MINIGUIDE

Slik forbereder du deg til NIS2-direktivet

Publisert juni 2024
Revidert mai 2025

advania

Oversikt over NIS2

NIS2-direktivet (Network and Information Security 2) ble vedtatt på EU-nivå i 2022 og trådte formelt i kraft for land i EU 18. oktober 2024. Direktivet representerer en betydelig skjerping av kravene i cybersikkerhet for virksomheter som leverer samfunnskritiske og viktige tjenester. I Norge implementeres NIS2 i nasjonal lov gjennom en forskrift til «Lov om digital sikkerhet (digitalsikkerhetsloven)», som er ventet å tre i kraft i løpet av 2025.

Formålet med NIS2 er ikke bare å redusere risikoen for digitale angrep, det handler om å beskytte grunnleggende samfunnsfunksjoner og sikre kontinuitet i tjenester som er avgjørende for liv, helse, økonomi og offentlig trygghet. Direktiver pålegger derfor berørte virksomheter å styrke sin digitale motstandskraft gjennom tekniske, organisatoriske og tiltak. Det er ikke bare ett spørsmål om etterlevelse, men om samfunnsansvar: å holde kritiske tjenester i gang, selv når truslene øker.

Hvorfor sikre samsvar?

Å etterleve kravene i den nye digitalsikkerhetsloven er ikke bare en juridisk plikt, men også en strategisk investering for virksomheter. Det kan bidra til å redusere risiko for alvorlige sikkerhetsbrudd og driftsavbrudd, og styrker tilliten fra kunder, partnere og myndigheter. Samtidig øker det virksomhetens beredskap mot stadig mer komplekse cybertrusler. I mange tilfeller kan etterlevelse også gi et konkurransefortrinn, særlig i anbud og leverandørkjeder der sikkerhet vektlegges.

Hvem omfattes?

- **Essensielle virksomheter**; som blant annet inkluderer aktører innen energi, transport, bank og finans, helse, vannforsyning, digital infrastruktur, offentlig forvaltning og romfart.
- **Viktige virksomheter**; slik som aktører innen post- og kurertjenester, produksjon av kritiske produkter (legemidler, kjemikalier mfl.), avfallshåndtering, matvaredistribusjon samt visse digitale tjenestetilbydere.

Klassifiseringen baseres på en kombinasjon av sektortilhørlighet og størrelseskriterier, hvor blant annet mellomstore og store virksomheter (50+ ansatte og/eller €10M+ i omsetning) omfattes. Tersklene og vurderingene kan tilpasses nasjonalt av norske myndigheter.

Selv om virksomheten ikke direkte omfattes, kan direktivet likevel fungere som en nyttig referanse for god praksis. Kravene bør vurderes som en del av proaktivt sikkerhetsarbeid, spesielt for organisasjoner med høy digital avhengighet eller samfunnsoppdrag.

Hva betyr dette for norske virksomheter?

Med implementeringen av NIS2 i norsk rett får berørte virksomheter sannsynligvis en rekke krav de må overholde:

- Styrket risikohåndtering og sikkerhetsstyring, herunder krav til forebyggende tekniske og organisatoriske tiltak
- Rapporteringsplikt ved sikkerhetshendelser, i henhold til definerte tidsrammer
- Ledelsesansvar, hvor virksomhetens øverste leder pålegges et tydelig ansvar for etterlevelse
- Tilsyn og sanksjoner, hvor tilsynsmyndighet (i Norge blir dette NSM) får hjemmel til å føre kontroll og ilegge sanksjoner ved brudd

Nøkkelkrav

For å etterleve NIS2 og digitalsikkerhetsloven, må virksomheter oppfylle en rekke krav knyttet til styring, beredskap og sikkerhetskontroll.

Sikkerhetsledelse og risikostyring

Virksomheten må ha strukturerte prosesser for risikohåndtering, identifisere kritiske systemer og beskytte digitale verdier med tekniske og organisatoriske tiltak. Fokus skal være på det som er mest kritisk for driften.

Hendelseshåndtering og varsling

Det må være på plass rutiner for å oppdage, varsle og håndtere sikkerhetshendelser. Alvorlige hendelser skal meldes til NSM innen 24 timer. Virksomheten må også lære og forbedre seg etter hendelser.

Leverandør- og tredjepartsstyring

Risiko i forsyningskjeden må vurderes og følges opp. Det innebærer sikkerhetskrav i kontrakter, jevnlig oppfølging og sikring mot sårbarheter hos underleverandører og skytjenester.

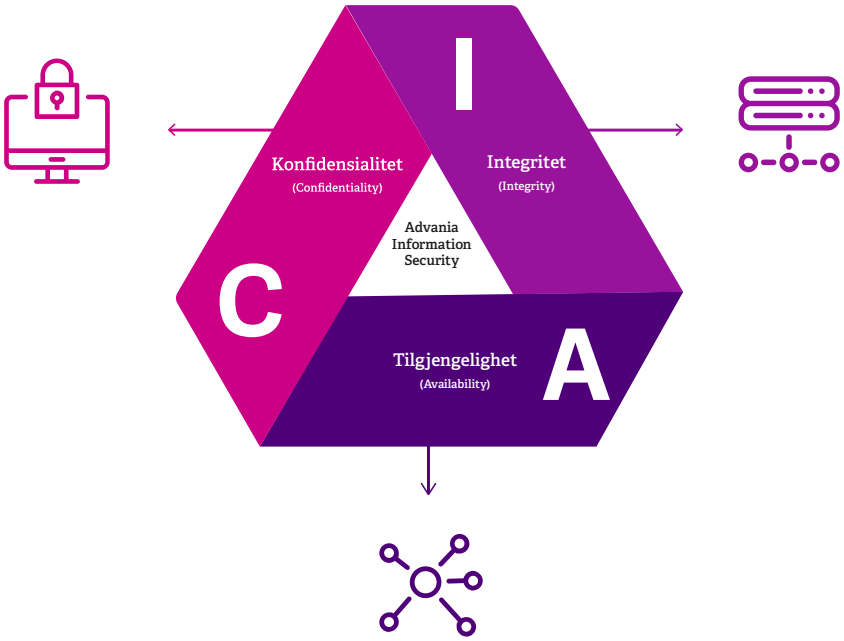
Ledelsesforankring og organisering

Toppledelsen har ansvar for etterlevelse og må involveres i sikkerhetsstyringen. Roller må være tydelige, og det kreves regelmessig opplæring og bevisstgjøring i hele organisasjonen.

Kontinuitet og beredskap

Virksomheten skal ha oppdaterte og testede beredskapsplaner for å håndtere hendelser og gjenopprette drift. Planene må beskrive roller, teknisk håndtering og kommunikasjon.

Konfidensialitet, integritet og tilgjengelighet



NIS2 bygger på **tre sentrale sikkerhetsprinsipper**, som sammen danner grunnlaget for alt arbeid med informasjonssikkerhet. Disse prinsippene må gjennomsyre både tekniske løsninger og organisatoriske tiltak.

Konfidensialitet

Tilgang til sensitiv informasjon skal begrenses til autoriserte brukere. Kryptering, tilgangskontroller og flerfaktorautentisering (MFA) er sentrale tiltak for å hindre autorisert innsyn eller lekkasje av data.

Integritet

Informasjon og systemer må beskyttes mot uautorisert endring. Tiltak som tilgangsstyring og digital signering sikrer at data forblir nøyaktige og pålitelige, og at innholdet ikke kan manipuleres av uvedkommende.

Tilgjengelighet

Systemer og tjenester skal være tilgjengelige når brukeren trenger dem, også under press. For å oppnå dette må virksomheten etablere robust infrastruktur, sikre redundans, driftskontinuitet og planer for katastrofegjenoppretting.

Trinn for samsvar

For å oppfylle kravene i NIS2-direktivet og den kommende digitalsikkerhetsloven, anbefales virksomheter følge en strukturert og risikobasert tilnærming. En slik metodikk gjør det mulig å identifisere sårbarheter, prioritere tiltak og etablere gode rutiner for styring, beredskap og dokumentasjon.

Her er fem praktiske trinn for å komme i gang med arbeidet:

1. Avklar om dere er omfattet

Start med å avklare om virksomheten omfattes av NIS2/digitalsikkerhetsloven. Dette avhenger blant annet av sektor, størrelse og tjenestene dere tilbyr. I mange tilfeller krever dette en kombinasjon av juridisk og teknisk vurdering.

2. Forankre arbeidet i ledelsen

Ledelsen må ha et bevisst forhold til direktivet og forstå hva det innebærer. Det er viktig at sikkerhetsarbeid forankres på toppnivå, og at det utnevnes en person eller gruppe med tydelig mandat og nødvendige ressurser for å gjennomføre og følge opp krav.

3. Kartlegg dagens modenhet og risiko

Kartlegg digitale verdier og vurder modenhet. Start med å identifisere hva som er kritisk for å opprettholde drift, inkludert verdier, systemer, tjenester og avhengigheter. Deretter vurder hvilke sikkerhetstiltak som allerede er på plass, og hva som mangler for å oppnå ønsker sikkerhetsnivå.

4. Etabler styringssystem og plan for tiltak

Bygg eller tilpass allerede eksisterende styringssystem for sikkerhet og lag en konkret handlingsplan for å lukke gapene. Ett styringssystem basert på ISO 27001 kan være lurt å implementere.

5. Dokumenter og forbered dere på tilsyn

Sørg for at tiltak, prosesser og ansvarsområder er dokumentert. Ha oversikt som kan fremvises ved tilsyn, og sørg for at beredskap og hendelseshåndtering er på plass og øvet på.

Implementering av sikkerhetstiltak

For å oppfylle NIS2-direktivet må virksomheter innføre en rekke sikkerhetstiltak som dekker både tekniske og organisatoriske forhold, samt arbeidsrutiner og sikkerhetsprosedyrer.

Policyer for risikovurdering og informasjonssikkerhet
Virksomheten skal ha dokumenterte rutiner for å identifisere og håndtere sikkerhetsrisiko.

Håndtering av sikkerhetshendelser
Det må være etablert prosedyrer for deteksjon, rapportering og håndtering av hendelser.

Forretningskontinuitet og krisehåndtering
Planer for backup, gjenoppretting og håndtering av kriser må være på plass og testet jevnlig.

Sikkerhet i leverandørkjeden
Risiko knyttet til leverandører og tjenesteleverandører må vurderes og følges opp systematisk.

Sikkerhet i systemanskaffelser og -utvikling
Krav til sikkerhet og sårbarhetshåndtering skal inngå i anskaffelse, utvikling og vedlikehold av systemer.

Evaluering av sikkerhetstiltak
Det må finnes rutiner for å vurdere effekten av implementerte sikkerhetstiltak

Grunnleggende sikkerhetshygiene og opplæring
Ansatte må få jevnlig opplæring, og virksomheten skal følge gode praksiser for digital sikkerhet.

Bruk av kryptografi og kryptering
Det skal være policyer for bruk av kryptering der dette er relevant og nødvendig.

Sikkerhet i personalforvaltning
Det kreves tilgangskontroll, rolleavklaringer og oversikt over digitale eiendeler

Sikre autentiserings- og kommunikasjonsløsninger
Bruk av flerfaktorautentisering (MFA) og sikre kommunikasjonskanaler for krisehåndtering anbefales sterkt.

Grunnleggende tiltak for cybersikkerhetsstyring

Strukturert risikoarbeid spiller en sentral rolle i NIS2-direktivet. For å sikre kontinuerlig beskyttelse av digitale verdier, må virksomheter jobbe systematisk med å identifisere, vurdere og håndtere risiko.

Identifiser kritiske eiendeler

Kartlegg og klassifiser systemer, tjenester og digitale eiendeler ut fra hvor viktige de er for virksomhetens funksjon og sikkerhet.

Gjennomfør risikovurderinger

Benytt anerkjente metoder for å identifisere trusler og sårbarheter, og dokumenter funnene som grunnlag for prioriterte tiltak.

Overvåk og oppdater jevnlig

Utfør jevnlige sikkerhetsrevisjoner og tilpass tiltak i tråd med endringer i trusselbilder og virksomhetens behov.

Se opptak av vårt seminar om NIS2-direktivet

Vi holdt et seminar sammen med Microsoft og advokatfirmaet Brækhus om hvordan du kan forberede deg til NIS2. Her kan du se opptaket.

Du lærer mer om:

- Hva det innebærer å innføre et sikkerhetsrammeverk
- Hvordan kravene i NIS2 kan løses ved hjelp av teknologi
- Compliance-strategier etter NIS2 og DORA

Se webinar her

The tech company
with people at heart

advania

advania.no