Ministeriet for Samfundssikkerhed og Beredskab

Vejledning til test af reetableringsplaner for samfundskritiske it-systemer

Januar 2025

Indhold

Formål

Denne vejledning har til formål at understøtte statslige myndigheder i at teste reetableringsplaner, så de kan evalueres, og myndighederne derved er bedre rustet til at genoprette data og samfundskritiske it-systemer i tilfælde af skadelige hændelser. For at anvende denne vejledning er det en forudsætning, at al forudgående planlægningsarbejde inden for it-beredskab og kontinuitet foreligger, er godkendt og anvendes af myndigheden.

Vejledningen giver en række gode råd til, hvad statslige myndigheder skal være opmærksomme på før, under og efter udførelsen af en test af en reetableringsplan for et henholdsvis internt og eksternt driftet it-system samt for systemer driftet af Statens It. Vejledningen er udarbejdet, så hvert kapitel kan læses uafhængigt af de andre kapitler. Hvis man skal planlægge en reetableringstest af et system, som driftes af en ekstern leverandør, kan man derfor gå direkte til dette kapitel, når man har læst indledningen.

Vejledningen er udarbejdet med særligt henblik på test af reetableringsplaner for samfundskritiske it-systemer, men er ikke begrænset hertil. Vejledningen er til ledere og medarbejdere, der er involveret i at drifte, udvikle eller risikovurdere kritiske it-systemer og/eller som er ansvarlige for at styre og vedligeholde et it-beredskab. Det kan eksempelvis være ledere med ansvar for informationssikkerhed, systemejere, medarbejdere på sikkerhedsområdet eller beredskabsansvarlige.

Vejledningen bør benyttes i sammenhæng med vejledningerne i risikostyring og leverandørstyring, som findes på sikkerdigital.dk. Vejledningen er udarbejdet af en arbejdsgruppe bestående af Digitaliseringsstyrelsen, Center for Cybersikkerhed (CFCS) og Statens It i samarbejde med systemejende myndigheder og driftsleverandører. Cybersikkerhedsrådet har bidraget med gode råd til brug for denne vejledning.

Indledning

Som en del af organisationens it-beredskab, vil der ofte være behov for at have en eller flere reetableringsplaner, der hver især beskriver, hvordan et eller flere it-systemer kan reetableres i en beredskabssituation, hvor en hændelse har forårsaget systemnedbrud.

Formålet med en reetableringstest er at afprøve en reetableringsplan i praksis ved at udsætte et it-system for et simuleret nedbrud, hvorved it-systemet bliver utilgængeligt. Testen kan simulere en eller flere hændelser, som fx tekniske fejl, cyberangreb eller naturkatastrofer. Formålet med at simulere et nedbrud er, at organisationen kan identificere svagheder og udfordringer og rette op på dem, inden en reel hændelse opstår.

Reetableringstests kan således styrke en organisations evne til at håndtere uventede situationer og katastrofer. Ved at teste og finjustere procedurer trænes organisationen i hurtigt at reetablere driften og undgå langvarige perioder med afbrydelser og utilgængelighed, der kan have negative økonomiske, operationelle eller samfundskritiske konsekvenser.

Endelig kan reetableringstests fremme samarbejde i organisationen. Forskellige teams og interessenter bliver inddraget i planlægningen og udførelsen af testen, hvilket fremmer klar kommunikation samt rolle- og ansvarsfordeling under en hændelse.

Det kræver omhyggelig planlægning at gennemføre en reetableringstest, herunder at den ansvarlige for reetableringstesten har gjort sig overvejelser om systemets kompleksitet og potentielle risici - eventuelt i samarbejde med leverandører.

Ofte vil en reetableringstest tage udgangspunkt i et scenarie for en hændelse, der er identificeret i en risikovurdering. Hvordan systemet er opbygget og understøttet, og hvilket scenarie man tester, kan have indflydelse på, hvordan testen udføres, og hvilke succeskriterier testen har. Det følgende afsnit indeholder eksempler på scenarier, man kan lade sig inspirere af.

Et gennemgående råd er: *keep it simple*. Hvis en organisation ikke har stor erfaring med reetableringstests på hverken internt eller eksternt driftede systemer, skal man hellere starte med at planlægge en overskuelig test på et simpelt system. Jo flere erfaringer man får, jo bedre forudsætninger får man for efterfølgende at øge kompleksiteten.

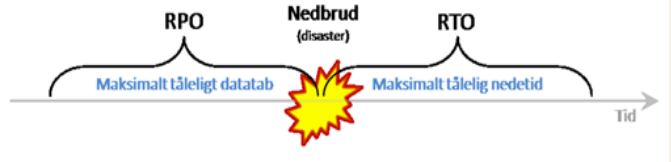
Bemærk, at reetableringstests afprøver et scenarie, hvor der er sket et nedbrud. Denne vejledning beskæftiger sig ikke med tiltag, der har til formål at reducere risikoen for nedbrud fx ved hjælp af redundans eller driftsprocesoptimering, selvom sådanne tiltag ofte vil være yderst relevante for især samfundskritiske systemer.

Overvejelser om kriterier, scenarier og testtyper

Hvordan en reetableringstest konkret udformes, afhænger af systemets beskaffenhed og af en vurdering af systemets risici og kritikalitet.

Som kriterier for en reetableringstest stilles der som regel krav til hvor lang tid, det maksimalt må tage at gendanne et system efter et nedbrud – kaldet maksimal tålelig nedetid eller recovery time objective (RTO), og/eller hvor lang en periode før et nedbrud man maksimalt kan acceptere at miste data fra – kaldet maksimalt tåleligt datatab eller recovery point objective (RPO). Sammenhængen er vist i Figur 1.

Figur 1 - Illustration af RPO og RTO



Behovene for RPO og RTO kan være forskellige fra system til system og kan variere afhængigt af kontekst. Typisk vil krav til RPO og RTO være skærpede for samfundskritiske systemer. Vurderingen af RPO og RTO vil typisk fremgå af organisationens risikovurdering af systemet. Det bemærkes, at der kan være situationer, hvor reetableringstesten anvender en anden RPO og RTO end dem, der fremgår af risikovurderingen fx for at afspejle, at en planlagt test forventes at forløbe hurtigere end en uforudset reel hændelse.

Ved planlægningen af en reetableringstest bør myndigheden overveje, hvilken type test der bedst afdækker de identificerede risici under hensyn til, hvilke ressourcer en given testtype vil kræve. Her er det relevant at overveje, hvilket scenarie der simuleres, hvilken infrastruktur der simuleres ramt samt hvordan systemet er opbygget og understøttet.

Overvejelser om nedbrudsscenarie:

- Eksempler på relevante hændelser at simulere:
    - Strømsvigt
    - Oversvømmelse
    - Brand
    - Hardwarenedbrud
    - Fysisk angreb
    - Hackerangreb
    - Fejlkonfiguration

- Eksempler på infrastruktur, der kan simuleres ude af drift:
    - Lokationer (fx arbejdspladsen, primært datacenter, redundant datacenter og/eller backup-lokation)
    - Datacenterfaciliteter (fx køl eller strøm)
    - Netværk (fx lokalt netværk, internetforbindelser, et/flere VLAN)
    - Centrale services (fx AD eller deployment)
    - Serverhosts eller clustre
    - Enkelte virtuelle servere
    - Storage

- Eksempler på faktorer for it-systemet og -infrastrukturen, der kan inddrages i testens design:
    - Redundans

  - Integrationer og afhængigheder
  - Resultater fra eventuelle tidligere reetableringstests af samme eller lignende systemer

Nedbrudsscenariet kan identificere, hvilken type af reetablering der er behov for at teste. Her kan man med fordel gøre sig følgende overvejelser:

- Testes reetablering af et helt system, en eller flere servere og/eller udvalgte data?
- Testes reetablering fra backup eller (eventuelt spejlet) live data?
- Testes reetableringen i produktionsmiljøet eller på identiske præproduktions- og/eller testmiljøet?
- Testes reetableringen så alle systemets eksterne grænseflader eller indgår blot et udsnit?

Hyppigheden af organisationens reetableringstest bør bero på en risikovurdering, der blandt andet inddrager it-systemets kritikalitet og tekniske omstændigheder. Resultatet af en reetableringstest kan også være med til at pege på, hvornår den næste test bør foretages.

Kritiske it-systemer kan have en højere frekvens af reetableringstest, der i visse tilfælde kan være årlig eller oftere.

Tekniske omstændigheder omkring systemet kan forhindre hyppige reetableringstest. Der kan også være høje omkostninger forbundet med hyppige reetableringstest. Man bør lægge en plan for hyppigheden, der tager udgangspunkt i systemets kritikalitet, krav fra myndigheder og interessenter samt organisationens risikovurdering af systemet og resultatet fra tidligere reetableringstests. Hvis en test fx viste væsentlige udfordringer, kan det give anledning til at genteste den opdaterede reetableringsplan snart efter opdateringen.

Test af reetableringsplaner for internt driftede it-systemer

Det følgende kapitel fokuserer på reetableringstest af internt driftede systemer. Med "internt driftede systemer" refereres der til it-systemer, som er administreret og vedligeholdt internt i en organisation. Det betyder, at organisationen selv har ansvaret for at installere, konfigurere, opdatere, overvåge og supportere systemerne uden i større omfang at involvere eksterne parter som leverandører eller tredjepartsudbydere.

Planlægningsfasen

I det følgende afsnit præsenteres en række punkter, som I skal være opmærksomme på, inden I gennemfører en reetableringstest på et it-system, der er driftet internt.

1. **Afgrænsning:** Med udgangspunkt i jeres eksisterende reetableringsplan samt kritikalitets- og risikovurderinger i jeres systemportefølje og eventuelt inspireret af overvejelserne nævnt i indledningen afgrænses, hvad I ønsker at opnå, og hvilket scenarie reetableringstesten skal afprøve. Herunder definerer I testens succeskriterier i form af fx RTO og RPO. I skal også overveje, hvilke parter der skal orienteres.
2. **Vurdér reetableringsrisici:** Identificér potentielle risici og udfordringer, der kan påvirke opfyldelsen af succeskriterierne. Overvej også, om testen kan risikere at påvirke driften af systemet negativt. Hvad kan gå galt? Hvordan kan disse risici mindskes eller håndteres?
3. **Backup og reetableringsstrategi:** Sikr, at I har en velfungerende backupstrategi på plads. Dette inkluderer regelmæssig sikkerhedskopiering af data og konfigurationer, så jeres backup er i stand til at opfylde RPO-kravene. Sørg også for at have en plan for, hvordan disse data gendannes.
4. **Præproduktionsmiljø, testmiljø eller produktionsmiljø:** I kan vælge at udføre reetableringstest i både præproduktions-, test- og produktionsmiljøet. En reetableringstest har typisk til formål at påvise, at organisationen kan genetablere produktionsmiljøet ved et nedbrud. Hvis I udelukkende udfører testen i et præproduktions- eller testmiljø, skal miljøerne derfor være tilstrækkeligt identiske med produktionsmiljøet, for at testen giver værdi og skaber sikkerhed for, at produktionsmiljøet kan genskabes ved et nedbrud.

   Hvis I ønsker at udføre reetableringstesten i selve produktionsmiljøet, er det oftest en god idé at starte med at teste i et testmiljø. I testmiljøet skal I kunne måle reetableringshastigheden og gendannelsespunktet for systemet. Dette miljø skal afspejle produktionsmiljøet så tæt som muligt. Erfaringerne kan I anvende til kommunikationen til interne og eksterne parter om den forventede utilgængelighed ved reetableringstesten i produktionsmiljøet.

   Hvis I vælger at udføre reetableringstesten i produktionsmiljø, skal I minimere risikoen for afbrydelser eller problemer med systemets drift forårsaget af selve reetableringstesten. Kontrollér, at backup- og reetableringsprocedurer er fuldt funktionelle, og at de eventuelt er blevet testet i et separat testmiljø før testen i produktionsmiljøet.

5. **Dokumentation:** Det er vigtigt at sikre, at al relevant dokumentation er opdateret og tilgængelig. Dette inkluderer reetableringsprocedurer, konfigurationsfiler, systemafhængigheder, kode og andre nødvendige ressourcer. Det sikrer, at erfaringerne bliver gemt og dokumenteret, og at andre medarbejdere fx ville kunne gennemføre opgaven på et senere tidspunkt.
6. **Planlæg**: Læg en plan for, hvornår testen gennemføres, hvor lang tid den forventes at vare, og hvem der bliver involveret eller påvirket.
7. **Involverede parter:** Kommunikér med relevante interessenter, herunder it-teamet, funktionstestere, ledelsen og brugerne, om den forestående reetableringstest. Dette sikrer, at alle er opmærksomme på testen, dens formål og eventuelt forventet utilgængelighed af systemet under reetableringstesten.

Gennemførelsesfasen

I det følgende afsnit præsenteres en række punkter, som I skal være opmærksomme på under gennemførelsen af en reetableringstest af et it-system, der er driftet internt.

Gennemførelsen af en reetableringstest handler om at genskabe systemets tilgængelighed og teste den reetableringsplan, I har udarbejdet på forhånd. Samtidigt skal I være fleksibel nok til at kunne håndtere uforudsete situationer undervejs. Reetableringstesten skal vise, om I kan gennemføre reetableringsplanen som tiltænkt, og hvor den eventuelt har mangler, I skal samle op på ved en efterfølgende evaluering. Dette skal være med til at sikre, at systemet kan gendannes korrekt i tilfælde af et reelt nedbrud.

1. **Etablér baseline:** Efterprøv, om systemet fungerer som det skal, så I efterfølgende har vished for om eventuelle problemer skyldes reetableringstesten eller eksisterende forhold. Vurder også, om systemet kan håndtere belastningen under testscenarierne. Når nedbruddet simuleres, bør I også efterprøve, om det har den forventede effekt på funktionaliteten.
2. **Overvågning:** Overvåg testprocessen nøje for at identificere eventuelle problemer eller afvigelser fra planen. Hold øje med systemets ydeevne, ressourcer og tilgængelighed under hele testen.
3. **Kommunikation**: Hold kommunikationen opdateret med relevante interessenter, herunder it-teamet, ledelsen og eventuelt brugerne. Informér dem om testens status og eventuelle midlertidige ændringer.
4. **Dokumentation:** Registrér alle handlinger, beslutninger og resultater under testen. Dette omfatter fejl, løsninger og eventuelle midlertidige ændringer, der er foretaget i systemet. Notér observerede afvigelser fra planen til brug for evalueringen. Angiv klokkeslæt for alle handlinger, beslutninger og resultater - tidsangivelserne skal blandt andet anvendes til at vurdere, om den ønskede RPO og RTO er overholdt.
5. **Reetableringsprocedurer:** Følg de specificerede reetableringsprocedurer for at sikre, at systemet gendannes korrekt og inden for de ønskede tidsrammer.
6. **Overvågnings- og logningsdata:** Gem alle overvågnings- og logningsdata fra testen for at kunne evaluere resultatet og identificere eventuelle problemer.
7. **Kritiske processer:** Identificér og prioritér de kritiske processer og tjenester, der skal gendannes først. Dette sikrer, at de mest afgørende dele af systemet er tilgængelige hurtigst muligt.
8. **Brugeroplevelse:** Hvis testen foretages i produktionsmiljø, kan I med fordel evaluere, hvordan testen påvirker brugeroplevelsen. Kommuniker eventuelle midlertidige ændringer eller nedetid til brugerne og undgå at påvirke dem negativt.
9. **Overgang til normal drift:** Når testen er færdig, skal I sørge for at implementere en glat overgang til normal driftstilstand. Dette kan inkludere at tilbagerulle ændringer, gendanne data og sikre, at systemet fungerer som forventet.

10. **Funktionstest:** Foretag tekniske- og brugertests for at sikre, at systemet fungerer som forventet efter reetableringen.
11. **Kommunikation:** Informer involverede og påvirkede parter om, at testen er afsluttet.

Efter reetableringstesten

Når reetableringstesten er afsluttet, er det vigtigt at I evaluerer resultaterne sammen med teamet og relevante interessenter. I det følgende afsnit præsenteres en række punkter, I med fordel kan være opmærksomme på efter gennemførelsen af reetableringstesten.

1. **Evaluering af testresultater:** Gennemgå grundigt resultaterne af testen. Identificér, hvad der fungerede godt, og hvor der var udfordringer eller fejl. Ramte I RTO? Var al udstyr tilgængelig? Var der uforudsete ressourcer eller personer, som ikke var tilgængelige? Var der forsinkelser i genetableringen eller lignende?
2. **Fejl og løsninger:** Hvis der opstod fejl eller udfordringer under testen, skal I analysere årsagerne til disse fejl og arbejde på at finde løsninger for at forhindre, at de gentager sig i en faktisk nedbrudssituation.
3. **Dokumentation:** Opdater dokumentationen for reetableringsprocedurer på basis af resultaterne af testen og de eventuelle ændringer, der blev foretaget under testen.
4. **Justering af reetableringsplan:** Brug de opnåede erfaringer til at justere jeres reetableringsplan. Identificér områder, der kræver forbedringer, eller hvor de faktiske forhold afstedkom andre handlinger, end der var planlagt, og opdater jeres planer i overensstemmelse hermed, så planen afspejler den virkelighed, testen påviste.
5. **Kommunikation til interessenter:** Informér de relevante interessenter om resultaterne af reetableringstesten, de trufne beslutninger og de forbedringer, I vil implementere som følge af testens resultater.
6. **Fortsæt med planlægning:** Selv efter en vellykket reetableringstest bør I fortsætte med at opdatere og forfine reetableringsplanen. Fx kan systemopdateringer og organisatoriske ændringer have indflydelse på processerne i reetableringsplanen.
7. **Opfølgning:** Planlæg regelmæssige opfølgningsmøder eller evalueringsperioder med it-teamet og relevante interessenter for at sikre, at I har implementeret de foreslåede forbedringer. I bør som minimum ajourføre reetableringsplanerne årligt. Planlæg og gennemfør en ny reetableringstest, der påviser, at ændringerne til planen virker som tilsigtet.

Test af reetableringsplan for eksternt driftede it-systemer

Når I planlægger en reetableringstest af et it-system, der bliver driftet af en ekstern leverandør, er der ekstra hensyn, I skal tage for at sikre en vellykket test. Dette kapitel præsenterer en række vigtige punkter, som I bør være opmærksomme på før, under og efter en reetableringstest af et eksternt driftet system.

Udbud og leverandørstyring

En af forskellene mellem internt og eksternt driftede systemer er behovet for at indtænke muligheden for reetableringstest allerede i udbudsprocessen og i den løbende leverandørstyring.

Ofte er driften af centrale dele af organisationers it-systemer udliciteret til eksterne leverandører. Det er vigtigt, at I tydeligt definerer leverandørens ansvar i en it-beredskabssituation. Hvis det eksempelvis er et it-system, som en leverandør drifter, der bryder ned, er det leverandøren, der har ansvar for reetablering af it-systemet.

Offentlig myndigheder har ansvar for at stille klare krav til leverandøren og at føre tilsyn med, at leverandørens it-beredskabsplaner lever op til myndighedens krav. Udgangspunktet for at definere kravene til leverandørens beredskab bør – ligesom med det resterende it-beredskabsarbejde – være en risiko- og konsekvensanalyse samt myndighedens overordnede målsætning for it-beredskabet.

Krav til it-beredskabet skal være dokumenteret i leverandøraftaler. Udførelsen af en reetableringstest kan både være med til at teste eller forbedre leverandørens evne til at reetablere, men kan også være en effektiv måde at teste myndighedens leverandørsamarbejde i forbindelse med it-beredskab. Eksempler på aftaleelementer, en reetableringstest kan være med til at efterprøve i praksis er:

- Hvilket ansvar har leverandøren, hvis der sker en ekstraordinær hændelse, der påvirker myndighedens it-systemer?
- Hvilket it-beredskab skal leverandøren have?
- Hvilke snitflader er der mellem myndighedens og leverandøres it-beredskab, og er det aftalt, hvordan der samarbejdes?
- Hvordan skal kommunikationen foregå mellem leverandør og organisation under en hændelse?

Læs mere om generel cybersikkerhed i leverandørforhold i vejledningen på sikkerdigital.dk.

Planlægningsfasen

I det følgende afsnit præsenteres en række punkter, som I skal være opmærksomme på, inden I gennemfører en reetableringstest på et it-system, der er driftet hos en ekstern leverandør.

1. **Afgrænsning:** Med udgangspunkt i jeres eksisterende kritikalitets- og risikovurderinger og i jeres systemportefølje og eventuelt inspireret af overvejelserne nævnt i indledningen, afgrænses, hvad I ønsker at opnå og hvilket scenarie reetableringstesten skal afprøve. Herunder definerer I testens succeskriterier i form af fx RTO og RPO. Ofte vil målsætningerne allerede på forhånd være defineret i aftalen med leverandøren. I skal også overveje, hvilke parter der skal orienteres.

2. **Kommunikation med leverandøren:** Informér jeres eksterne leverandør om, at I vil udføre en reetableringstest. Hyppigheden af reetableringstest kan med fordel være defineret i kontraktgrundlaget med leverandøren. Det kan også være aftalt på forhånd, at reetableringstest afholdes på bestemte tidspunkter af året. I bør under alle omstændigheder genbekræfte aftalerne med leverandøren. Dette inkluderer aftale om formål, omfang, datoer og forventede resultater. Sørg for at etablere en åben og klar kommunikationskanal.
3. **Leverandørens rolle:** Afklar leverandørens rolle i reetableringstesten. Leverandørens rolle kan I med fordel på forhånd have defineret i kontraktgrundlaget, I har indgået med leverandøren om drift af systemet. Selvom leverandørens rolle fremgår af kontraktgrundlaget, er det ofte nødvendigt at I definerer detaljerne omkring den praktiske udførelse. Leverandøren står typisk for selve den tekniske reetablering og tilhørende test af genetableringen, men skal leverandøren fx også være involveret i testprocessen af systemets grænseflader fra en ekstern lokation, eller udfører I den selv? Er det klart defineret, hvordan og i hvilket omfang leverandøren skal bistå med teknisk support eller ressourcer i de forskellige dele af testen?
4. **Backup- og reetableringsstrategier:** Få en fuld forståelse af leverandørens backup- og reetableringsstrategier. Hvordan håndterer de regelmæssig sikkerhedskopiering og reetablering af data? Sørg for, at leverandørens strategier og praktiske håndtering af kravene opfylder kontraktgrundlagets krav, og passer til de krav, der fremgår af jeres risikovurdering af systemet.
5. **Kriterier:** Drøft og afklar med leverandøren, hvordan leverandøren planlægger at opfylde fx RTO- og RPO-målene under testen. Dette bidrager til at undgå misforståelser omkring forventede reetableringstider og datatab. Kravsæt, hvis der er forhold, som leverandøren skal medtage i testen og dokumentationen af testen – det kan fx være krav, der stammer fra myndigheder eller tidligere revisionsgennemgange af jeres styring af systemet.
6. **Dokumentation:** Forventningsafstem med leverandøren, hvilket skriftligt produkt der skal leveres i forbindelse med reetableringstesten – herunder detaljeringsgraden og formatet – det kan fx aftales, i hvor høj grad I forventer uddybende prosa-beskrivelser af testen, og hvor tabelopstillinger er tilstrækkelige.
7. **Testscenarier og planlægning:** Sammen med leverandøren skal I designe realistiske testscenarier og udvikle en detaljeret testplan, der inkluderer tidspunkter, involverede parter og ressourcer. Spørg leverandøren, hvis I er i tvivl om, hvorvidt testscenariet er dækkende for jeres formål.
8. **Sikkerhed:** Vurder, hvordan leverandørens sikkerhedsprocedurer påvirkes af testen. Sørg for, at testaktiviteter ikke kompromitterer datasikkerhed eller systemets integritet.
9. **Præproduktionsmiljø, testmiljø eller produktionsmiljø:** I kan vælge at udføre reetableringstest i både præproduktions-, test- og produktionsmiljøer. En reetableringstest har typisk til formål at påvise, at organisationen kan genetablere produktionsmiljøet ved et nedbrud. Hvis I udelukkende udfører testen i et præproduktions- eller testmiljø, skal miljøerne derfor være tilstrækkeligt identiske med produktionsmiljøet, for at testen giver værdi og skaber sikkerhed for, at produktionsmiljøet kan genskabes ved et nedbrud.

   Hvis I ønsker at udføre reetableringstesten i selve produktionsmiljøet, er det oftest en god idé at starte med at teste i et testmiljø. I testmiljøet skal I kunne måle reetableringshastigheden og gendannelsespunktet for systemet. Dette miljø skal afspejle produktionsmiljøet så tæt som muligt. Erfaringerne kan I anvende til kommunikationen til interne og eksterne parter om den forventede utilgængelighed ved reetableringstesten i produktionsmiljøet.

   Hvis I vælger at udføre reetableringstesten i produktionsmiljø, skal I minimere risikoen for afbrydelser eller problemer med systemets drift forårsaget af selve reetableringstesten. Kontrollér, at backup- og

reetableringsprocedurer er fuldt funktionelle, og at de eventuelt er blevet testet i et separat testmiljø før testen i produktionsmiljøet.

10. **Kommunikation med interessenter:** Informér interessenter om testen og de potentielle påvirkninger på forhånd. Dette inkluderer både internt, hos leverandøren og hos brugere.
11. **Fortrolighedsaftaler:** Vær opmærksom på, at systemets kritikalitet og jeres risikovurdering af systemet kan gøre, at forhold omkring reetableringstesten skal holdes fortrolige – der kan også være eventuelle fortrolighedsaftaler eller kontraktlige forpligtelser i forhold til leverandørens kommercielle driftsforhold, der kan påvirke, hvordan I deler oplysninger om testen med tredjeparter

Gennemførelsesfasen

I det følgende afsnit præsenteres en række punkter, som I skal være opmærksomme på i gennemførelsesfasen.

1. **Etablér baseline:** Efterprøv, om systemet fungerer som det skal, så I efterfølgende har vished for, om eventuelle problemer skyldes reetableringstesten eller eksisterende forhold. Vurder også, om systemet kan håndtere belastningen under testscenarierne. Når nedbruddet simuleres, bør I også efterprøve, om det har den forventede effekt på funktionaliteten.
2. **Overvågning:** Hold øje med testens forløb ved at overvåge de aftalte aktiviteter, resultaterne og eventuelle fejl, der opstår undervejs.
3. **Kommunikation med interessenter:** Orientér interessenter, herunder ledelsen og andre relevante parter, om testens status undervejs. Dette sikrer, at alle er opdaterede omkring fremdriften i testprocessen, den forventede afslutning af testen og den efterfølgende reetablering af tilgængeligheden af systemet. Dette er særligt vigtigt, hvis I udfører testen i produktionsmiljøet, hvor systemet er utilgængeligt under testen. Hvis der er flere interessenter involveret i testen, skal I sikre, at alle arbejder sammen og koordinerer deres aktiviteter effektivt.
4. **Kommunikation med leverandøren:** Hold en åben kommunikationskanal med leverandøren for at kunne diskutere testens fremgang og eventuelle beslutninger i realtid. Sørg for, at alle beslutninger, der tages under testen, er klart kommunikeret og dokumenteret, så der ikke er tvivl omkring handlingsforløbene.
5. **Dokumentation:** Hvis I er til stede under testen, så tag noter om, hvad I observerer under testen, herunder eventuelle beslutninger, fejl og løsninger. Notér tidsangivelser for de observerede centrale handlinger, der indtræf under testen. Dette kan være værdifuld dokumentation senere og bidrage til jeres egen vurdering af, om den ønskede RPO og RTO er overholdt.
6. **Tilbagerulning og normal drift (hvis testen er udført i produktionsmiljø):** Sørg for, at eventuelle midlertidige ændringer, der blev implementeret under testen, er blevet rullet tilbage, og at systemet er tilbage i normal driftstilstand.

Efter reetableringstesten

Efter reetableringstesten er der flere vigtige punkter, som I skal være opmærksomme på for at få de bedst mulige erfaringer ud af testen og for at forbedre systemets beredskab. Her er nogle af de ting, I med fordel kan overveje at gøre, når reetableringstesten er foretaget.

1. **Evaluering af testresultater:** Gennemgå resultaterne af reetableringstesten i samarbejde med jeres leverandør samt eventuelle interessenter i organisationen. Identificér styrker og områder, hvor der er brug for forbedring. Ramte I RTO? Var al udstyr tilgængelig? Var der uforudsete ressourcer eller personer, som ikke var tilgængelige? Var der forsinkelser i genetableringen eller lignende?

2. **Fejl og løsninger:** Hvis der opstod fejl eller udfordringer under testen, skal I arbejde sammen med leverandøren om at identificere årsagerne og implementere løsninger for at forhindre, at fejlene gentages.
3. **Dokumentation:** Sørg for at dokumentationen for systemets reetableringsprocedurer bliver opdateret med resultaterne fra testen og de tiltag, der blev taget for at håndtere eventuelle udfordringer.
4. **Forbedringer:** Samarbejd med jeres leverandør om at bruge erfaringerne fra testen til at identificere områder, hvor I kan styrke reetableringsstrategien og -processerne. Dette kan inkludere tilpasninger af fx kommunikation.
5. **Kommunikation med interessenter:** Informér alle relevante interessenter om resultatet af reetableringstesten og de beslutninger, der er blevet truffet vedrørende eventuelle forbedringer.
6. **Opfølgning:** Planlæg opfølgningsmøder for at sikre, at de foreslåede forbedringer er blevet gennemført, og at systemet fortsat er parat til at håndtere eventuelle nedbrud. Planlæg en ny reetableringstest, der påviser, at erfaringerne og ændringerne har medført de ønskede resultater.
7. **Vurdér det nuværende kontraktgrundlag - og tag stilling til eventuelle ændringer til kommende genudbud:** Overvej, om erfaringerne fra testen giver anledning til at tilpasse det eksisterende kontraktgrundlag med leverandøren gennem allonger. Erfaringerne kan også give anledning til at I justerer udbudskriterier eller nyt kontraktgrundlag, når driften af systemet skal genudbydes.

Test af reetableringsplaner for systemer driftet af Statens It

Der er nogle enkelte forskelle på at foretage en genetableringstest hos Statens It og hos andre leverandører. Dette kapitel præsenterer en række vigtige punkter, som I bør være opmærksomme på før, under og efter en reetableringstest af et system, der driftes hos Statens It.

Planlægningsfasen

Følgende skal I være opmærksomme på, når I planlægger at gennemføre en reetableringstest på et it-system, der er driftet af Statens It.

1. **Afgrænsning:** Med udgangspunkt i jeres eksisterende kritikalitets- og risikovurderinger og i jeres systemportefølje og eventuelt inspireret af overvejelserne nævnt i indledningen, afgrænses, hvad I ønsker at opnå og hvilket scenarie reetableringstesten skal afprøve. Herunder definerer I testens succeskriterier i form af fx RTO og RPO. Det er en god idé tidligt at være i dialog med Statens It om målsætningerne. I skal også overveje, hvilke parter I skal orientere. Afhængigt af driftsmodel, kan det være relevant at inddrage andre parter, fx systemleverandør.
2. **Kommunikation med Statens It:** Informér Statens It om, at I vil udføre en reetableringstest ved at lave en bestilling gennem Statens Its serviceportal. Dette inkluderer formål, omfang, datoer og forventede resultater. Sørg for at have en åben og klar kommunikation så tidligt som muligt i forløbet.
3. **Statens Its rolle:** Afklar Statens Its rolle i reetableringstesten. Brug Statens It som sparringspartner allerede ved udarbejdelse af reetableringsplanen. Så kan Statens It sikre, at der stilles de nødvendige ressourcer til rådighed, når reetableringstesten skal gennemføres.
4. **Backup- og reetableringsstrategier:** Få en fuld forståelse af Statens Its backup- og reetableringsstrategier. Hvordan backup tages fremgår af aftalegrundlaget mellem Statens It og jer som kunde. Eventuelle afvigelser fra standard vil fremgå af allonge.
5. **Kriterier:** Drøft og afklar med Statens It, hvordan det planlægges at opfylde fx RTO- og RPO-målene under testen. Dette bidrager til at undgå misforståelser omkring forventede reetableringstider og datatab. Italesæt, hvis der er forhold, som skal medtages i testen og dokumentationen af testen – det kan fx være krav, der stammer fra myndigheder eller tidligere revisionsgennemgange af jeres styring af systemet.
6. **Dokumentation:** Forventningsafstem med Statens It, hvilket skriftligt produkt der skal leveres i forbindelse med reetableringstesten – herunder detaljeringsgraden og formatet – det kan fx aftales, i hvor høj grad I forventer uddybende prosa-beskrivelser af testen, og hvor tabelopstillinger er tilstrækkelige.
7. **Testscenarier og planlægning:** Sammen med Statens It skal I designe realistiske testscenarier og udvikle en detaljeret testplan, der inkluderer tidspunkter, involverede parter og ressourcer. Spørg Statens It, hvis I er i tvivl om, hvorvidt testscenariet er dækkende for jeres formål.
8. **Sikkerhed:** Vurder, hvordan Statens It sikkerhedsprocedurer påvirkes af testen. Sørg for, at testaktiviteter ikke kompromitterer datasikkerhed eller systemets integritet.

9. **Præproduktionsmiljø, testmiljø eller produktionsmiljø:** I kan vælge at udføre reetableringstest i både præproduktions-, test- og produktionsmiljøer. En reetableringstest har typisk til formål at påvise, at organisationen kan genetablere produktionsmiljøet ved et nedbrud. Hvis I udelukkende udfører testen i et præproduktions- eller testmiljø, skal miljøerne derfor være tilstrækkeligt identiske med produktionsmiljøet, for at testen giver værdi og skaber sikkerhed for, at produktionsmiljøet kan genskabes ved et nedbrud.

   Hvis I ønsker at udføre reetableringstesten i selve produktionsmiljøet, er det oftest en god idé at starte med at teste i et testmiljø. I testmiljøet skal I kunne måle reetableringshastigheden og reetableringspunktet for systemet. Dette miljø skal afspejle produktionsmiljøet så tæt som muligt. Erfaringerne kan I anvende til kommunikationen til interne og eksterne parter om den forventede utilgængelighed ved reetableringstesten i produktionsmiljøet.

   Hvis I vælger at udføre reetableringstesten i produktionsmiljø, skal I minimere risikoen for afbrydelser eller problemer med systemets drift forårsaget af selve reetableringstesten. Kontrollér, at backup- og reetableringsprocedurer er fuldt funktionelle, og at de eventuelt er blevet testet i et separat testmiljø før testen i produktionsmiljøet.

10. **Kommunikation med interessenter:** Informér interessenter om testen og de potentielle påvirkninger på forhånd. Dette inkluderer både internt, hos Statens It og eventuelle andre leverandører samt hos brugere.

11. **Fortrolighedsaftaler:** Vær opmærksom på eventuelle fortrolighedsaftaler eller kontraktlige forpligtelser, der kan påvirke, hvordan I deler oplysninger om testen med tredjeparter.

Gennemførelsesfasen

I det følgende afsnit præsenteres en række punkter, I skal være opmærksomme på i gennemførelsesfasen.

1. **Etablér baseline:** Efterprøv, om systemet fungerer som det skal, så I efterfølgende har vished for, om eventuelle problemer skyldes reetableringstesten eller eksisterende forhold. Vurder også, om systemet kan håndtere belastningen under testscenarierne. Når nedbruddet simuleres, bør I også efterprøve, om det har den forventede effekt på funktionaliteten.

2. **Overvågning:** Hold øje med testens forløb ved at overvåge de aftalte aktiviteter, resultaterne og eventuelle fejl, der opstår undervejs.

3. **Kommunikation med interessenter:** Orientér interessenter, herunder ledelsen og andre relevante parter, om testens status undervejs. Dette sikrer, at alle er opdaterede omkring fremdriften af testprocessen, den forventede afslutning af testen og den efterfølgende reetablering af tilgængeligheden af systemet. Dette er særligt vigtigt, hvis I udfører testen i produktionsmiljøet, hvor systemet er utilgængeligt under testen. Hvis der er flere interessenter involveret i testen, skal I sikre, at alle arbejder sammen og koordinerer deres aktiviteter effektivt.

4. **Kommunikation med Statens It:** Hold en åben kommunikationskanal med Statens It for at kunne diskutere testens fremgang og eventuelle beslutninger i realtid. Sørg for, at alle beslutninger, der tages under testen, er klart kommunikeret og dokumenteret, så der ikke er tvivl omkring handlingsforløbene.

5. **Dokumentation:** Hvis I er til stede under testen, så tag noter om, hvad I observerer under testen, herunder eventuelle beslutninger, fejl og løsninger. Notér tidsangivelser for de observerede centrale handlinger, der indtræf under testen. Dette kan være værdifuld dokumentation senere og bidrage til jeres egen vurdering af, om den ønskede RPO og RTO er overholdt.

6. **Tilbagerulning og normal drift (hvis testen er udført i produktionsmiljø):** Sørg for, at eventuelle midlertidige ændringer, der blev implementeret under testen, er blevet rullet tilbage, og at systemet er tilbage i normal driftstilstand.

Efter reetableringstesten

Efter reetableringstesten er der flere vigtige punkter, som I skal være opmærksomme på for at få de bedst mulige erfaringer ud af testen og for at forbedre systemets beredskab. Her er nogle af de ting, I med fordel kan overveje at gøre, når reetableringstesten er foretaget.

1. **Evaluering af testresultater:** Gennemgå resultaterne af reetableringstesten i samarbejde med Statens It samt eventuelle interessenter i organisationen. Identificér styrker og områder, hvor der er brug for forbedring. Ramte I RTO? Var al udstyr tilgængelig? Var der uforudsete ressourcer eller personer, som ikke var tilgængelige? Var der forsinkelser i genetableringen eller lignende?
2. **Fejl og løsninger:** Hvis der opstod fejl eller udfordringer under testen, skal I arbejde sammen med Statens It om at identificere årsagerne og implementere løsninger for at forhindre, at fejlene gentages.
3. **Dokumentation:** Sørg for at dokumentationen for systemets reetableringsprocedurer bliver opdateret med resultaterne fra testen og de tiltag, der blev taget for at håndtere eventuelle udfordringer.
4. **Forbedringer:** Samarbejd med Statens It om at bruge erfaringerne fra testen til at identificere områder, hvor I kan styrke reetableringsstrategien og -processerne. Dette kan inkludere tilpasninger af fx kommunikation.
5. **Kommunikation med interessenter:** Informér alle relevante interessenter om resultatet af reetableringstesten og de beslutninger, der er blevet truffet på baggrund af eventuelle forbedringer.
6. **Opfølgning:** Planlæg opfølgningsmøder for at sikre, at de foreslåede forbedringer er blevet gennemført, og at systemet fortsat er parat til at håndtere eventuelle nedbrud. Planlæg en ny reetableringstest, der påviser, at erfaringerne og ændringerne har medført de ønskede resultater.
7. **Aftal:** Overvej, om erfaringerne fra testen giver anledning til at tilpasse ansvarsfordelingen med Statens It. Er driftsmodel, systemkritikalitet og eventuel allonge retvisende og hensigtsmæssig?