistance fra 30 eksterne konsulenter i kampen for at genskabe IT-systemerne. Og alt imens varehusene var åbne taber kæden omsætning overvejer Bauhaus at betale den uspecificerede og meget høje løsesum.

Direktør Mads Jørgensen fra Bauhaus kommenterede, "Du er stort set prisgivet over for de her angreb. Vi syntes jo, vi havde styr på sikkerheden. Vi troede, vi havde købt Mercedes'en inden for alt, men vi skulle åbenbart have haft fat i en Rolls-Royce".

Bauhaus overvejer at betale løsesummen til den rusiske hacker gruppe Revil, der også har stået bag andre spektakulære hackerangreb, f.eks. på det Amerikanske slagteri JBS, som endte med at betale 60 mkr. i løsesum. Og udfordringen er, at hver gang der bliver betalt løsesum, så vil afpresningsforretningerne eskalere og fortsætte. Jo flere der betaler, jo bedre er forretningen for hackerne.

Og virkeligheden er, at stadigt flere virksomheder vil vågne op med en "pistol" for panden. Digital afpresning driver virksomheder til desperation. Virksomhederne er nødt til at have procedurer og nødberedskab, således at man kan redde virksomheden, hvis en angreb skulle ske.

(Kilde: retailnews.dk, version2.dk)

Hvorfor er BCDR vigtig?

BCDR praktiseres for at begrænse konsekvenserne af afbrydelser og forstyrrelser i forretningsdriften. Nogle virksomheder har muligvis et lille forspring, når det gælder BCDR. Katastrofehåndtering er nemlig en etableret funktion i mange IT-afdelinger. Men BCDR handler om mere end blot IT; det omfatter en række andre overvejelser - herunder krisestyring, medarbejderes sikkerhed, kommunikation samt alternative arbejdslokationer.

En holistisk BCDR-tilgang kræver grundig planlægning og forberedelse. BCDR-fagfolk kan hjælpe med at skabe en strategi, som skaber større modstandsdygtighed. Udviklingen af sådan en strategi er en kompleks proces, der involverer konsekvensanalyser, risikoanalyser samt udvikling af BCDR-planer, tests, øvelser og træning.

Planlægning og dokumentation er hjørnestenen i enhver effektiv BCDR-strategi. Det hjælper også med håndteringen af ressourcer såsom kontaktlister over medarbejdere, leverandører, instruktioner til udførelse af tests, udstyrslister samt tekniske diagrammer over systemer og netværk.

Man kan grundlæggende angive fire gode grunde til at implementere en BCDR-plan:

- Resultaterne af konsekvensanalysen identificerer mulighederne for procesoptimering og måder, hvorpå en organisation kan forbedre brugen af teknologi.
- Planen fungerer som alternativ dokumentationskilde.
- Planen samler vigtige kontaktoplysninger.

- **Planen fungerer som en brugbar reference i forhold til produktplanlægning, design, service design, levering og andre aktiviteter.**

Hvis en organisation går i gang med en BCDR-proces, bør den samtidig stræbe at skabe en kultur med løbende forbedringer.

Målet med BCDR er at begrænse risici og dermed sikre, at en organisation hurtigst muligt kører så normalt som muligt efter en uventet afbrydelse eller nødsituation.

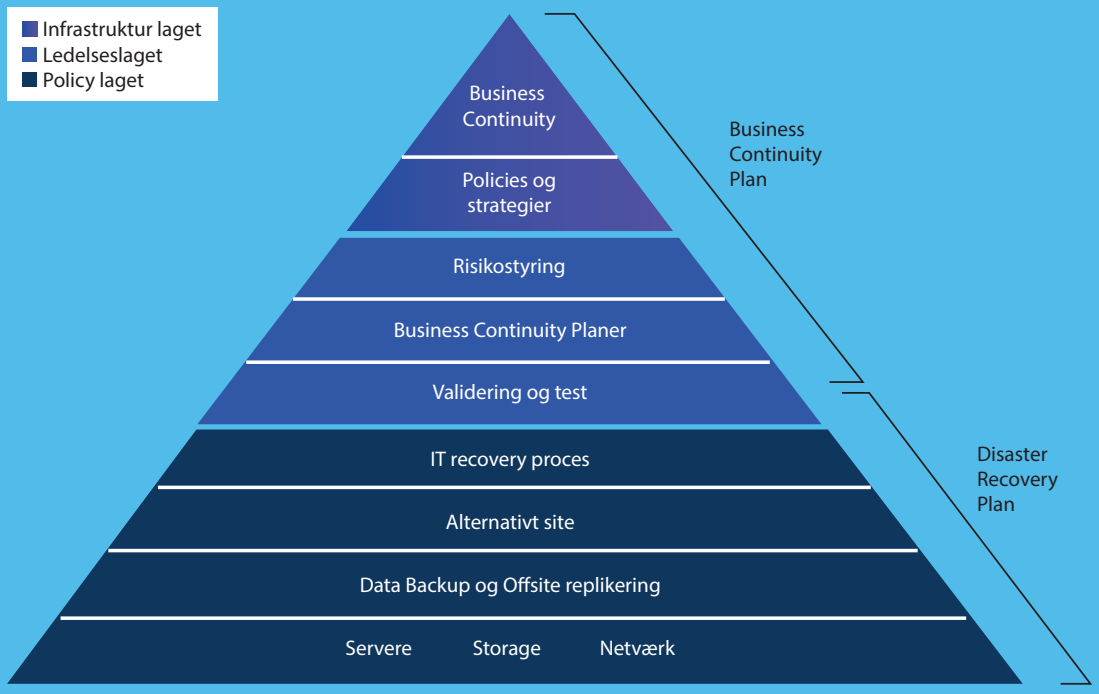
Flere og flere vælger netop at samle BCDR, under én paraply, hvilket skal ses som en almen erkendelse af, at forretnings- og teknologiledere har brug for at arbejde tæt sammen for at forberede sig bedst muligt på kritiske scenarier i stedet for at have hver deres nødberedskab klar.

PRIMOREELS

Primoreels i Vipperød (tidligere Superfos) blev i september 2020 hårdt ramt af en kraftig brand i virksomhedens industribygning. Branden opstod i forbindelse med udskiftning af tagpap og hele virksomhedens trykkeri blev ødelagt af branden. Primoreels som i 2018 var Børsen Gazelle producerer plastfolielåg fra bl.a. youghurt bægre. Med hjælp fra kollegaer er produktionen blevet opretholdt.

Kilde: sn.dk

Planlægning af business continuity og disaster recovery



COMBY

Hvad er forskellen mellem forretningskontinuitet og katastrofehåndtering?

Forretningskontinuitet er den mere proaktive del af praksissen og refererer til de processer og procedurer, organisationen skal implementere for at sikre, at missionskritiske funktioner kan fortsætte under og efter katastrofen. Dette område indebærer en mere omfattende planlægning tilpasset mod de langsigtede udfordringer, som måtte stå i vejen for organisationens succes.

Katastrofehåndtering er den reaktive del af praksissen og omfatter specifikke trin, som en organisation skal igennem for at kunne genoptage driften efter en katastrofe. Katastrofehåndteringen finder altid sted efter en ugunstig hændelse, men den nødvendige responstid kan variere fra dage til sekunder og i de værste tilfælde og dage, uger og måneder.

Forretningskontinuitet fokuserer typisk på organisationen, mens katastrofehåndtering fokuserer på de teknologiske infrastrukturer. Katastrofehåndteringen er en del af forretningskontinuiteten og skal sørge for, at vigtige data er tilgængelige – selv efter en katastrofe. Forretningskontinuitet inkluderer også dette element, men fokuserer i højere grad på risikostyring og anden planlægning, som en organisation har brug for, for at holde sig oven vande under en krisesituation.

Der er også ligheder mellem forretningskontinuitet og katastrofehåndtering. Begge tager de tager højde for ikke-planlagte begivenheder – fra cyberangreb til menneskelige fejl til naturkatastrofer. De har også begge som mål at få virksomheden til hurtigst muligt at køre så normalt som muligt, særligt med henblik på missionskritiske applikationer og data. I mange tilfælde er det også det samme team, som planlægger både forretningskontinuitet og katastrofehåndtering.

EM-fiberglas a/s

Glasfiberfabrikken EM-fiberglas i Hornsyld brød i brand i december 2016. Som følge af en brand i 2012 var virksomheden forberedt og sammen med diverse partnere blev EM-fiberglas genetableret i et andet lejemål. Gennem en ihærdig indsats samt gode nedskrevne procedurer og stærke systemer blev driftstabet minimeret. Kunderne mærkede stort set ikke noget.

Kilde: plast.dk

COMBY

Hvad er forskellen mellem modstandsdygtighed og forretningskontinuitet?

Ordet modstandsdygtighed, i forretningsmæssig forstand, begyndte at dukke op i BCDR-regi i starten af 00'erne. Ordet har tidligere været brugt i flæng, når man har talt om forretningskontinuitet, men udtrykkene har alligevel forskellige betydninger.

En modstandsdygtig virksomhed vil være i stand til at vende tilbage til normal drift efter en nedlukning. Forvaltning af forretningskontinuitet, håndtering af teknologiske nødsituationer og hændelsesrespons er blandt de discipliner, der bestemmer en organisations modstandsdygtighed.

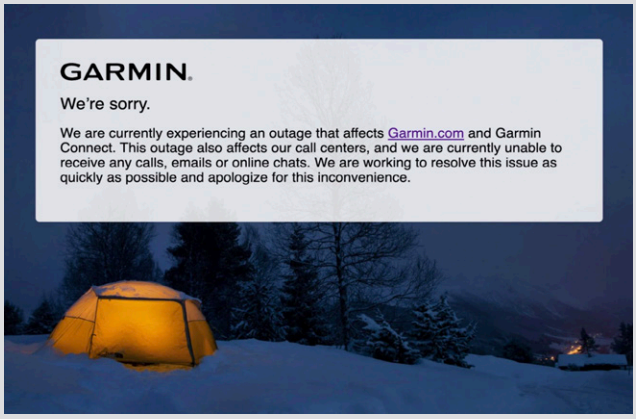
En virksomhed, der arbejder med modstandsdygtighed, forsøger at gøre sig uigennemtrængelig over for

Garmins GPS blev slukket

I juli 2020 blev Fitness & GPS-giganten Garmin ramt af et ransomware angreb - kaldet WastedLocker, hvilket betød at flere af deres systemer ved nede i op til en måned. I følge flere medier betalte virksomheden hackerne, som menes at være den rusiske gruppe Evil Corp, et beløb på $10m. for at Garmin igen kunne få adgang til sine data.

Efterfølgende er det kommet gisninger frem om, at det var basale ting, såsom administrator rettigheder, der gav hackerne adgang til de interne systemer. Herved mistede kunderne adgang til Garmin connect og websitet gik ned. Herudover har sikkerheden hvor medarbejdere har arbejdet hjemmefra været en nøgle til flere af de andre store angreb som fandt sted i 2020. Og Garmins såvel som de øvrige kunder sidder tilbage med en uvidenhed om, hvor mange data, som hackerne sidder tilbage med.

Garmin blev fra flere sider beskyldt for at være meget sparsomme med den information, som blev videregivet til kunder og partnere. I modsætning til f.eks. AK



Techotel som på forsiden af deres website holdt en meget åben kommunikation til kunder og omverden generelt. Umiddelbart vil dem som er mest åbne i denne situation også være dem, som bedst beskytter deres omdømme på den lange bane.

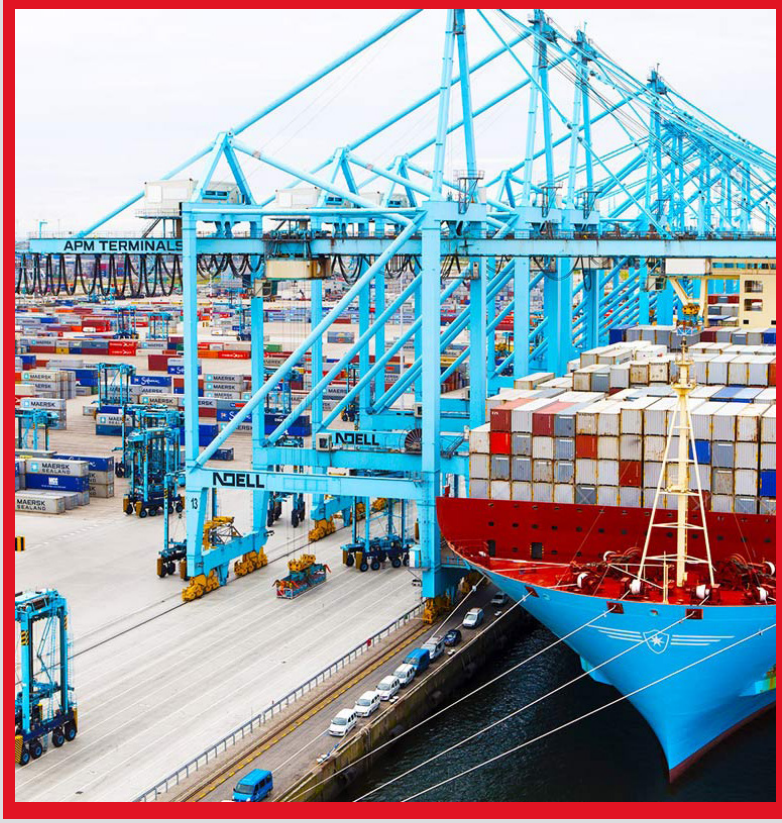
Kilde: theverge.com, orangedyberdefense.com og mitnicksecurity.com

potentielle trusler, siger Stefan Boel, som er direktør for Comby Denmark. Forretningskontinuitet indebærer derimod en sikring af den fortsatte drift, efter at katastrofen er sket, siger han.

Modstandsdygtighed ”handler i højere grad om at modstå problemer, mens forretningskontinuitet handler om at kunne fortsætte driften efter et udfald eller en forstyrrelse,” siger Stefan Boel.

Stefan Boel bruger en elastikmetafor til at beskrive, hvordan de fleste virksomheder ’strækkes’, når de gennemgår kriser, men at den rette modstandsdygtighed

Lifting Global Trade
APM TERMINALS

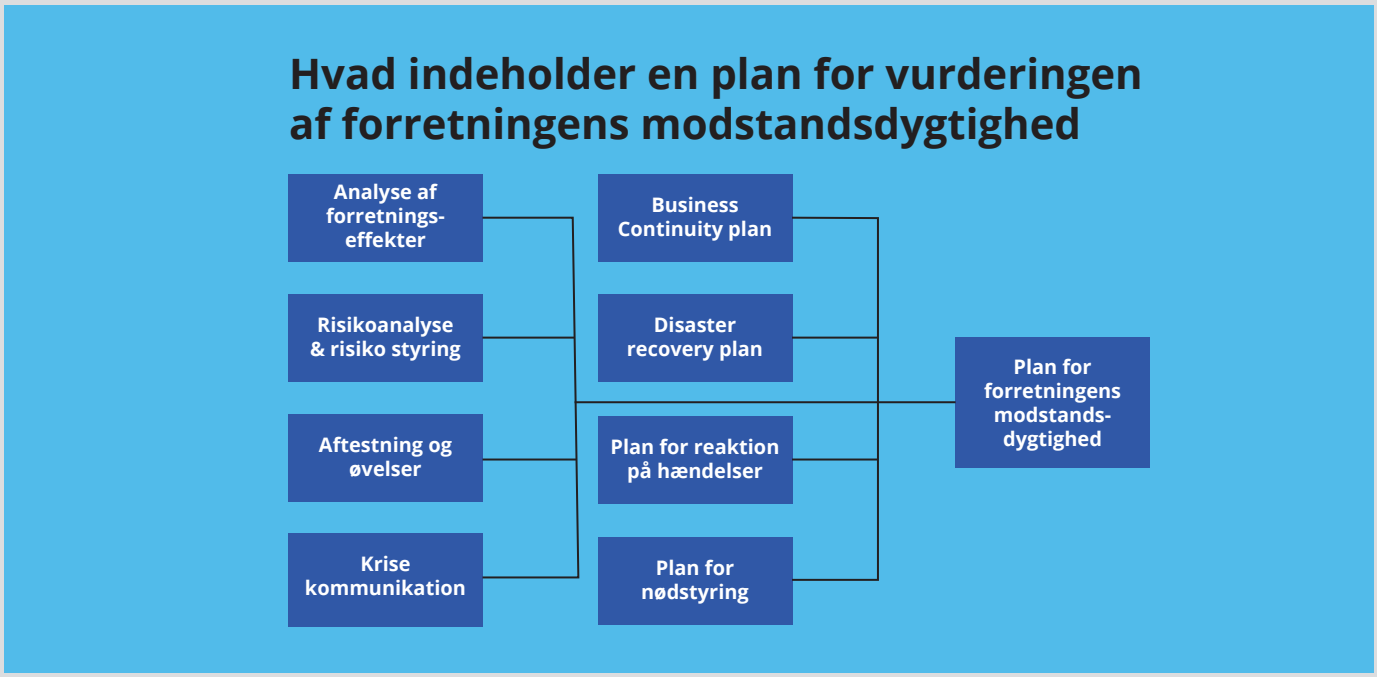


Da AP Møller Mærsk ejede APM Terminals i sommeren 2017 blev ramt at globalt ransomware angreb fik det betydning for mange millioner container i havne verden over. Selskabet står for håndteringen af 1 ud af 7 containere der flyttes verden over.

Det var malware angrebet NotPetya som udover APM Terminals ramte DLA Piper, fødevarevirksomheden Mondalez, Saint Gobain og annoncebureauet WPP. Petya anvendte sårbarheden i Microsoft Windows kendt som EternalBlue. Maersk betegner angrebet som en ny type malware, som updates og antivirussystemer ikke ydede effektiv beskyttelse imod. Selskabet har indført yderligere beskyttelsesforanstaltninger for at forsvare sig mod angreb.

Selvom Maersk relativt hurtigt fik styr på tingene og allerede dagen efter var på vej til normal drift, så kostede det dyrt. I flg. scm.dk landede den samlede regning for APM Terminals på et sted mellem 1,3 og 1,9 mia. kr.

Kilde: reuters.com, the Guardian & SCM.dk



kan gøre, at en virksomhed kan stå imod og derved opretholde sin form. Forretningskontinuitet praktiseres derimod først, når elastikken er knækket, og organisationen aktivt skal adressere skaderne, tilføjer han.

Ifølge Combys Stefan Boel, drejer forretningskontinuitet sig om evnen til at kunne mislykkes, uden at det får de store konsekvenser for diverse systemers tilgængelighed og drift, mens modstandsdygtighed er evnen til helt at undgå problemerne til at starte med.

Risikoanalyse, effektanalyse og BCDR-strategier

Risikoanalyser og effektanalyser er vigtige værktøjer for organisationer, der står over for at skulle lave en BCDR-strategi. Det er nemlig vigtigt både at vurdere interne og eksterne risici i BCDR-processen.

Risikoanalysen identificerer sådanne risici og man vurderer sandsynligheden for, at de vil forekomme. Risikoanalysen arbejder parallelt med effektanalysen, hvor den hjælper med at kvantificere de potentielle konsekvenser af forskellige typer af afbrydelser og forstyrrelser. Finansiel analyse er også ét aspekt af effektanalysen, men den tager også hensyn til omkostninger, som ikke er af økonomisk karakter. Effektanalysen identificerer også de missionskritiske funktioner, som organisationen skal opretholde eller gendanne efter en kritisk hændelse, samt de nødvendige ressourcer der skal til for at understøtte disse.

Det er vigtigt at få ledelsesstøtte, hvis du har ambitioner om at gennemføre en effektanalyse, da det kan være en meget intens proces. En effektanalyse giver en organisation større selvindsigt og synliggør samtidig en masse uforløst potentiale.

En organisation bør i flg. Comby bruge risiko- og effektanalyser til at udforme strategier for forretningskontinuitet og katastrofehåndtering. Hver strategi omdannes til en række konkrete handlinger, der skal hjælpe med at genoprette orden ved f.eks. at overføre data til cloud-baserede tjenester eller aktivere alternative netværksveje.

Hvorfor skal jeg bruge BCDR, og hvornår skal jeg sætte i gang?

Motivationen for at implementere en BCDR-strategi kunne være ønsket om at ville beskytte sine medarbejderes liv og sikkerhed – men det kunne også være ønsket om at ville sikre tilgængeligheden af serviceydelser og/eller konkrete indtægter. Konkurrencepositionering og omdømmekontrol er begge faktorer, der også ligger til grund for motivationen. En virksomhed, der er ude af stand til at beskytte sine medarbejdere eller kunne levere de efterspurgte services, vil ofte skulle kæmpe ekstra hårdt for at tiltrække medarbejdere og kunder.

Det store fokus på GDPR og compliance har også været medvirkende til, at mange organisationer ønsker at implementere BCDR. F.eks. skal man inden for sundhedsvæsenet helst have en alternativ driftsplan klar, som sikrer den fortsatte beskyttelse af digitale sundhedsinformationer, uden at det må gå ud over kritiske arbejdsfunktioner.

Opererer man i USA kræver Financial Industry Regulatory Authority (FINRA) - en organisation der fører tilsyn med aktiehandlere - at firmaer ”opretter og vedligeholder skriftlige planer for sikring af forretningskontinuitet.” FINRA skitserer disse foranstaltninger i sin beredskabsregel.

Nogle offentlige amerikanske instanser er ligeledes forpligtet til at udvikle BCDR-strategier eller ’continuity

of operations plans'. Målet er, at "sikre, at vigtige offentlige services er tilgængelige i nødsituationer såsom terrorangreb, vejrkatastrofer eller lignende." Noget tilsvarende findes endnu ikke i Danmark, men der presses på for at emnet tages op politisk.

I nogle tilfælde kan det også være kunder, som presser organisationer til at lave BCDR-planer. En virksomheds holdning til BCDR kan have indflydelse på en potentiel kundes vurdering af virksomheden. Nationale tilsynsmyndigheder, såsom finanstilsynet, tilskynder banker at inkludere modstandsdygtighed som en del af deres risikoanalyser. "

Spørgsmålet om hvorfor man bør have en BCDR-strategi kan have mange forskellige svar, og svaret til hvornår man skal lave en BCDR-strategi er mindst lige så nuanceret. Organisationer bør overveje flere faktorer, før de vurderer, om der er tale om en katastrofe og dermed effektuerer BDCR-planen. De vigtigste af disse er den forventede varighed af afbrydelsen, afbrydelsens konsekvenser, de økonomiske omkostninger ved at aktivere BCDR-planen samt mulige forstyrrelser i forbindelse med aktivering af BCDR-planen. Paradoksalt

nok kan en tilbagevenden til normal drift skabe endnu flere problemer.

Derfor er det vigtigt, at organisationens ledelse omhyggeligt dimensioneres efter den vedtagne BDCR-plan. Dét at gå over til en backup-facilitet ”har en indvirkning på budgettet”. For en organisation kan en seks timer lang afbrydelse ikke være væsentlig nok til at blive kategoriseret som en katastrofe. Mens det for andre kan være livstruende.

Beslutningen om at aktivere BCDR-planen tages, særligt i større virksomheder, af en komité frem for en enlig beslutningstager. En sådan komité består typisk af CEO, CFO, CIO etc.

Hvordan laver man en BCDR-plan?

Organisationer kan bryde en BCDR-plan ned i BC- og DR-dele. Derfor indeholder en forretningskontinuitetsplan kontaktinformationer, procedurer for ændringsstyring, retningslinjer for hvordan og hvornår, man skal bruge planen, step-by-step-procedurer og en tidsplan for gennemgang, tests og opdatering. En katastrofehåndteringsplan indeholder en opsummering af vigtige handlingstrin og kontaktinformationer, en defineret skitsering af ansvarsfordelingen, retningslinjer for hvornår man skal bruge planen, målsætning, gendannelsestrin etc. En katastrofehåndteringsplan bør også tage højde for, at de medarbejdere, som er i stand til at eksekvere planen, altid er tilgængelige til at påtage sig kritiske gendannelsesopgaver.

Gode BCDR-planer tager ligeledes højde for, at der er forskellige niveauer af risici. Det kræver definition af handlinger for forskellige udfordringer og den efterfølgende gendannelse. Det er vitalt at BCDR-planen indeholder kommunikationsaspekter, der beskytter organisationens medarbejdere, faciliteter og image.

Fastsættelse af retningslinjer er et vigtigt skridt til at komme i gang. Retningslinjerne lægger nemlig grundstenen til processen og dækker typisk styringen af forretningskontinuitetsplanen, hvilke medarbejdere der er ansvarlige samt de pågældende aktiviteter såsom udvikling og konsekvensanalyse.

Retningslinjer kan også etablere et fælles sæt af målinger såsom key performance-indikatorer og key risk-

indikatorer. Retningslinjerne bliver ofte overset, men de er ikke desto mindre vigtige i forhold til at føre kontrol over sin forretningskontinuitet.

Udvikling af forretningskontinuitetsplaner og katastrofehåndteringsplaner starter typisk med at samle et BCDR-team for derefter at lave en risikoanalyse og en konsekvensanalyse. Organisationen identificerer de mest kritiske aspekter af virksomheden samt hvor hurtigt og i hvilket omfang, de skal op at køre efter en utilsigtet hændelse. Når organisationen har nedskrevet de trinvise procedurer, skal de testes, gennemgås og opdateres.

Selvom visse aspekter af processen kun involverer enkelte medarbejdere, er det vigtigt, at alle væsentlige personer i organissationen forstår planen og er inkluderet på et eller andet tidspunkt i processen. Planen bør også omfatte udvalgte leverandører, partnere og de serviceydelser, de leverer. F.eks. er en bank afhængig af data, som et tredjepartsfirma leverer, og derfor bør et sådant forhold også dokumenteres i BCDR-planen. Eksterne enheder som disse skal involveres i processen, så også de forstår, hvordan planen fungerer.

Andre trin i BCDR-tjeklisten inkluderer risikoreduktion og en kriseplan. Sidstnævnte beskriver metoden eller metoderne, som en organisation vil tage i brug til at formidle information om en given nødsituation til medarbejderne.

Samlet set vil processen med at opbygge en BCDR-plan involvere følgende aktiviteter:

- identificering af risici
- vurdering af infrastruktur
- konsekvensanalyse
- designplan
- implementering af plan
- tests

Hvordan tester man sin BCDR-plan?

Tests af ens BCDR-plan skal give vished om, at de gendannelsesprocedurer, der er indført, fungerer som forventet, så man kan bevare driften af forretningen. Testfasen kan også identificere forbedringsområder, som organisationen kan adressere og indarbejde i den næste version af planen.

Tests kan variere fra at være helt simple til meget komplekse. En diskussionsbaseret øvelse gør f.eks., at deltagerne sammen kan gennemgå planens forskellige trin. En sådan type test hjælper de medarbejdere, som er involverede i planen med at blive mere fortrolige med reaktionsprocessen, mens administratorer kan vurdere planens effektivitet.

I den anden ende af testspektret skal medarbejderne simulere selve udførelsen af deres BCDR-funktioner. Disse øvelser kan f.eks. involvere brugen af backup-systemer.

Tests er tidskrævende og kræver finansiering, ledelsessupport og medarbejderdeltagelse. Testprocessen kræver også forudgående planlægning, træning, de rigtige testpersoner og efterfølgende rapportering.

Hyppigheden af hvor tit der er behov for test, varierer fra organisation til organisation. Større virksomheder bør lave diskussionsbaserede øvelser mindst én gang pr. kvartal, mens mindre organisationer ikke behøver at teste nær så ofte. En fuldbyrdet BCDR-test, der er mere tids- og

ressourcekrævende, bør udføres én gang årligt.

Comby anbefaler ligeledes en kvartalsvis testplan med en katastrofehåndteringstest udført to gange om året med diskussionsøvelser imellem disse tests. Derudover bør forretningskontinuitetsplanen testes separat én gang årligt. I følge Stefan Boel, comby Denmark er det mere effektivt at adskille testene, fordi en separat udførelse af katastrofehåndteringstesten er mindre forstyrrende for organisationen.

Periodevise tests, vedligeholdelse og opdateringen af plane samt modstandsdygtighed er tre sammenhængende elementer. En organisation forbedrer naturligt sin modstandsdygtighed, når den opdaterer sine BC- og DR-planer og derefter tester dem løbende.

COMBY

Styring af BCDR-omkostninger

Ændringer i trusselslandskabet eller nye konkurrenter kan tvinge en organisation til at udvide sin BCDR-dækning. Sådanne ændringer kan kræve ekstra udgifter i form af konsulentservices eller backup- og gendannelsesteknologier.

BCDR-ledere må i nogle tilfælde søge ny finansiering til den udvidede BCDR-plan, hvis ikke pengene findes i det aktuelle budget.

Et investeringsforslag bør bygge på en forretningscase, som fokuserer på de positive resultater, som de nye BCDR-funktioner vil give organisationen. I finansieringsforslaget bør det også tydeliggøres, om den reviderede BCDR-plan vil påvirke andre områder, såsom cybersikkerhed. Sikkerhedsundersøgelser og services, der understøtter de udvidede krav, bør også tages med i betragtningen, når man forsøger at opnå finansiering.

Organisationer skal finde en balance mellem investeringsniveauet i fremgangsmåden og de forventede økonomiske tab, der vil være ved et givet katastrofescenarie. ”Du ønsker jo naturligvis ikke en løsning, der koster 200 gange mere end katastrofen selv.

At bede virksomhedsledere, med udgangspunkt i forskellige virksomhedsdiscipliner, om at estimere de forventede omkostninger, forbundet med forskellige typer af begivenheder, kan hjælpe organisationer med at etablere en god base, hvorfra de kan træffe velfunderede beslutninger om BCDR-investeringer.

Standarder, skabeloner, software og services til BCDR-planlægning

Organisationer, der påbegynder en BCDR-planlægningsproces, har mange ressourcer at trække på, såsom standarder, skabeloner, softwareprodukter og rådgivningsservices.

”Du har muligvis allerede nogle brugbare skabeloner, konsulenter eller ’best practices’ ved hånden, som du kan bruge til at udforme din BCDR-plan”. ”Så der er ingen grund til ikke at have en stærk katastrofehåndteringsplan.”

Standarder

Statslige og private sektorers standardiseringsorganer, herunder Det Norske Veritas (DNV) og Den Internationale Organisation for Standardisering (ISO) har offentliggjort en række BCDR-retningslinjer. Standarderne, der dækker alt fra krisestyring til risikovurdering, giver nogle rammer for, hvordan virksomheder kan udforme deres BCDR-planer.Følgende er en række eksempler på standarder:

- ISO 22301: 2019: Sikkerhed og modstandsdygtighed - Forvaltning af forretningskontinuitetssystemer - Krav
- ISO 22313: 2012: Samfundssikkerhed - Forretningskontinuitetssystemer -Vejledning
- ISO 22320: 2018: Sikkerhed og modstandsdygtighed - Nødstyring - Retningslinjer for håndtering af hændelser
- ISO / IEC 27031: 2011: Informationsteknologi - Sikkerhedsteknikker - Retningslinjer for informations- og kommunikationsteknologiberedskaber til forretningskontinuitet

(genudvikles som ISO / IEC WD 27031)

- ISO 31000: 2018, Risikostyring - Retningslinjer
- ISO-guide 73: 2009: Risikostyring - Vokabular
- IEC 31010: 2019: Risikostyring - Teknikker til risikovurdering
- ISO / TS 22317: 2015: Samfundssikkerhed - Forvaltning af forretningskontinuitetssystemer - Retningslinjer for konsekvensanalyse (BIA) (skal erstattes af ISO / AWI TS 22317)

BCDR-skabeloner

BCDR-skabeloner består af nogle præindstillede formularer, som organisationer kan udfylde og bruge som dokumentation i BCDR-planlægningen. Nogle skabeloner dækker hele BCDR-planen, mens andre kun dækker dele af BCDR-planen. Forretningskontinuitetsplaner kan f.eks. indeholde bestemmelser for naturkatastrofer, brande, netværksafbrydelser eller oversvømmelser. En planlægningsskabelon kan særligt være til hjælp for mellemstore og små virksomheder, da det kan forenkle processen en del.

En BCDR-plan kan i nogle tilfælde kræve en SLA - Service Level Agreement, der fastlægger standarderne for kvaliteten af en organisations BCDR. Den kan også hjælpe med at sikre, at services gennem tredjeparter lever op til et acceptabelt niveau.

Som nævnt ovenfor kan gennemførelsen af en konsekvensanalyse hjælpe organisationer med forretningskontinuitetsplanlægningen. Denne skabelon til en konsekvensanalyserapport giver nogle værktøjer til at dokumentere dokumentationen af hovedprocessen, delprocesserne samt de økonomiske og operationelle konsekvenser ved evt. afbrydelser.

Organisationer kan også drage fordel af at planlægge BCDR-aktiviteter, da disse løbende vedligeholder forretningskontinuitetsstrategien. Sådanne aktiviteter

kan variere fra planlægning af konsekvensanalyser til gennemgange af teknologinedbrudsplaner.

BCDR-software

Specialiseret BCDR-software giver nogle andre værktøjer til organisationer, som vil udforme en BCDR-plan. BCDR-produkter, sommetider kaldt forretningskontinuitetssoftware eller software til styring af forretningskontinuitet, er udviklet til at hjælpe organisationer med at udforme forretningsplaner for BCDR. De dækker typisk en række planlægningsaktiviteter, såsom konsekvensanalyser og risikovurderinger.

Services til planlægning af BCDR

En anden mulighed er at outsource organisationens BCDR-behov til et tredjepartsfirma, der kan levere risikoanalyse samt planlægge udvikling, vedligeholdelse

BCDR forhandlere, produkter og serviceydelser

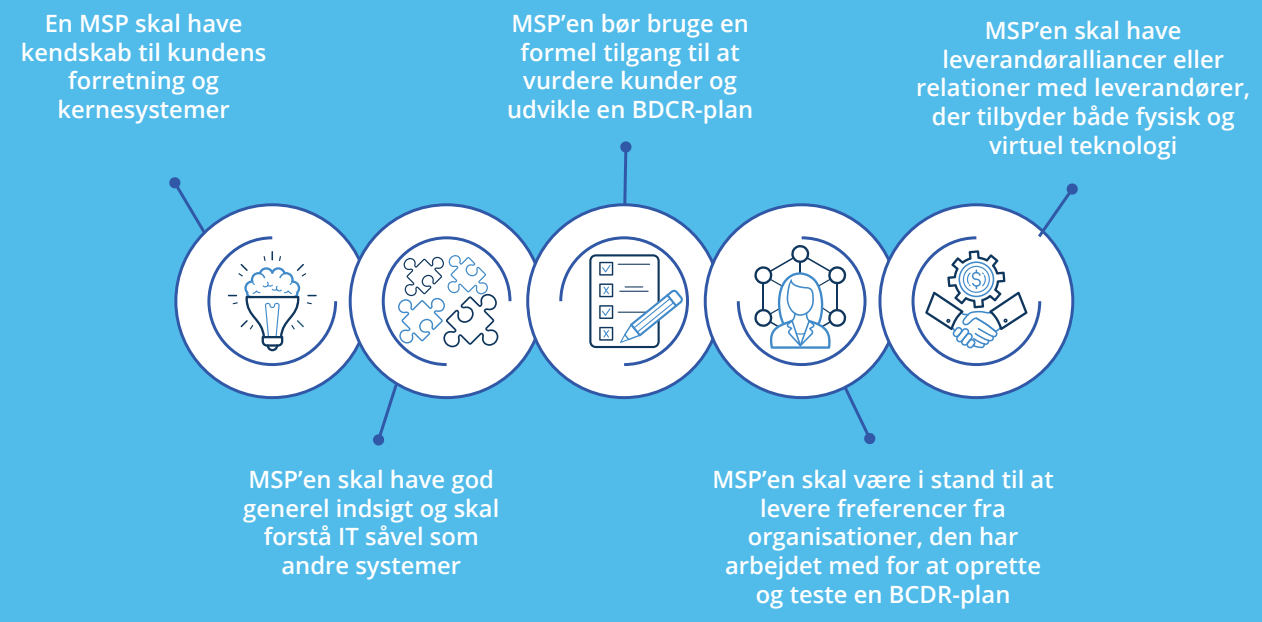
BC serviceydelser Business Continuity	**BC virksomheder** Business Continuity	**Tilgange**	**BCDR software**	**DR forhandlere** Disaster Recovery
■ Planlæg udvikling ■ Forberedelse af analyse af forretningseffekter ■ Revision ■ Risikoanalyse ■ Planlæg trænings-forberedelse ■ Rådgivning ■ Tekniske og rådgivende tjenester ■ Vurderinger ■ Politik og procedure ■ Udvikling ■ Interviewer ■ Administrative aktiviteter ■ Data indsamling ■ Dokumentation	■ De fire store regnskabsfirmaer ■ Boutique konsulentfirmaer ■ Revisionsfirmaer ■ BCDR konsulenter ■ Rådgivende virksomheder ■ Softwarefirmaer	■ Forskellige BC-tjenester / firmaer og BCDR-værktøjer ■ BC-tjenester samarbejder med en bestemt DR-administreret managed service udbyder ■ BC MSP og DR som en serviceydelse	■ Backup af data ■ System backup ■ Fjernlagring	■ Lokale leverandører ■ Cloud-udbydere ■ DR som en serviceydelse ■ Hybrid løsning ■ MSP'er ■ Teknologi-virksomheder

og træning. Det er her vigtigt, at virksomheden analyserer sine behov, inden de vælger et BCDR-firma og dermed gør det klart, hvad det er, de vil outsource, hvilke tjenester de forventer at få gennem udbyderen, overvejer risikoen ved en outsourcing-aftale, og hvor meget det må koste.

En god støtte til at planlægge BCDR kan være revisorer, som bl.a. kan hjælpe med at udføre konsekvensanalyser. Revisorer skal typisk være i stand til at hjælpe klienter med at bestemme omkostningerne ved evt. afbrydelser, men ideelt set bør man vælge et firma med erfaring inden for forretningskontinuitet eller IT-ressourceplanlægning, f.eks. et konsulentfirma.

Managed Service-udbydere (MSP'er) fungerer ofte som virtuelle CIO'er for deres SMB-kunder. I den rolle kan disse udbydere også hjælpe med planlægningen. Da deres forretning går ud på at styre kundernes IT-aktiviteter, er de i stand til at udvikle en plan for håndtering af evt. teknologiafbrydelser.

5 overvejelser ved valg af MSP til udvikling af BCDR plan



Støtteteknologier og -strategier

Teknologimulighederne til udførelse af DR-delen af en BCDR-plan er blevet bedre de seneste år på grund af fremkomsten af 'cloud computing'. Traditionelt set har organisationer måttet bygge eller leje en ekstern server for at håndtere deres gendannelsesbehov. En sådan ekstern løsning kræver en kopiering af samtlige interne produktionssystemer katastrofe genoprettelsessteder kræver en kopiering af interne produktionssystemer, hvilket er uden for økonomisk rækkevidde for mange mindre virksomheder. Dog har cluod-baserede løsninger været med til at gøre katastrofehåndtering lettere tilgængelig for selv små organisationer.

Andre løsninger, der giver større modstandsdygtighed, inkluderer alarmsystemer, cybersikkerhedssystemer og hændelsesreaktionssystemer, som muligvis allerede indgår i forskellige BCDR-produkter. Organisationer har muligvis også sørget for, at der kan stilles alternative arbejdslokationer til rådighed i tilfælde af, at katastrofen sker.

BCDR-styring

Det team, som administrerer og, i tilfælde af katastrofe, eksekverer en BCDR-plan, skal være tværfunktionnel og skal kunne trække på flere forskellige interessenter og ekspertise på tværs af organisationen.

Ledelsesfordelingen i teamet varierer fra organisation til organisation. I en stor virksomhed for eksempel, er det typisk den, som er ansvarlig for risikostyring, som leder

BCDR-teamet med en repræsentant fra IT-afdelingen som næstformand. Mindre organisationer har oftest ikke en risikostyringsafdeling, hvorfor man ofte udnævner CFO'en til at lede teamet. I nogle tilfælde er det også IT-afdelingschefen, som leder BCDR-teamet.

Andre medlemmer af teamet inkluderer typisk repræsentanter fra nogle af organisationens nøglefunktioner: økonomi og regnskab, den juridiske afdeling - herunder in-house og eksterne rådgivere - samt marketing og PR.

Opgaven med at samle flere interessenter for at udvikle en BCDR-plan – og udføre de nødvendige konsekvens- og risikoanalyser - kan vise sig at være udfordrende. Projektledelse er derfor en vigtig del. Organisationer bør derfor overveje at udnævne en projektleder til at lede processen.

BCDR-teamet bør også have ansvaret for den løbende forretningskontinuitetsledelse og sørge for, at planerne hele tiden er opdaterede. Forretningskoncepter og datacenterteknologier ændrer sig ofte, så BCDR-planer har brug for regelmæssig vedligeholdelse for at forblive aktuel. En organisation skal først og fremmest vurdere om den nuværende plan skal opdateres, eller om det er nødvendigt med en helt ny plan. Organisationer er dog nødt til at teste deres BCDR-plan for at vurdere, i hvilket omfang den skal revideres.

Ud over tests kan et BCDR-team også overveje at udføre en planrevision, som vurderer effektiviteten af planen. Revisionen skal specificere de risici, der kan komme i vejen for at planen lykkes og teste de kontrolenheder, der er med til at afgøre, om risiciene er til fare for organisationen. En IT-kontrolrevision kan også bruges til at vurdere de risici, der er forbundet med IT-

infrastrukturen og dermed identificere områder, der kan forbedres.

De forskellige roller og ansvarsområder BCDR-teammedlemmerne har - fra planlægning til tests - kan specificeres i organisationens forretningskontinuitetspolitik. En sådan politik kan også omfatte eksternt personale, såsom leverandører og kunder.

5 ting du skal bruge til en audit af din BCDR-plan

1. **Dit auditeringsteam.** Dette kan være egne ansatte eller et eksternt firma. Objektivitet og kendskab til BCDR blandt teamets medlemmer kan bidrage til at sikre ordentlige resultater.
2. **Dokumentation.** Analyser af effekt på forretningen, risikovurderinger og etablerede BCDR respons-planer giver en integreret auditeringsinformation.
3. **Vejledning**. Standarder og generel industriel praksis kan styre din audit for at sikre, at alle dine baser er dækket, og din BCDR-plan opfylder alle kravene indenfor dit felt.
4. **Interviews**. At gennemføre interviews med personale, der er fortrolige med BCDR-processen, kan tilføje en betydelig indsigt i en audit.
5. **Konkrete handling og resultater**. Når din audit er afsluttet, skal dine resultater give dig de næste skridt til at forbedre din BCDR-plan og gøre dig klar til din næste audit.

Et andet vigtigt aspekt, når man skal finpudse sit BCDR-team, er at få enkeltpersoner til følge 'best practices'. Med henblik herpå kan BCDR-teammedlemmer benytte sig af diverse træningsforløb og certificeringsprogrammer.

Certificeringsudbydere arbejder normalt med en intern eller ekstern træningsgruppe, der forbereder de studerende til en eksamen.

På forskellige konferencer kan man også få uddannet sit BCDR-team bl.a. Disaster Recovery Journal-events (www.drj.com) være nyttige for folk, der ønsker at lære mere om forretningskontinuitet.

BCDR-faldgruber

Forandring er måske BCDR-planens største fjende. Udviklingen inden for teknologi accelererer hurtigt, hvilket efterlader mange organisationer med en stor opgave i forhold til løbende at opdatere deres IT-udstyr. En 5 år gammel BCDR-plan vil sandsynligvis ikke afspejle - og vise sig tilstrækkelig til at beskytte - det nuværende IT-setup.

En organisations forandringsledelsesproces kan hjælpe med at løse dette problem. Forandringsledelsen fører tilsyn med tilpasninger af systemer, netværk, infrastrukturer og dokumenter. Der adresseres lignende situationer som ved BCDR-planlægning og tests, så en organisation kan beslutte sig for at tage BCDR med i forandringsledelsesprocessen.

Forandringsstyringsprocessen består af seks hovedaktiviteter:

1. identificer en potentiel forandring
2. analyser årsagen til forandring
3. evaluer forandringen
4. planlæg forandringen
5. gennemfør forandringen
6. gennemgå og afslut forandringsprocessen

En organisation er naturligvis også underlagt forandringer. Organisationer opkøber, frasælger og går ind i nye forretningsterritorier. En effektiv BCDR-plan skal regelmæssigt opdateres for at tage højde for sådanne

udviklinger. Hyppige BCDR-tests kan afsløre huller i planen, såsom manglende redegørelser for teknologi og forretningsændringer. Ifølge Comby A/S kan mange organisationer, der har en ekstern softwareudbyder, have en falsk forståelse af, hvor godt deres data er beskyttede.

Nogle har den opfattelse at apps, som f.eks. Microsoft 365 og Salesforce, ikke behøver at blive sikkerhedskopieret. Ifølge Comby, er det en stor misforståelse. F.eks. bevarer Office 365 kun slettede e-mails i en begrænset periode alt efter, hvilket abonnement man har.

”Disse applikationers modstandsdygtighed bliver ofte forvekslet med deres tilgængelighedsniveau”. ”applikationerne er ofte ikke ordentligt beskyttede.”

Organisationer, der bruger disse cloud-baserede applikationer, bør se grundigt på deres udbyderes betingelser for databeskyttelse og gendannelse og sørge for, at BCDR-planen tager højde for disse applikationer og deres tilgængelighedsniveauer. Erfaringerne viser at omkring halvdelen af IT folk og virksomheder mener at være fortrolige med deres udbyderes databeskyttelses- og gendannelsesbetingelser, men ofte viser det sig desværre at være helt forkert.

For at sikre at ens plan ikke har for mange svage punkter, kan en organisation bruge en BCDR-tjekliste eller en række andre tjeklister, der dækker alt fra planer til politikker og gendannelsesstrategier. BCDR-teamet bør også holde sig ajour med det skiftende trussellandskab og hele tiden sørge for, at deres plan afspejler evt. nye trusler. De trusler, som organisationer bør holde øje med, kan være alt fra cyberangreb til fysiske trusler.

COMBY

Hvordan ser fremtiden ud for BCDR?

BCDR-planlægning og -udførelse vil fortsætte med at udvikle sig i takt med, at de forskellige trusler skifter karakter og bliver flere. Her er et par udviklinger, som skal overvejes:

Sammenløbet mellem cybersikkerhed og forretningskontinuitet.

Cyberangreb, såsom ransomware, som er i stand til at afbryde forretningsdriften, ser ud til at fortsætte – og det vil givetvis tage til i styrke. Cybersikkerhed og forretningskontinuitet er typisk to adskilte funktioner i en organisation. Men ifølge Kirvan vil disse discipliner i fremtiden komme til at høre under samme tag.

Tilbage til fremtiden med opbevaring af bånd.

Backup-filer kan være krypterede i et ransomware-angreb. Organisationer har dog muligheden for at isolere de filer, de har brug for at redde ved at lave et såkaldt 'air gap' i virksomhedsnetværket. Det er her, at opbevaring af bånd kommer i spil. Bertrand mener, at denne gamle metode genopstår som en måde, hvorpå organisationer kan bevare kopier af deres data, offline og off-site.

Kunstig intelligens indflydelse på BCDR-planlægning.

Ifølge Kirvan, vil kunstig intelligens i fremtiden være i stand til at hjælpe BCDR-teams med at træffe beslutninger om tilrettelæggelsen af deres planer og kan også spille en rolle i gennemførelsen af konsekvensanalyser og risikovurderinger. Kunstig intelligens kan også blive en vigtig brik i forhold til hændelsesrespons ved f.eks. at anbefale bestemte handlinger baseret på detaljerne i et bestemt katastrofescenarie.

Serviceudbydere kommer til at spille en større BCDR-rolle.

En stor procentdel af serviceudbyderne er allerede involveret i backup- og katastrofehåndtering. Men udbuddet af forretningskontinuitetsservices vil blive større, da mange små virksomheder fortsat vil mangle ekspertisen internt. Serviceudbyderne vil også i højere grad få en rådgivende rolle i forhold til BCDR-planlægning og teknologi. Nogle leverer deres egen gendannelsesservice, mens andre samarbejder med leverandører, der leverer et sådant værktøj.

COMBY

Vil Covid-19 få indflydelse på din 2021 BCDR-strategi

COVID-19 har ændret mange organisationers syn på BCDR. Sammen med den øgede interesse for modstandsdygtighed, er interessen i at få lavet en pandemisikker BCDR-plan steget markant.

I lyset af COVID-19-pandemien har BCDR-planlægning og -teknologi udviklet sig i takt med at flere og flere hjemmearbejdspladser er taget i brug. Det er en tendens, der forventeligt vil fortsætte gennem 2021.

Med næsten et års tilpasningstid til ændringer i forretningsprocesser, forårsaget af COVID-19, er BCDR blevet endnu mere værdifuldt i organisationer af alle typer og størrelser. Derudover er modstandsdygtighed blevet en måde at omfavne adskillige discipliner på med henblik på at beskytte og genoptage forretningsdrift.

BCDR-strategier, programstyring og modstandsdygtighed vil i år blive endnu vigtigere i mange virksomheders forretningsdrift.

Hvad har – og hvad har ikke – ændret sig?

Ændringer i branchestandarder, forskrifter og produkter afspejler, hvordan BCDR og andre relaterede discipliner, såsom hændelsesrespons og nødstyring, har udviklet sig med Corona-pandemien.

Der er ikke sket nogen større ændringer relateret til

COVID-19 i de primære BC- og DR-standarder, såsom ISO 22301: 2019, og der er endnu ikke kommet nogle specifikke pandemistandarder. ISO opdaterer sine standarder hvert tredje til femte år, så ændringer relateret til COVID-19 kan komme i løbet af det næste år.

Fordi de enten er blevet udviklet eller opdateret for nylig, har BCDR-standarder, såsom effektanalyser, forsyningskædebeskyttelse og cloud-teknologier, stort set ikke ændret sig gennem COVID-19-pandemien.

Imidlertid har mange BCDR-leverandører tilføjet services, såsom udvikling af pandemiplaner. Nogle har tilføjet softwaremoduler, som er designet til at tackle pandemier, udviklet uddannelsesprogrammer, baseret på erfaringer fra den igangværende pandemi, mens andre tilbyder vejledningsdokumenter om, hvordan man forbereder sig bedst til fremtidige pandemier.

Ændringer i en BCDR-strategi og andre relaterede planer vil være forskellige fra virksomhed til virksomhed, men kan påvirke følgende:

- modeller for fjernarbejde
- hvordan medarbejdere udfører deres arbejde
- hvordan medarbejdere interagerer med hinanden
- organisering af kontorlokaler
- hvordan virksomheden opretholder medarbejdernes sundhed og sikkerhed
- kundebehov
- hvordan virksomheden interagerer med kunder og forsyningskæder.

Langsigtede virkninger af pandemien

Tilgængeligheden af COVID-19-vacciner vil naturligvis have en positiv effekt på den nuværende pandemi.

Men potentielle mutationer kan dog give anledning til nye bølger. I betragtning af den tid, det tager at udvikle, producere og distribuere vacciner, vil BCDR forblive lige så vigtig i de kommende år, som de har været under COVID-19-pandemien.

Planlægning af genoptagelse efter pandemi - traditionelt betragtet som en separat disciplin – vil nu, sandsynligvis, blive en del af BCDR-planlægningen og andre relaterede discipliner. Erfaringer fra COVID-19 har vist, at pandemiforberedelse inden for IT involverer flere aktiviteter, herunder de potentielle ændringer, der er anført ovenfor.

Erfaringerne med fjernarbejde vil sandsynligvis ændre virksomheders politikker og procedurer. Forbedring af metoder til at beskytte medarbejdernes sundhed og produktivitet, håndtering af forsyningskæder samt forbedring af kundeoplevelser er et must. Hovedmålet for forretningen er at øge indtægterne og minimere tab, beskytte omdømme og konkurrencepositioner samt at

tiltrække og fastholde kunder.

Modstandsdygtighed vs. BCDR

Modstandsdygtighed som disciplin opstod for omkring 20 år siden. Og i dag er det defineret som en organisations evne til at reagere på forstyrrende begivenheder og tilpasse forretningsprocesserne i overensstemmelse hermed. Modstandsdygtighed kræver de nødvendige ressourcer og medarbejderengagement for hurtigt at kunne genoptage forretningsdriften.

Nogle ser modstandsdygtighed som en paraplyterm for alle discipliner relateret til forretningsgenoptagelse.

Andre ser modstandsdygtighed som afslutningen eller resultatet af en korrekt udførelse af BCDR og andre praksisser. Uden en BCDR-strategi vil man som udgangspunkt ikke kunne opnå modstandsdygtighed.

Få hjælp til udarbejdelsen

For at udarbejde en BCDR-strategi for 2021 og årene der kommer, skal der tage hensyn til ovenstående procedurer og overvejelser. Det er en kompleks affære og vi foreslår, at du får uvildig og teknisk kompetent assistance.

Kontakt Comby, vi kan hjælpe dig:

Danmark: +45 88 32 60 20
Grønland: +299 34 26 70

Hvad så nu?

Tak fordi du læste med.
Har du spørgsmål til hvordan Comby Denmark kan hjælpe dig med BCDR - Forretningskontinuitet og katastrofehåndtering, er du velkommen til at kontakte os.

COMBY

Japanvej 3, 4200 Slagelse

Tlf. 88 32 60 20
www.comby.dk
info@comby.dk

CVR nr. 40881751