NIS2-koncepter til
kommunal implementering

Hændelseshåndtering

KL

Forord

Som del af den fælleskommunale digitale handlingsplan 2021-2025 har KL i samarbejde med en række kommuner og med ekstern konsulentbistand igangsat projekt til støtte for kommunernes arbejde med cybersikkerhed, specifikt ift. implementering af NIS2. Leverancen herfra er en kommunale NIS2-drejebog. Dette dokument er et kapitel til denne drejebog.

Den fælleskommunal NIS2-drejebog har til formål at understøtte og inspirere kommunernes arbejde med egen cybersikkerhed. Dette gøres via redskaber, skabeloner, årshjul, eksempler mv. der indgår i drejebogen. 16 kommuner har i fire temagrupper bidraget med egen erfaring og input, således at materialet afspejler kommunale behov og vilkår, baseret på kommunal erfaring, baseret på kommunal erfaring.

Drejebogen indeholder bud på, hvordan man som kommune kan arbejde med fire centrale NIS2-temaer: Risikovurdering, Ledelsesansvar, Forsyningskædesikkerhed og Hændelseshåndtering.

De to første Drejebogskapitler (Ledelsesansvar og Risikovurdering) publiceres i december 2025 og kan frit bruges. De to følgende drejebogskapitler forventes publiceret i løbet af februar 2026, hvor materialet for alle fire kapitler udgives i én samlet kommunal NIS2-drejebog.

Drejebogen giver anbefalinger til oversættelse og operationalisering - men ikke gengivelse - af NIS2-krav. I materialet synliggøres desuden de konkrete krav og forpligtelser fra NIS2-loven og vejledninger, således at man som kommune kan se sammenhæng hertil.

Materialet er udarbejdet med blik for, at såvel store som mindre kommuner skal kunne se sig selv i det. Samtidigt er der taget højde for øvrige forskelle kommunerne imellem. I sidste ende skal kommunen selv tage stilling og kunne begrunde egne valg bl.a. ifm. et tilsyn.

Udgangspunktet er, at ansvaret for NIS2-efterlevelse og sikkerhedsniveau ligger hos kommunen selv. Topledelsens (direktionen) ansvar er helt centralt for at få arbejdet med cybersikkerhed forankret og prioriteret i kommunen.

Opgaver kan dog uddelegeres. Det er således vigtigt at forholde sig til, hvordan og hvilke beslutninger der træffes hvor og hvor ofte.

Drejebogstema Hændelseshåndtering
I dette kapitel af den kommunale NIS2-drejebog præsenteres en tilgang til kommunens håndtering af NIS2-hændelser, hvorved kommunen kan reagere hurtigt, sikrer at information deles og at forløbet omkring hændelsen og håndteringen sideløbende dokumenteres med henblik på eventuel underretningspligt.

Hændelseshåndtering og -underretning ved væsentlige hændelser er helt bærende elementer i NIS2-implementering, når man skal arbejde effektivt med cyber- og infomrationssikkerhed. Det drejer sig i høj grad om at kunne sikre sig, at de trusler og faktiske hændelser, man som enhed og kommune står overfor, ikke bliver til alvorlige brud som påvirker driftskontinuiteten. Særligt ift. samfundskritiske opgaver, og hvor konsekvenser meget hurtigt kan blive store, bl.a. for borgerne.

Hændelseshåndtering handler om, at man som NIS2-enhed indgår i sammenhænge, hvor en hændelse ét sted kan sprede sig og få endnu større og mere kritiske konsekvenser, Dermed er der behov for struktureret og hurtig underretning via Virk, således at såvel sektormyndigheden (Styrelsen for Samfundssikkerhed) og den nationale CSIRT får overblik og kan planlægge og handle derefter.

Kommunerne kan have etablerede procedurer og har også hidtil håndteret hændelser af forskelligt omfang. Med drejebogen gives en systematisk gennemgang med udgangspunkt i dét fokus, der anlægges i NIS2 samt tilbyder praktisk anvendelige redskaber. Alle kommuner kan have gavn at følge op på nuværende praksis og sikre sig, at man er godt klædt på til at reagere hurtigt og i overensstemmelse med NIS2.

Drejebogsmateriale giver således metode til, hvordan man som kommune kan gå til værks. Materialet omfatter desuden inspiration fra kommuner, der kan bruges i egne lokale overvejelser.

Baggrund
Den danske NIS2-lov trådte i kraft 1. juli 2025 med det formål at højne og ensartet cybersikkerheden – på tværs af EU og på tværs af sektorer i EU-medlemslandene. NIS2-loven udmønter EU's Netog Informationssikkerhedsdirektiv (NIS2).

Fokus i NIS2 er at opretholde driftskontinuitet og sikre robustheden over for cyberangreb på samfundskritiske områder. NIS2 har fokus på at forhindre hændelser og udlevelsen af konsekvenserne af angreb Det stiller krav til, at man som omfattet enhed har overblik over sammenhænge mellem kommunale arbejdsprocesser og IT-systemer at kunne vurdere konsekvenser ved hændelser og være i stand til at håndtere og indrapportere kritiske hændelser. Man skal også som omfattet enhed være opmærksom på kritiske led i ens forsyningskæder og leverandører.

Kommunerne er omfattet som helhed, dvs. alle IT-systemer og opgaver pga. kommunernes tværgående opgaver og nære kontakt til borgerne på vitale områder. Ved eksempelvis sundhedsområdet, gør at kommunerne i NIS2 udpeges som væsentlig enhed.

Styrelsen for Samfundssikkerhed (SAMSIK), der er overordnet NIS2-ansvarlig myndighed i Danmark, har lanceret fire generelle vejledninger og en Kommunevejledning: NIS 2-vejledninger | Styrelsen for Samfundssikkerhed

Vejledninger og selve NIS2-loven danner udgangspunkt for arbejdet med den kommunale NIS2-drejebog og de koncepter for implementering, der her gives. SAMSIK har desuden lanceret infosiden 'Introduktion til Risikovurdering' på Sikker Digital. Her har SAMSIK samlet viden og gode råd om digital sikkerhed: Introduktion til risikostyring. Sikker Digital og materialet kan være godt at orientere sig i for mange, bl.a. ift. NIS2 men også risikovurderinger i øvrigt.

Den kommunale NIS2-drejebog og redskaber adresserer tilsvarende emner, men tilpasset en kommunal kontekst. Det samme gælder for det sikkerheds-relaterede materiale på KL's Videnscenter, der kan være et godt sted at starte for mange kommuner: Cyber- og informationssikkerhed.

Indholdsfortegnelse

Indhold

Bilag

4.1 Hændelseshåndtering under NIS2

NIS2-lovens § 6, stk. 1, nr. 2 forpligtiger kommunerne til at etablere og implementere procedurer, der sikrer en effektiv håndtering af hændelser.

NIS2-lovens § 12 fastlægger kommunens pligt til at underrette om væsentlige hændelser.

NIS2-lovens § 13 beskriver indholdskrav og tidsfrister for underretning.

NIS2-lovens § 14 giver mulighed for frivillig underretning af hændelser, nærved-hændelser og cybertrusler.

NIS2-loven stiller krav om, at kommuner hurtigt og korrekt kan identificere, vurdere og underrette om væsentlige hændelser. SAMSIK's Vejledning om Hændelsesunderretning præciserer, at vurderingen af væsentlighed skal ske rettidigt, samt at underretningen skal følge de krav og tidsfrister der er i NIS2-lovens §§ 12-14.

SAMSIK's Vejledning til Implementering af Cybersikkerhedsforanstaltninger fremhæver, at hændelseshåndtering skal være en integreret del af kommunens samlede styringsmodel for cybersikkerhed. Vejledningen angiver bl.a. at kommunerne skal:

- Etablere procedurer for identifikation, analyse og reaktion på hændelser
- Sikre klare roller og ansvar, så hændelser håndteres hurtigt og ensartet
- Dokumentere hændelser og læring, så erfaring omsættes til forbedringer i styringsgrundlaget
- Sikre evnen til at genoprette stabil drift, herunder koordinering med leverandører og beredskab

Disse krav understøtter NIS2-lovens § 6, stk. 1, nr. 2, som forpligtiger kommunerne til at have passende og forholdsmæssige foranstaltninger til håndtering af hændelser.

For at understøtte tidlig opdagelse og ensartet rapportering på tværs af organisationen kan kommunen med fordel anvende "Pixibog for alle medarbejdere", som giver en enkel og praksisnær guide til, hvordan mistænkelige forhold kan opfanges og rapporteres internt.

NIS2-loven stiller krav om at kommuner:

Model 4.1.1

4.2 Hvad er en hændelse

Hvad er en hændelse, og hvilke hændelser er underlagt underretningsforpligtigelse?
NIS2-lovens § 3, stk. 1, nr. 12 definerer en hændelse som '*en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare*.' Det omfatter både tekniske fejl, sikkerhedsbrud og hændelser, der opstår via leverandører eller forsyningskæden.

En hændelse kan være:
- Driftsforstyrrelser i kommunens kritiske systemer
- Sikkerhedsbrud herunder uautoriseret adgang eller datalæk
- Leverandørfejl der påvirker kommunens drift
- Hændelser med direkte borgerpåvirkning f.eks. forsinkede ydelser eller sundhedsrisici

Hændelser er dermed noget, der kan påvirke en kommunes evne til at levere ydelser.
I NIS2-loven skelnes der mellem *hændelser* og *væsentlige hændelser*, og sidstnævnte udløser jf. NIS2-lovens § 12 en underretningsforpligtelse.

Væsentlige hændelser
En hændelse anses jf. NIS2-lovens § 12, stk. 2 som væsentlig hvis:

1. 'Hændelsen har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomisk tab for den berørte enhed'
2. 'Hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke-fysisk skade'

Vurderingen af om en hændelse er væsentlig skal ske hurtigt og ensartet, så forpligtelsen, inklusiv de fastsatte tidsrammer, til at underrette myndighederne og berørte modtagere af kommunens tjenester kan opfyldes. Dertil er det grundlaget for at sikre en effektiv og god hændelseshåndtering. "Spørgeguide til vurdering af væsentlighed" kan anvendes som et operationelt værktøj, der understøtter en ensartet vurdering af hændelser i kommunen.

Frivillig underretning
Udover lovpligtig underretning ved væsentlige hændelser giver NIS2-lovens § 14 kommunerne mulighed for at foretage frivillig underretning af hændelser til CSIRT'en f.eks. ved:

- Nærved-hændelser
- Cybertrusler
- Hændelser der ikke opfylder kriterier for væsentlighed

Kommunerne kan overveje frivillig underretning, når det vurderes, at hændelsen kan have en væsentlig sikkerhedsmæssig betydning. Ifølge SAMSIK's Vejledning om Hændelsesunderretning bør kommunerne gennemføre underretningen hurtigst muligt for at sikre, at CSIRT'en har de bedste vilkår for at vurdere hændelsen.

Frivillig underretning styrker videndeling og kan bidrage til at forhindre, at mindre hændelser udvikler sig til væsentlige.

4.3 Hændelseshåndtering

Hændelseshåndtering er ikke en isoleret disciplin, og bør være en integreret del af kommunens governancemodel, hvor ledelsesansvar, risikostyring og beredskab spiller sammen. Det betyder, at kommunen skal have klare roller, ansvar og eskalationsveje, så der hurtigt og ensartet kan reageres. Læs mere om governancemodellen i drejebogens kapitel om Ledelsesansvar.

For at sikre robusthed bør kommunen definere en ikke-personafhængig organisering for hændelseshåndtering. Kommunerne varierer i størrelse og kapacitet, hvilket giver forskellige muligheder for organisering. Det vil dog udgøre en væsentlig risiko, hvis ansvaret hviler på enkeltpersoner. Et centralt kontaktpunkt som f.eks. en servicedesk kan sikre kontinuitet ved sygdom, jobskifte eller fravær, understøtte videndeling og sikre, at relevante funktioner inddrages rettidigt. For at sikre resilience i hændelsesprocessens faser f.eks. intern anmeldelse, vurdering og eskalation, kan kommunerne anvende "Pixibog for interne teams", og sikre at alle relevante medarbejdere er informeret om de fast trin i en hændelseshåndteringsproces.

NIS2-loven og SAMSIK's vejledning om Hændelseshåndtering forudsætter, at kommunerne kan håndtere både den faktiske hændelse, den formelle underretning til myndighederne samt underretning af berørte modtagere af kommunens tjenester. Det kræver en organisering, hvor der er plads til to parallelle spor, som hver især har tydelige roller, ansvar og kompetencer. Nedenfor gennemgås de to spor samt anbefalinger til en model for roller og ansvar.

Spor A: Håndtering af den faktiske hændelse (drift, teknik og afværge)
Dette spor fokuserer på at begrænse skade, genetablere drift og sikre teknisk og operationel stabilitet.

Typiske opgaver
- Teknisk analyse og fejlfinding
- Inddæmning og afværgeforanstaltninger
- Koordinering med leverandører & relevante partnere
- Genetablering af systemer og tjenester
- Løbende statusvurdering og dokumentation

Roller:
Dette spor er formentlig allerede implementeret i kommunens eksisterende hændelsesproces og drives ofte af IT-drift, sikkerhedsfunktioner, leverandører og beredskabsteams.

Spor B: Håndtering af vurdering og underretning (compliance, dokumentation og governance)
Dette spor fokuserer på at sikre, at kommunen overholder NIS2-lovens krav til vurdering, dokumentation og underretning til myndigheder via virk.dk samt modtagere af de påvirkede tjenester.

Typiske opgaver:
- Vurdering af hændelsens væsentlighed
- Beslutning om tidlig varsling og underretning
- Udarbejdelse af 24-t, 72-t og 1-måneders rapporter
- Dokumentation af beslutninger, vurderinger og læring
- Afklaring af og underretning til berørte modtagere af tjenester
- Koordinering med ledelse og relevante myndigheder

Roller:
Dette spor kan drives af f.eks. compliance, informationssikkerhed, risikostyring og ledelsesrepræsentanter.

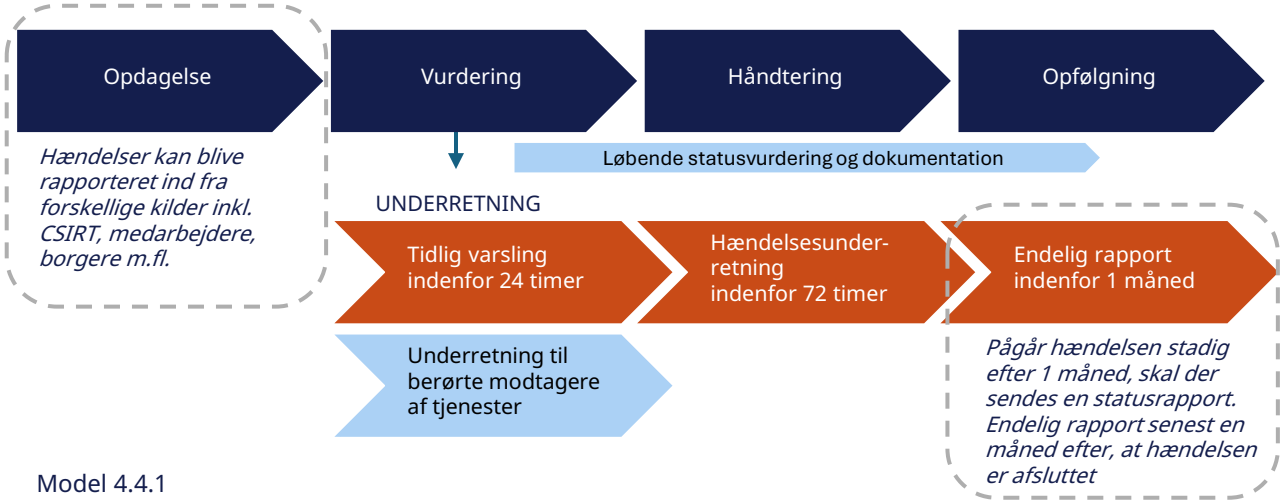
Model 4.3.1

Spor	Roller (tilpasses den enkelte Kommunes behov og kapacitet)	Primært ansvar
A	Hændelsesmodtager (første kontaktpunkt)	Registrering og aktivering
A	Teknisk Hændelsesansvarlig	Teknisk analyse og afværge
A	Leverandørkoordinator	Ekstern koordinering
A	Driftsgenopretningsansvarlig	Genetablering af drift
B	Væsentlighedsvurderingsansvarlig	Vurdering og dokumentation
B	Underretningsansvarlig	Myndighedsunderretning, underretning til berørte modtagere
B	Governance- og Dokumentationsansvarlig	Sporbarhed og læring
B	Ledelsesbeslutningstager	Godkendelser og eskalation

Model 4.3.2
Se detaljeret rolle, ansvar og kompetencemodel i Bilag 4c

4.4 Proces for hændelseshåndtering

Faser i hændelseshåndtering : fra hændelsen opdages



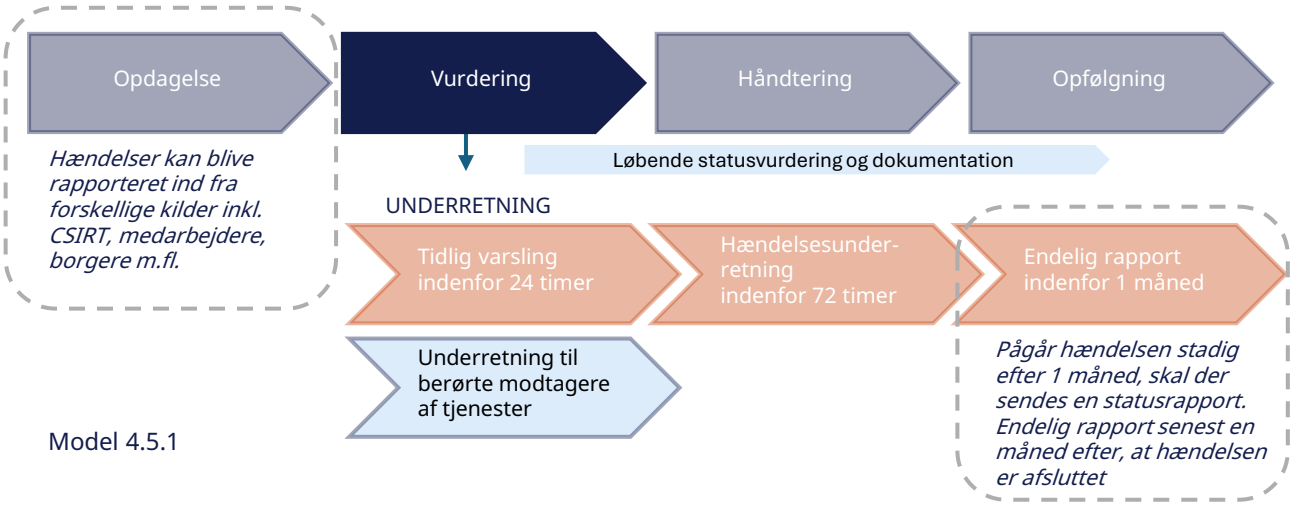
Model 4.4.1

Det anbefales, at hændelser håndteres i en række af faste faser, der tilsammen kan sikre en hurtig, ensartet og dokumenteret reaktion. Herunder følger en kort gennemgang af faserne:

Fase	Formål	Aktiviteter	Output
Opdagelse	At identificere, at noget er unormalt, og at sikre hurtig intern rapportering.	• Hændelsen opdages f.eks. via alarmer, KommuneCERT, medarbejdere, borgere eller leverandører. • Første observation beskrives kort: hvad, hvor, hvornår. • Hændelsen rapporteres til kommunens interne kontaktpunkt, der f.eks. kan via en servicedesk eller som en telefonisk hotline.	Registreret hændelse med kort beskrivelse og tidspunkt for opdagelse
Vurdering: Første vurdering	At afgøre, om hændelsen kan være væsentlig og kræver underretning.	• Gennemgang af første del af spørgeguiden. • Vurdering af påvirkning på drift, borgere, data og leverandører. • Beslutning om eskalation og aktivering af procedurer og processer herunder beredskabsprocedurer.	Foreløbig vurdering af kritikalitet og beslutning om næste skridt.
Vurdering: Uddybende vurdering	At skabe dokumenteret og sporbar grundlag for håndtering og underretning.	• Gennemgang af alle relevante vurderingspunkter i spørgeguiden. • Indsamling af fakta om omfang, varighed, berørte systemer og borgere. • Afklaring af leverandørpåvirkning og afhængigheder.	Dokumenteret vurdering af hændelsens karakter, omfang og konsekvenser.
Underretning til myndighederne	At sikre rettidig og korrekt underretning til myndighederne.	• Udfyldelse af underretning efter NIS2-lovens krav. • Beskrivelse af hændelsesforløb, påvirkning, afværgeforanstaltninger og usikkerheder. • Indsendelse via Virk og registrering i kommunens register,	Indsendt indberetning og dokumenteret sporbarhed.
Underretning til berørte modtagere	At sikre, at berørte modtagere hurtigt får den nødvendige information, hvis en hændelse påvirker deres adgang til eller brug af en kommunal tjeneste.	• Udarbejdelse af klar og rettidig information om hændelsens karakter og forventede påvirkning. • Identifikation af berørte modtagere. • Udsendelse via relevante kanaler (f.eks. hjemmeside, direkte besked, fagsystemer). • Eventuel vejledning om forholdsregler	Underretning sendt til berørte modtagere og dokumenteret sporbarhed i kommunens hændelsesregister.
Håndtering og afværgeforan-staltninger	At begrænse skade og genetablere (normal) drift.	• Iværksættelse af tekniske og organisatoriske tiltag. • Koordinering med leverandører og interne funktioner. • Løbende vurdering af status og behov for yderligere handling.	Stabiliseret situation og dokumentation af alle tiltag.
Opfølgning og læring	At sikre læring, forbedring og opdatering af styringsgrundlaget	• Udarbejdelse af afsluttende rapport. • Opdatering af risikovurderinger, kritikalitet og leverandørstyring. • Inddragelse af læring i ledelsesrapportering og governance.	Afsluttet hændelse og opdateret styringsgrundlag og risikovurderinger

Model 4.4.2

4.5 Vurdering af væsentligheden



Model 4.5.1

Kommunens evne til at vurdere hændelser hurtigt og ensartet er afgørende for både driftssikkerhed og efterlevelse af NIS2-loven. Når der anvendes de samme kriterier, samme spørgeguide og samme beslutningsproces, kan hændelser håndteres mere effektivt. Det reducerer risikoen for fejl, misforståelser og forsinkelser, og det sikrer, at kommunen aktiverer de rette procedurer på det rette tidspunkt.

En struktureret og genkendelig vurderingsproces giver kommunerne en række fordele:

- Hurtigere beslutninger, fordi medarbejdere og ledelse arbejder ud fra de samme kriterier.
- Større kvalitet i underretninger, da vurderingen skaber et dokumenteret og sporbart grundlag for myndighedsunderretning.
- Bedre koordinering, fordi alle parter ved, hvornår og hvordan en hændelse skal eskaleres.
- Hurtigere orientering af borgere, hvilket øger trygheden og mindsker risikoen for tab af tillid og omdømme.
- Styrket læring og governance, da ensartede vurderinger gør det muligt at identificere mønstre, forbedre beredskabet og opdatere risikobilledet.

En hurtig og ensartet vurdering er dermed ikke kun et lovkrav. Det er en forudsætning for robust drift, effektiv hændelseshåndtering og understøtter, sammen med en moden governancemodel, kommunens samlede cybersikkerhedsniveau. Samtidig giver det mulighed for af få bistand fra CSIRT (jf. NIS2-loven § 13, stk. 3) samt sikkerhed for at offentligheden informeres, hvis myndighederne vurderer det relevant jf. NIS2-lovens § 16.

"Pixibog for interne teams" kan hjælpe i vurderingsfasen. Den er designet til at understøtte processen for vurdering, eskalation og koordinering.

SAMSIK's Vejledning om Hændelsesunderretning præciserer, at vurderingen af, om en hændelse er væsentlig, skal ske rettidigt og baseres på en indledende vurdering af hændelsens potentielle påvirkning af kommunens tjenester.

"Spørgeguide til vurdering af væsentlighed" er et operationelt værktøj, der understøtter kommunernes hurtige beslutning om eskalation og kravet til *tidlig varsling* jf. NIS2-lovens § 13, stk. 1, nr. 1.

Den første del af spørgeguiden anvendes til at foretage en hurtig vurdering af om en hændelse kan anses som væsentlig.

Når den første vurdering er gennemført og en eventuel underretning er foretaget, anvendes spørgeguidens anden del til yderligere vurdering af hændelsens detaljer. Denne del skaber et sporbart beslutningsgrundlag for den nærmere håndtering af hændelsen og dokumentation til senere rapporteringer og læring.

Find eksempler på processen for hændelsesvurdering og –håndtering i Bilag 4b

Bilag 4a Overblik over centrale krav

Juridisk grundlag
Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS2-loven), vedtaget 29. april 2025, trådte i kraft 1. juli 2025. Gælder for kommunerne, der er identificeret som væsentlige enheder jf. § 2 og § 3 i loven.
Direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau (NIS2-direktivet) 2022/2555

Centrale paragraffer i NIS2-loven vedr. krav til hændelseshåndtering

§	Krav	Kravstype	Indhold
§ 6 stk. 1, nr. 2	Pålægger kommuner (enheder) at have passende og forholdsmæssige foranstaltninger til håndtering af hændelser	Skal	Det er her, kravet om at have procedurer, beredskab og evne til at håndtere hændelser er forankret.
§ 12	Underretningspligt ved væsentlige hændelser.	Skal	Kommuner (enheder) skal underrette om enhver væsentlige hændelser og underretningen skal ske rettidigt jf. de fastsatte tidsrammer i § 13.
§ 13	Fastsætter hvad en underretning skal indeholde og tidsrammerne for underretningen.	Skal	Kommunerne (enhederne) er underlagt en række specifikke krav til indhold og tidsramme for indberetninger.
§ 14	Omhandler frivillige underretninger	Kan	Offentlige og private enheder har mulighed for at underrette CSIRT'en om hændelser, nærvedhændelser og cybertrusler, uanset om de er omfattet af NIS2-loven.
§ 15	Underretning af modtagere af kommunens tjenester	Skal	Kommunen skal hurtigt informere de berørte modtagere, hvis en væsentlig hændelse kan påvirke deres adgang til eller brug af en kommunal tjeneste. Underretningen skal være tydelig og forklare, hvad der er sket, hvordan det påvirker dem, og hvad de eventuelt bør gøre.

Vejledningsbaserede krav (SAMSIK)

Kilde	Krav	Kravstype	Indhold
SAMSIKs Vejledning til Implementering af Cybersikkerheds-foranstaltninger (juni 2025)	Procedurer for håndtering af hændelser	Skal	Kommunen skal udarbejde og implementere procedurer for at identificer, opdage, analysere og reagere på hændelser, herunder genoprettelse af stabil drift og håndtering af underretningsforpligtigelser ved væsentlige hændelser.
SAMSIKs vejledning om Hændelsesunder-retning (juni 2025)	Uddybning af kriterier for væsentlighed	Uddybning	Vejledningen uddyber de tre kriterier for væsentlighed (alvorlig driftsforstyrrelse, betydeligt økonomisk tab, betydelig skade på tredjepart) og giver illustrative eksempler, der kan understøtte kommunens vurdering

Vejledningsbaserede krav (SAMSIK)

Kilde	Krav	Kravstype	Indhold
SAMSIKs Vejledning om Hændelsesunderretning (juni 2025)	Uddybning af indholdskrav til tidlig varsling	Uddybning	Vejledningen beskriver, hvilke oplysninger der skal indgå i den tidlige varsling, herunder om hændelsen mistænkes for at være forårsaget af ulovlige handlinger og om den kan have grænseoverskridende virkninger
SAMSIKs Vejledning om Hændelsesunderretning (juni 2025)	Uddybning af indholdskrav til hændelsesunderretning	Uddybning	Vejledningen uddyber, hvilke oplysninger der skal indgå i hændelsesunderretningen, herunder beskrivelse af alvor, indvirkning og kompromitteringsindikatorer
SAMSIKs Vejledning om Hændelsesunderretning (juni 2025)	Uddybning af krav til endelig rapport	Uddybning	Vejledningen beskriver indholdet i den endelige rapport, herunder detaljeret beskrivelse af hændelsen, årsag, afbødende foranstaltninger og eventuelle grænseoverskridende virkninger
SAMSIKs Vejledning om Hændelsesunder-retning (juni 2025)	Underretning ved outsourcing	Skal (vejlednings-baseret)	Hvis drift eller vedligeholdelse er outsourcet, er det fortsat kommunen, der har ansvaret for rettidig underretning. Leverandører kan underrette på vegne af kommunen, men ansvaret kan ikke overdrages
SAMSIKs Vejledning om Hændelsesunderretning (juni 2025)	Frivillig underretning	Uddybning	Kommunen kan frivilligt underrette CSIRT om hændelser, nærved-hændelser og cybertrusler, også selvom de ikke opfylder kriterierne for væsentlighed. Frivillig underretning kan styrke videndeling og forebyggelse
SAMSIKs Vejledning om Hændelsesunderretning (juni 2025)	Præcisering af krav om vurdering af grænseoverskridende påvirkning	Præcisering	Vejledningen præciserer, at kommunen skal vurdere og angive, om hændelsen kan have grænseoverskridende konsekvenser. CSIRT håndterer herefter koordinering med andre medlemsstater

Bilag 4b Eksempler

I bilag 4b findes eksempler på, hvordan hændelsesvurdering finder sted i kommuner.

Mellemstor kommune	
Governance og organisatorisk forankring - roller	Informationssikkerhedsarbejdet er organisatorisk forankret med et klart skel mellem formelt og operativt ansvar. **Overordnet ansvar:** Det formelle ansvar er ved IT-chefen. **Operativt ansvar:** Lederen for informationssikkerhedsteamet har ansvaret og Informationssikkerhedsteamet varetager den praktiske håndtering af hændelsen. **Tværgående involvering:** Mange af funktionerne ligger i informationssikkerhedsteamet, som dækker ind på hele processen. Både teknisk, organisatorisk og juridisk
Opdagelse og identificering af hændelser	**Hvordan opdager og registrerer vi hændelser?** Hændelser opdages primært via en MDR-løsning, som foretager løbende overvågning og varsler ved tegn på kompromittering. Derudover kan forvaltningsområderne kontakte IT-afdelingen ved leverandørnedbrud, hvorefter der oprettes en ticket. Hændelser kan registreres både via ticketsystemet og via direkte kontakt til informationssikkerhedsteamet, som også råder over en 24/7 vagttelefon.
Vurdering af hændelser	**Hvordan vurderer og klassificerer vi hændelser?** Hændelser vurderes uden brug af automatiserede værktøjer. Ved modtagelse foretages en manuel afdækning baseret på kendskab til IT-landskabet, kontekst og trusselsbilledet. Hændelser, der indmeldes via ticketsystemet, tildeles automatisk høj prioritet, hvis de vedrører sikkerhed. Lederen af informationssikkerhedsteamet inddrages altid, men teamet har mandat til at iværksætte nødvendige tiltag for at stoppe hændelsen uden forudgående godkendelse.
Tidlig varsling	**Hvordan arbejder vi med tidlig varsling?** Ved hændelser omfattet af NIS2 sikres tidlig varsling gennem tæt overvågning af relevante kilder og informationskanaler. Organisationen følger aktivt med i eksterne trusselsindikatorer og bidrager selv med information til relevante samarbejdspartnere for at styrke det fælles situationsbillede.
Hændelsesunderretning	**Hvordan arbejder vi med underretning?** Underretning håndteres af informationssikkerhedsteamet, som følger den eksisterende proces kendt fra GDPR-underretninger. Organisationen er vant til at arbejde inden for en 72-timers frist, og denne praksis videreføres i relation til NIS2.
Endelig rapport	**Hvordan gennemfører vi afsluttende evaluering og rapportering?** Den afsluttende rapport udarbejdes af informationssikkerhedsteamet, når hændelsen er håndteret. Rapporten bygger på den dokumentation, der er indsamlet under forløbet, og beskriver hændelsesforløb, årsager, konsekvenser og de tiltag, der er gennemført. Teamet gennemfører en samlet evaluering af håndteringen og identificerer eventuelle forbedringspunkter. Rapporten kvalitetssikres af lederen for informationssikkerhedsteamet og IT-chefen, før den fremsendes inden for den gældende tidsfrist. Hvis hændelsen fortsat pågår, udarbejdes en foreløbig rapport, og den endelige rapport fremsendes senest en måned efter, at hændelsen er afsluttet.

Mellemstor Kommune	
Governance og organisatorisk forankring - roller	**Overordnet ansvar:** Ledelsen (Chef for IT, Digitalisering og Borgerservice + Sektionsleder for IT-Service og sikkerhed) har det formelle ansvar for korrekt håndtering, kritikalitet, eskalering og evt. beredskabsaktivering. **Operativt ansvar:** • IT-driftsmedarbejdere: teknisk afhjælpning og leverance af oplysninger. • Ledelsen: vurderer kritikalitet og udpeger underretningsansvarlig. • Informationssikkerhedskoordinator: dokumenterer i ISMS og er typisk underretningsansvarlig. • Underretningsansvarlig: indberetter på virk.dk og journaliserer i ESDH. **Tværgående involvering:** Ledelse, drift, informationssikkerhedskoordinator; evt. DPO og systemejere afhængigt af hændelsen.
Opdagelse og identificering af hændelser	**Hvordan opdager og registrerer vi hændelser?** Hændelser opdages via brugerhenvendelser eller driftens log-observationer. Drift indsender elektronisk blanket i helpdesk, hvorefter automatisk advisering sendes til ledelse, sikkerhed og relevante driftsmedarbejdere. Ledelsen og drift følger deres arbejdsgange parallelt. Hvis hændelsen vurderes NIS2-relevant, udpeges underretningsansvarlig, og tidlig varsling indsendes. **Efterhændelsesgennemgang:** fast punkt på ugentlige driftsmøder; samlet arbejdsgang evalueres månedligt på sikkerhedsmøder.
Vurdering af hændelser	**Hvordan vurderer og klassificerer vi hændelser?** Ledelsen vurderer hændelsen inden for 4 timer. Vurderingen baseres på: • Datatyper (fx følsomme oplysninger) • Kritikalitet af berørt tjeneste • Geografisk spredning • Realiserede og potentielle skader • Eksterne parter • Samfundsmæssig betydning **Kategorier:** *Lav:* intern håndtering, ingen indrapportering. *Mellem:* alvorlig, intern eskalering; frivillig indrapportering mulig. *Høj:* kritisk/samfundskritisk; obligatorisk indrapportering og evt. beredskab.
Tidlig varsling	**Hvordan arbejder vi med tidlig varsling?** Ved *høj* kategorisering udpeger ledelsen en underretningsansvarlig (typisk informationssikkerhedskoordinator). Underretningsansvarlig indsender tidlig varsling på virk.dk og udfylder obligatoriske felter samt evt. yderligere kendt information. Manglende oplysninger indhentes primært hos drift. Relevante dokumenter journaliseres i ESDH.
Hændelsesunderretning	**Hvordan arbejder vi med underretning?** Samme ansvarsfordeling som ved tidlig varsling. Underretningsansvarlig indhenter ny viden, indsender opfølgende underretning på virk.dk og journaliserer ny dokumentation. Informationssikkerhedskoordinator dokumenterer i ISMS. Drift bidrager med tekniske oplysninger og kontakt til leverandører.
Endelig rapport	**Hvordan gennemfører vi afsluttende evaluering og rapportering?** Underretningsansvarlig samler og sammenfatter dokumentation om forløb, årsager, konsekvenser og håndtering. Ledelsen kvalitetssikrer rapporten, som fremsendes inden for fristen. Hvis hændelsen fortsat pågår, indsendes foreløbig rapport; endelig rapport senest én måned efter afslutning.

Mellemstor kommune	
Governance og organisatorisk forankring - roller	**Overordnet ansvar:** Stabschefen for IT **Operativt ansvar:** Informationssikkerhedskoordinatoren har ansvaret for at indsamle de nødvendige oplysninger, sikre dokumentation og anmeldelser til de rette myndigheder. **Tværgående involvering:** De fagområder som skal bidrage med info om hændelsen inddrages. F.eks. systemejer, fagområde, IT-drift.
Opdagelse og identificering af hændelser	**Hvordan opdager og registrerer vi hændelser?** Hændelser kan komme ind via forskellige kanaler: • Telefon til IT-support • Skriftlig henvendelse til IT via helpdesk system • Skriftlig anmeldelse af hændelse via formular til formålet • Mail fra databehandler til DPO-mail (SPOC for henvendelse fra databehandlere) Uden for almindelig arbejdstid beror opdagelsen på, at leder fra fx hjemmeplejen tager telefonisk kontakt til Stabschefen for IT eller lederen af IT og giver besked. Der er ikke nogen vagtordning som sikre, at de normale kanaler overvåges.
Vurdering af hændelser	**Hvordan vurderer og klassificerer vi hændelser?** Der er et meget lavt modenhedsniveau for registrering af hændelser i almindelighed. IT-driften, Ældre-IT og Skole-IT skal registrere hændelser på en formular. Det sker meget sjældent, så den reelle hændelseshåndtering er meget håndholdt og beror på at informationssikkerhedskoordinatoren får nys om, at der er en hændelse. Sikkerhedskoordinatoren vurderer om hændelsen kræver en indberetning til myndighederne.
Tidlig varsling	**Hvordan arbejder vi med tidlig varsling?** Totalt håndholdt af informationssikkerhedskoordinator
Hændelsesunderretning	**Hvordan arbejder vi med underretning?** **GDPR hændelser:** Organisationen indberetter via en intern formular. Indberetningen lander i DPO-postkassen som overvåges alle ugens dage (uformelt, da der formelt ikke er en vagtordning). Informationssikkerhedsteamet sørger for vurdering, evt. indberetning til Datatilsynet, journalisering, indtastning i ark med overblik over alle GDPR-sager. Fagområdet har ansvaret for at underrette evt. forurettede. **NIS2 hændelser** Håndholdt håndtering af IT-leder og informationssikkerhedskoordinator Koordinator sørger for journalisering, dialog med systemejer/faglige ansvarlige, indhentning af yderligere info og indberetninger.
Endelig rapport	**Hvordan gennemfører vi afsluttende evaluering og rapportering?** Informationssikkerhedskoordinator laver evaluering og endelig rapport. De nødvendige oplysninger indtastet på blanketten til SAMSIK (det er meget få oplysninger der kræves der). Ind til videre har de nedbrud som er anmeldt ikke relation til kommunens IT-drift. Det er nedbrud i fx Serviceplatform eller NemLogin. Der er ikke noget at evaluere i kommunen. Vi har ikke indflydelse på årsag og fejlretning.

Stor kommune	
Governance og organisatorisk forankring - roller	Informationssikkerhedsarbejdet er organisatorisk forankret med et klart skel mellem formelt og operativt ansvar. **Overordnet ansvar:** Det formelle ansvar har IT direktøren/direktøren, der sidder i ISU. **Operativt ansvar:** Er det en tværgående hændelse f.eks. på infrastrukturen, der påvirker store dele/hele kommunen, er det Central IT, der håndterer hændelsen. Er det hændelser på applikationslaget, så håndteres hændelsen typisk decentralt. De enkelte forvaltninger har deres egne IT-kompetencer, herunder en informationssikkerheds-koordinator, en GDPR-ansvarlig samt system-ansvarlige, der vil arbejde sammen omkring forløbet. **Tværgående involvering:** Afhængig af hændelsen vil der være mere eller mindre tværgående organisatorisk involvering samt evt. involvering af leverandørleddet.
Opdagelse og identificering af hændelser	**Hvordan opdager og registrerer vi hændelser?** Hændelser opdages via intern SOC, øvrige alarmer eller via medarbejdere/leverandører. Hændelsen registreres som en ticket i ITSM systemet. Afhængig af hændelsen følges et procesflow. Hvis det f.eks. vedrører et fagsystem går hændelsen til forvaltningens informationssikkerheds-koordinator. Forvaltningsområderne kan kontakte central IT, hvis der er behov for deres inddragelse.
Vurdering af hændelser	**Hvordan vurderer og klassificerer vi hændelser?** Der foretages en initial vurdering af hændelsen på baggrund af impact og urgency jf. ITSM systemet. Vurderes det, at der er tale om en sikkerhedshændelse, så mærkes sagen som "sikkerhedshændelse" og den vil have høj prioritet. Sagsløsning igangsættes og de nødvendige ressourcer/kontakter involveres. Afhængig af hændelsens kritikalitet orienteres forvaltningens IT-chef, forvaltningsdirektør/er, CISO m.fl.
Tidlig varsling	**Hvordan arbejder vi med tidlig varsling?** Der foretages en screening af hændelsen i forhold til muligt driftstab, muligt økonomisk tab og mulig skade på 3. mand. Samtidig vurderes det, om der kan være sammenhæng til aktuelle trusselsindikatorer og informationer fra samarbejdspartnere. Ud fra dette vurderes det, om der bør foretages tidlig varsling (24 timers indberetning)
Hændelsesunderretning	**Hvordan arbejder vi med underretning?** Tidlig varsling/Underretning håndteres af GRC/SOC teamet i central IT, hvis det er en hændelse, der har tværgående impact. Hvis det er en hændelse, der relaterer sig til et specifikt fagsystem/forvaltning, så er det den pågældende informationssikkerhedskoordinator, der indberetter evt. i dialog med forvaltningens GDPR ansvarlige samt systemansvarlige. Organisationen er vant til at arbejde inden for en 72-timers frist, og denne praksis videreføres i relation til NIS2.
Endelig rapport	**Hvordan gennemfører vi afsluttende evaluering og rapportering?** Den afsluttende rapport udarbejdes af den hændelsesansvarlige og indberettes indenfor 1 måned. Rapporten bygger på den dokumentation, der er indsamlet under forløbet, og beskriver hændelsesforløb, årsager, konsekvenser og de tiltag, der er gennemført. Teamet gennemfører en samlet evaluering af håndteringen og identificerer eventuelle forbedringspunkter. Rapporten kvalitetssikres af teamet omkring hændelseshåndteringen og, afhængig af kritikaliteten, den tilhørende IT chef og/eller CISO, før den fremsendes. Hvis hændelsen fortsat pågår, udarbejdes en foreløbig rapport, og den endelige rapport fremsendes senest en måned efter, at hændelsen er afsluttet.

Bilag 4c Anbefalinger til roller og ansvar

Nedenfor ses eksempler på, hvordan roller og ansvar kan fordeles i kommunens hændelseshåndtering. Modellen er fleksibel: nogle kommuner vil samle flere roller hos én person, andre vil bruge andre titler eller organiseringer. Det afgørende er, at alle opgaver i både Spor A og Spor B i model 4.3.1 er tydeligt placeret, ikke personafhængige og kan udføres rettidigt. Modellen kan derfor bruges som et praktisk udgangspunkt til at sikre klarhed, ensartethed og robusthed i kommunens samlede hændelses-håndtering.

Spor	Rolle	Primære kompetencer	Ansvar
A	**Hændelsesmodtager / Første kontaktpunkt**	• Grundlæggende forståelse for IT-drift og sikkerhed • Evne til at registrere hændelser korrekt • Kendskab til eskalationsveje	• Modtage og registrere hændelser • Sikre korrekt første beskrivelse (hvad, hvor, hvornår) • Aktivere relevante funktioner i Spor A og Spor B (se model 4.3.1) • Sikre sporbar registrering i system
A	**Teknisk Hændelsesansvarlig**	• Dybt teknisk kendskab til systemer og infrastruktur • Analyse af logdata, alarmer og fejl • Koordinering af tekniske teams og leverandører	• Lede teknisk analyse og afværgeforanstaltninger • Sikre inddæmning og begrænsning af skade • Dokumentere tekniske fakta løbende • Give løbende status til Spor B i model 4.3.1
A	**Leverandørkoordinator**	• Kontraktforståelse og SLA-kendskab • Kommunikation med eksterne parter • Forståelse for systemafhængigheder	• Inddrage relevante leverandører rettidigt • Indhente tekniske oplysninger og status • Sikre leverandørers efterlevelse af krav og tidsfrister • Dokumentere leverandørbidrag
A	**Driftsgenopretningsansvarlig**	• Planlægning og koordinering af driftsaktiviteter • Test og validering af systemer • Forståelse for forretningskritiske processer	• Planlægge og gennemføre genetablering af drift • Koordinere test og idriftsættelse • Informere berørte fagområder • Dokumentere genopretningsforløb
B	**Væsentlighedsvurderingsan-svarlig**	• Risikovurdering og analyse af væsentlighed • Kendskab til NIS2-lovens kriterier • Evne til at anvende spørgeguide og beslutningsmodel	• Foretage hurtigvurdering og fuld vurdering • Dokumentere vurderinger og beslutninger • Anbefale tidlig varsling og underretning • Sikre ensartet vurdering på tværs af kommunen
B	**Underretningsansvarlig**	• Kendskab til NIS2-lovens § 12–14 • Evne til at udarbejde myndighedsrapporter • Klar og præcis skriftlig formidling	• Udarbejde 24-t, 72-t og 1-måneders rapporter • Sikre rettidig indsendelse via Virk • Koordinere med CSIRT og myndigheder • Dokumentere alle underretninger og opdateringer • Sikre underretning til de omfattede af den påvirkede tjeneste
B	**Governance- og Dokumentationsansvarlig**	• Dokumentationsstyring • Forståelse for risikostyring og compliance • Evne til at omsætte læring til styringsdokumenter	• Sikre sporbarhed i alle beslutninger • Opdatere risikovurderinger, procedurer og beredskab • Udarbejde læringsopsamling og ledelsesrapportering • Sikre korrekt arkivering af hændelsesdokumentation
B	**Ledelsesbeslutningstager**	• Strategisk forståelse for drift og risiko • Beslutningskompetence i henhold til governance • Evne til at vurdere konsekvenser og behov for eskalation	• Godkende væsentlighedsvurdering • Godkende underretning til myndigheder • Beslutte aktivering af beredskab/krisestab • Sikre ledelsesmæssig opfølgning og prioritering