



Energistyrelsen

Vejledning: Backup-styring

Kontor/afdeling
Beredskab

Dato
06-07-2026



Energistyrelsen

Energistyrelsen

Carsten Niebuhrs Gade 43
1577 København V

T: +45 3392 6700
E: ens@ens.dk

www.ens.dk



Versionshistorik

Versions-nr.	Ændret	Ændret af	Kommentarer
1	10.07.2025	Søren Egede, konsulent	Dokumentet blev oprettet.
1.1	17.11.2025	Stine Buemann	Tydeliggørelse af fortrolighedsgrad i materialet i sidefod og på forsiden. Konsekvensændring af 'BEK' til 'bekendtgørelsen'.
1.2	06.07.2026	Stine Buemann	Fortrolighedsstempel fjernet.



Indhold

Indledning	4
Forudsætningskabende vurdering af systemer og netværk	4
Fastlæggelse af Recovery Point Objective (RPO)	5
Fastlæggelse af Maximum Tolerable Downtime (MTD)	5
Fastlæggelse af (Recovery Time Objective (RTO)	6
Politik og procedurer for backup-styring (§ 58)	6
Backup-frekvens	7
Opbevaring og arkivering	7
Cybersikkerhed og adgangskontrol	7
Test af backup	8
Dokumentation	8
Backup af forsyningskritiske net- og informationssystemer (§ 59, stk. 1 og 2)	9
Eksempel 1: Decentral backup	9
Eksempel 2: Central backup	10
Backup af forsyningskritiske net- og informationssystemer i niveau 4 og 5- virksomheder (§ 59, stk. 3)	11
Eksempel: Central backup-løsning med flere særskilt opbevarede kopier	12



Indledning

Virksomhederne i niveau 2-5 i el-, gas-, brint-, olie-, fjernvarme- og fjernkølingssektoren skal, jf. bekendtgørelse om modstandsdygtighed og beredskab i energisektoren nr. 260 af 6. marts 2025 (bekendtgørelsen) § 58, have en politik og procedurer for backup-styring for egne net- og informationssystemer. Samtidig skal de, jf. § 59, tage backup af egne forsyningskritiske net- og informationssystemer og netværkskonfigurationer, så de kan genoprette systemerne og netværksinfrastrukturen for forsyningskritiske net- og informationssystemer.

Formålet med denne vejledning er at give sektorens virksomheder inspiration til backup-styring. Vejledningen gennemgår og forklarer de konkrete krav i bekendtgørelsen og giver eksempler på, hvordan backup-sikringen kan gennemføres. Vejledningen beskriver metoder til, hvordan virksomhederne kan identificere deres tidsrammer for backup og genetableringstider. Vejledningen berører indledningsvist også kort § 19, stk. 3, nr. 5 om identificering af tidsrammer for genoprettelse og nedetid, som er forudsætningsskabende for alt arbejde med backup.

Forudsætningsskabende vurdering af systemer og netværk

Ifølge bekendtgørelsen § 19, stk. 3, nr. 5, litra a og b skal virksomhederne have procedurer for genoprettelse af net- og informationssystemer, herunder beskrivelser af:

- Den maksimalt accepterede nedetid og datatab for net- og informationssystemer. Det er det, man også kalder Maximum Tolerable Downtime (MTD) og Recovery Point Objective (RPO).
- Virksomhedens målsætning for genetableringstid og metoderne til at genoprette net- og informationssystemer fra backup. Dette kalder man også Recovery Time Objective (RTO).

MTD, RPO og RTO er nogle af nøglekoncepterne i disaster recovery og business continuity planning. I det følgende gennemgår vi en række eksempler på, hvordan det kan bruges til at definere jeres behov i forhold til backup og reetableringstider. Det er fælles for alle eksemplerne, at det netop er eksempler med hypotetiske oplysninger. Da forskellige implementeringer i forskellige virksomheder kan give store variationer, vil det følgende ikke nødvendigvis være relevant for alle virksomheder. Det er meget vigtigt, at I selv foretager vurderinger af jeres egne RPO'er, MTD'er og RTO'er.



Fastlæggelse af Recovery Point Objective (RPO)

Hvor meget data kan virksomheden tåle at tabe?

RPO definerer, hvor ofte I som virksomhed skal tage backup, og hvor gammel en backup I er villige til at gendanne data fra. RPO omhandler primært data, altså den maksimale datamængde, I kan acceptere at miste ved en hændelse.

Eksempel

Systemers RPO

SCADA	Ingen RPO, da kraftværkets SCADA er meget statisk. Vi vil miste den løbende optimering, som er lavet over flere år, jo længere vi går tilbage.
Markedssystem	En time. Hvis data er mere end en time gammel, er den ubrugelig.
GIS-system	Seks måneder. Hvis data er mere end seks måneder gammel, vil det medføre, at der mangler essentielle oplysninger om anlæg og stationer.

Når I har defineret RPO, kan I begynde at arbejde med at fastlægge kriterierne for, hvordan I skal tage backups og i hvilke intervaller, samt hvor gamle backups må være, hvis det skal give mening at gemme dem.

Fastlæggelse af Maximum Tolerable Downtime (MTD)

Hvad er den absolut længste tid, systemet må være nede?

Hvor lang tid kan I tåle, at et givent net- og informationssystem er ude af drift? I skal som virksomhed have defineret tidsaspektet på forretningsniveau. Eksempel på dette kan være følgende:

Eksempel

Systemers MTD

SCADA	En time
Markedssystem	Fem timer
GIS-system	24 timer

Analysen i eksemplet viser, at virksomheden har fastlagt, at den ikke kan tåle at være uden SCADA i en time, markedssystemet i fem timer og GIS-systemet i 24 timer. Disse tidssætninger angiver den maksimale acceptable nedetid, og derfor skal virksomheden kunne genetablere systemerne inden for hhv. en time, fem timer og 24 timer. Hvis virksomheden ikke kan gennemføre genetableringen inden for den tidsramme, vil det have alvorlige konsekvenser for leveringen af virksomhedens tjeneste.



Fastlæggelse af (Recovery Time Objective (RTO))

Hvor hurtigt skal systemet være oppe igen efter et nedbrud?

RTO er fastlæggelsen af, hvor hurtigt I kan genetablere virksomhedens forsynings-kritiske netværks- og informationssystemer. Det essentielle i fastlæggelsen af jeres RTO for systemer er, at I skal have tidssætninger, som er under virksomhedens fastsatte MTD.

Eksempel

Systemers RTO

SCADA	30 minutter
Markedssystem	2,5 timer
GIS-system	12 timer

Ved øvelser og genetableringer af systemerne skal I som virksomhed finde ud af, om I kan skabe procedurer og genetableringsplaner, som imødekommer, at I kan genetablere de forsyningskritiske netværks- og informationssystemer inden for RTO'en. De gyldne regler er følgende:

- MTD er højere end ens RTO, altså er man inden for den acceptable tids-ramme og kan fokusere på optimering af processer og planer, så man kan genetablere hurtigere og hurtigere.
- RTO er højere end ens MTD. Det er vurderet, at virksomheden ikke kan genetablere forsyningskritiske net- og informationssystemer, før man over-skridet virksomhedens definerede MTD. Dermed har man identificeret et behov for at kunne genetablere systemerne hurtigere, og dermed for at kunne genetablere før det får store konsekvenser for virksomhedens leve-ring af tjenesten.

Politik og procedurer for backup-styring (§ 58)

Backup-styring udgør en central del af de fleste virksomheders cybersikkerheds-strategi og risikostyring. Formålet er at sikre god tilgængelighed af data og syste-mer og en hurtig reetablering efter fejl eller hændelser, såsom systemnedbrud, cy-berangreb eller utilsigtet datatab.

Bekendtgørelsen § 58 stiller krav om, at virksomhederne i sektoren skal have en politik og procedurer for backup-styring for deres net- og informationssystemer, og der stilles krav om, at politikken som minimum skal indeholde en minimumsfre-kvens for at tage backup samt passende opbevaringstider for backup, jf. § 19, stk. 3, nr. 5, litra a. De næste afsnit af vejledningen beskriver de områder, som politik-ken og procedurerne bør omfatte.



Backup-frekvens

I skal risikovurdere backup-frekvensen, så I tager højde for den, jeres egne behov, for virksomhedens datatyper og systemernes kritikalitet. Politikken for backup-styring skal som minimum indeholde en minimumsfrekvens for at tage backup samt passende opbevaringstider for backup, jf. § 19, stk. 3, nr. 5, litra a, jf. bekendtgørelsen § 58, 2. pkt.

En generel vurdering af backup-frekvensen kunne være:

- **Daglig backup:** Backup bør udføres dagligt for alle kritiske systemer og data, herunder systemkonfigurationer, forretningskritiske applikationer og databaser.
- **Ugentlig backup:** Backup kan udføres ugentligt for øvrige ikke-kritiske systemer og arkivdata.
- **Ad hoc-backup:** Backup kan udføres i forbindelse med større ændringer, systemopgraderinger eller før implementering af ny funktionalitet.

Det er væsentligt, at I under risikovurderingen også tager højde for reetableringstiden, da denne kan have indvirkning på den nødvendige backup-frekvens. I bør også oprette detaljerede logfiler for alle backups.

Opbevaring og arkivering

Jeres risikovurdering af opbevaringstid, opbevaringssted og informationer om arkivering bør være baseret på relevant viden og identificeringen af tiderne ift. RPO og RTO. Nedenfor er der en generel beskrivelse af backup, opbevaring og arkivering:

- **Daglige backups:** Opbevares i minimum 30 dage (anbefalet 90 dage).
- **Ugentlige backups:** Opbevares i minimum tre måneder (anbefales ni måneder).
- **Månedlige backups** (hvor relevant): Arkiveres i 12 måneder afhængigt af dataklassifikation og lovgivningsmæssige krav.
- **Langtidsopbevaring:** For visse systemer eller data kan der være behov for opbevaring i op til fem år.

Backups bør opbevares både lokalt og off site. I bør implementere den såkaldte 3-2-1 backup-regel, hvilket indebærer tre kopier af data, som er opbevaret på to forskellige medier, hvoraf en kopi skal være off site.

Cybersikkerhed og adgangskontrol

Backup er også et attraktivt mål for en angriber, da der ofte gemmer sig følsomme oplysninger og vigtige konfigurationer i backup-filer. Ved angrebet på HackingTeam



i 2015 blev backup anvendt som et af angrebsmålene.¹ Derfor er det afgørende, at backup-løsningerne er ordentligt sikrede.

Nogle generelle anbefalinger er:

- Backup-filer krypteres under overførsel, og når de opbevares.
- Adgangen til backup-systemer er begrænset til autoriseret personale.
- Adgangen til backup-systemer sker via et management-netværk.

Test af backup

Det er vigtigt at teste virksomhedens backup for at sikre, at den virker. Det anbefales, at I vurderer behovet for frekvensen af testning af backups. Denne frekvens bør afspejle, hvor vigtige enheden og systemerne er, samt RPO som beskrevet ovenfor.

En generel test kan deles op i tre dele:

- **Logverifikation:** Dette bør gøres for alle backups. Det inkluderer at verificere, at backuppen er gennemført korrekt ved at gennemgå backup-loggen.
- **Filverifikation:** Dette består i at udføre en test af udvalgte filer eller objekter fra en specifik backup, hvor man foretager en gendannelse af det pågældende udsnit og efterfølgende verificerer, at det fungerer som forventet. Dette bør gøres regelmæssigt og minimum en gang i kvartalet.
- **Full restore:** Der laves en fuld restore af en server eller anden enhed, hvor I verificerer, at denne kan reetableres og er operationel efter restore. Dette skal gøres periodisk og minimum en gang om året for virksomheder i niveau 4-5.

For at sikre en afklaring af, om reetableringstiden lever op til jeres krav til, hvor hurtigt I skal kunne tilgå og anvende systemer og enheder, anbefales det, at I måler tiden for alle restore-tests.

Dokumentation

Dokumentation er vigtigt, også for backups. Dokumentation bør ikke kun fastlægge, om den enkelte backup er gået godt eller ej. For at vurdere, om I lever op til jeres egne politikker og procedurer, er det også vigtigt, at I sikrer jer evidens om:

- Alle backup-aktivitetens status og revision.
- At der er en log over hovedindholdet af den enkelte backup.

Politikken bør revideres mindst én gang årligt og ved væsentlige ændringer.

¹ https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/?utm_source=chatgpt.com#page-2



Backup af forsyningskritiske net- og informationssystemer

(§ 59, stk. 1 og 2)

Nedenfor er der beskrevet to eksempler på, hvordan en backup- og restore-implementering kan laves.

Eksempel 1: Decentral backup

En decentral backup oprettes per lokation, fx et kraftværk, en transformerstation eller lignende. Der skal laves backup af forsyningskritiske net- og informationssystemer og netværkskonfigurationer, så det er muligt at genoprette systemerne og kommunikationen inden for en acceptabel tidsramme.

Tidsrammen afhænger af virksomheden og af, hvor hændelsen er opstået. Svaret på dette findes i de fastsatte tider for RPO, RTO og MTD for den enkelte virksomhed. I dette eksempel er det vurderet, at dette er inden for én time, og det forventes, at man kan leve med data, der er op til én dag gamle ved opstart efter restore.

I dette tilfælde ville der skulle laves følgende:

- **Backup-frekvens:** En daglig, fuld backup.
- **Opbevaring:** 90 dage og arkivering i fem år (rotationsprincip kan anvendes).
- **Sikring af backup:** Backups, der er lagret uden for det forsyningskritiske netværk, skal være krypteret. Adgang til backup bør være adgangsstyret.
- **Test af backups:** Backups bør testes for validitet periodisk, herunder ved brug af log- og filverifikation samt årlig test af fuld restore af fx en server.
- **Dokumentation:** Der laves en datalog for alle backups.

Nedenfor er der beskrevet et eksempel på en implementering:

Virksomheden i eksemplet har valgt at lave en decentral backup-løsning, hvor der tages backup lokalt. For at kunne lave en restore af hele systemet, inklusive data, der ikke er ældre end én dag, laves der daglige backups (fuld backup).

Det er vigtigt at have god modstandsdygtighed mod cyberangreb, og derfor implementerer virksomheden i eksemplet en backup-opbevaring på 90 dage samt arkivering i fem år. Dette er vigtigt for at kunne beskytte virksomhedens systemer og enheder mod malware, der har været til stede i systemet i længere tid og er blevet en del af backuppen. Alle backups krypteres for at sikre, at de ikke kan misbruges af uautoriserede. På den måde opnår virksomheden både fleksibilitet og sikker lagring. Backups opbevares på lokationen, men på et særskilt management-netværk.

For at validere og dokumentere backups skal virksomheden have en proces, hvor backups gennemgås for fejl, og hvor man laver restore-tests månedlig og årligt.



Den månedlige test omfatter udvalgte filer, som restores og testes for indhold, mens den årlige test involverer en udvalgt server eller enhed, hvor der udføres en fuld restore (disaster recovery) af enheden.

Backup-rotationsprincip

Der findes forskellige typer af backup-rotationsprincipper, såsom FIFO, GFS og Hanoi.

Et backup-rotationsprincip beskriver, hvordan man roterer og håndterer back-ups, så man undgår at gemme unødvendigt store datamængder – fx ved ikke at skulle opbevare alle backups i fem år.

FIFO (First In, First Out):

FIFO-princippet betyder, at den ældste backup bliver slettet, når en ny backup oprettes, og der ikke er mere plads eller kapacitet til nye data. Det fungerer som en kø, hvor den første backup, der kommer ind, også er den første, der ryger ud.

GFS (Grandfather-Father-Son):

GFS er en hierarkisk backup-strategi, hvor data gemmes i tre niveauer:

- Søn: Daglige backups (korttidsopbevaring).
- Far: Ugentlige backups (mellemlangsigtet opbevaring).
- Bedstefar: Månedlige eller kvartalsvise backups (langtidsopbevaring).

Hanoi (Tower of Hanoi):

Hanoi-strategien er baseret på det matematiske spil "Tower of Hanoi". Den bruger et mønster, hvor hver backup kun bliver overskrevet efter et specifikt antal dage, afhængigt af hvor ofte backuppen er blevet taget før. Det giver en mere spredt og intelligent opbevaring af backups over tid.

Eksempel 2: Central backup

I dette eksempel laves der backup centralt. Dette gør man enten ved at tage back-ups over netværket eller ved at anvende lokale agenter, som tager backup og sender den til en central lokation.

Virksomheden skal tage backup af de forsyningskritiske net- og informationssystemer samt netværkskonfigurationer, så det er muligt at genoprette systemerne og kommunikationen inden for en acceptabel tidsramme. Tidsrammen afhænger af virksomheden og af, hvor hændelsen er opstået. Svaret på dette findes i de fastsatte tider for RPO, RTO og MTD for den enkelte virksomhed. I dette eksempel har



virksomheden vurderet, at dette er inden for én time, og det forventes, at man kan leve med data, der er op til én dag gamle ved opstart efter restore.

Når man bruger en central backup, anbefales det, at man har udstyr on site som en beredskabssikring. Dette kan være en NAS eller andet, som kan bruges, hvis lokationen er isoleret, og man har brug for en backup.

Der bruges samme information som i eksempel 1:

- **Backup-frekvens:** En daglig fuld backup.
- **Opbevaring:** 90 dage og arkivering i fem år (rotationsprincip kan anvendes).
- **Sikring af backup:** Backups, der er lagret uden for det forsyningskritiske netværk, skal være krypteret. Adgang til backup bør være adgangsstyret.
- **Test af backups:** Backups bør testes for validitet periodisk, herunder ved brug af log- og filverifikation samt årlig test af en fuld restore af fx en server.
- **Dokumentation:** Der laves en datalog for alle backups.

Virksomheden i eksemplet har valgt en central backup-løsning for de forsyningskritiske net- og informationssystemer. Backup-systemet er placeret centralt og indgår som en del af det forsyningskritiske område. For at kunne restore hele systemet, inklusive data, der ikke er ældre end én dag, udføres der daglige fulde backups.

Tidligere hændelser har vist, at malware, såsom ransomware, kan være inaktivt i en periode, før det aktiveres og inficerer backups. Derfor er det vigtigt at have en lang opbevaringstid som fx 90 dage samt arkivering i fem år. Derudover vil virksomheden skulle lagre to kopier af backuppen – én lokalt og én centralt. Disse backups er krypterede for at sikre, at de ikke kan læses af uautoriserede.

For at validere disse backups har virksomheden i eksemplet udarbejdet en proces for dokumentation, hvor backup-logs gennemgås for fejl. Virksomheden udfører samtidig restore-testning både månedligt og årligt. Den månedlige test omfatter udvalgte filer, som restores og testes for indhold, mens den årlige test involverer en udvalgt server eller enhed, hvor der udføres en fuld restore (disaster recovery) af enheden.

Backup af forsyningskritiske net- og informationssystemer i niveau 4 og 5-virksomheder (§ 59, stk. 3)

For virksomheder i niveau 4 og 5 stiller bekendtgørelsen § 59, stk. 3, ydermere krav om, at virksomhederne skal tage backups i flere kopier, og at disse kopier skal opbevares særskilt. Her kan eksemplet være:



Eksempel: Central backup-løsning med flere særskilt opbevarede kopier

Virksomheden implementerer en central backup-løsning, hvor virksomheden enten udfører backup over netværket, eller ved at lokale agenter tager backup og sender den til en central placering.

Det er et krav i bekendtgørelsen, at der skal tages backup af forsyningskritiske net- og informationssystemer og netværkskonfigurationer, så det er muligt at genoprette systemerne og kommunikation inden for en acceptabel tidsramme. Tidsrammen afhænger af virksomheden og af, hvor hændelsen er opstået. Svaret på dette findes i de fastsatte tider for RPO, RTO og MTD for den enkelte virksomhed.

I dette eksempel har virksomheden vurderet, at dette er inden for én time. Virksomheden accepterer dermed at leve med data, der er op til én dag gamle ved opstart efter restore. Bekendtgørelsen stiller desuden krav om, at virksomheden skal have flere kopier af backuppen, og at en backup skal være tilgængelig, selvom de forsyningskritiske områder ikke er tilgængelige.

Derfor har virksomheden i eksemplet besluttet:

- **Backup-frekvens:** En daglig fuld backup.
- **Opbevaring:** 90 dage og arkivering i fem år (rotationsprincip kan anvendes).
- **Backup 3-2-1:** Der tages tre backupkopier på to forskellige medier, hvor en af kopierne skal være offline og hurtigt tilgængelig.
- **Sikring af backup:** Backups, der er lagret uden for det forsyningskritiske netværk, skal være krypteret. Adgang til backup bør være adgangsstyret.
- **Test af backups:** Backups bør testes for validitet periodisk, herunder ved brug af log- og filverifikation samt årlig test af restore fra server.
- **Dokumentation:** Der laves en datalog for alle backups.

Virksomheden har valgt at lave en central backup-løsning for de forsyningskritiske net- og informationssystemer. Backup-systemet er placeret centralt og er en del af det forsyningskritiske område. For at kunne restore hele systemet med data, der ikke er ældre end en dag, laves der daglige, fulde backups.

Da det er kendt, at malware som fx ransomware kan ligge i systemet i en periode, før det aktiveres for at inficere backups, er det vigtigt med en lang opbevaringstid som 90 dage og arkivering i fem år.

Virksomheden vil lagre tre kopier af alle backups:

- En, som ligger centralt og er online.
- En, som ligger på en reservelokation og også er online.



- En, som er placeret offline i et brandsikkert skab.

Alle kopier er tilgængelige inden for en time.

For at sikre, at en angriber ikke kan få adgang til de online backups, er de alle krypterede. Det ville være muligt ikke at have krypterede backups, hvis de blev opbevaret inden for det forsyningskritiske område. For enkelthedens skyld har man valgt, at alle backups skal være krypterede – både under overførsel og når de er lagret.

For at validere backups og lave dokumentation etablerer virksomheden en proces, hvor backuplogs gennemgås for fejl, og der udføres restore-test hver måned og hvert år. Den månedlige test omfatter restore af udvalgte filer, som derefter testes for indhold, mens den årlige test indebærer restore af en udvalgt server eller enhed, hvor der udføres en fuld restore (disaster recovery) af enheden.