HOUSE OF CONTROL | A COMPANY IN VISMA

NIS2-kravene

En guide for berørte virksomheter

Viktig informasjon: House of Control er et programvareselskap. Vi tilbyr ikke rådgivningstjenester knyttet til NIS2-etterlevelse. **Det å følge denne veiledningen garanterer derfor ikke samsvar med alle juridiske krav i NIS2.**

Innholdet i denne guiden er basert på vår egen gjennomgang av NIS2-kravene og vår erfaring med etterlevelse av regelverk, samt inspirasjon fra ulike aktører som tilbyr rådgivningstjenester. Vi påtar oss ikke ansvar for manglende etterlevelse av NIS2-krav eller for konsekvenser som følge av bruken av denne veiledningen.

HOUSE OF CONTROL | A COMPANY IN VISMA

Innholdsfortegnelse

01.

Hva er NIS2 og hvorfor er det viktig?

02.

De viktigste forskjellene mellom NIS1 og NIS2

03.

Hvem omfattes av NIS2?

04.

Artikkel 21: Krav til risikostyring og sikkerhetstiltak

05.

Sikkerhet i leverandørkjeden: Du er ikke sterkere enn det svakeste leddet

06.

Artikkel 23: Varsling og rapportering av sikkerhetshendelser

07.

Andre viktige krav i NIS2 du må få med deg

08.

Vanlige fallgruver i arbeidet med NIS2

09.

Slik bygger dere en strukturert og bærekraftig NIS2-tilnærming

10.

Hvorfor struktur og verktøy er avgjørende

11.

Avslutning: Fra regelverk til robust virksomhet

HOUSE OF CONTROL | A COMPANY IN VISMA

Digital sikkerhet har gått fra å være et rent IT-ansvar til å bli et tydelig leder- og virksomhetsansvar. Cyberangrep, systemfeil og leverandørsvikt kan i dag stoppe drift, skade omdømme og få direkte økonomiske konsekvenser. Med NIS2-direktivet svarer EU på denne utviklingen ved å stille strengere krav til hvordan virksomheter skal jobbe med cybersikkerhet, risikostyring og hendelseshåndtering.

Denne guiden er laget for deg som jobber i IT-avdelingen, med compliance, juridiske spørsmål eller virksomhetsstyring. Hensikten er å hjelpe deg som trenger en praktisk forståelse av hva NIS2 faktisk krever. Vi har bevisst unngått unødvendig juss og teknisk kompleksitet. Målet er å gjøre det tydelig hva som forventes av virksomheten, og hva som skal til for å håndtere NIS2 på en god og strukturert måte.

1. Hva er NIS2 og hvorfor er det viktig?

NIS2 er EUs oppdaterte direktiv for nettverks- og informasjonssikkerhet. Det erstatter NIS1 fra 2016. Bakgrunnen er enkel: Samfunnet vårt er mer digitalt, mer sammenkoblet og mer sårbart enn noen gang tidligere.

Virksomheter er i dag avhengige av:

- Stabile IT-systemer
- Digitale leverandører
- Skybaserte tjenester
- Kontinuerlig tilgjengelighet

Når noe svikter, kan konsekvensene raskt bli større enn virksomheten selv. Nettopp derfor handler NIS2 ikke først og fremst om teknologi, men om **styring**.

NIS2 er ikke en teknisk manual. Det er et regelverk for god styring og kontroll. Det handler mindre om hvilke brannmurer dere bruker, og mer om:

- Hvordan dere identifiserer risiko
- Hvordan dere prioriterer tiltak
- Hvordan dere følger opp ansvar
- Hvordan dere dokumenterer at arbeidet faktisk blir gjort

For mange virksomheter er dette et tydelig signal om at sikkerhet ikke lenger kan håndteres som et sideprosjekt i IT-avdelingen.

2. De viktigste forskjellene mellom NIS1 og NIS2

Dersom dere allerede har et forhold til NIS1, er det viktig å forstå at NIS2 innebærer en reell skjerping. Her er de viktigste endringene du bør merke deg:

Flere bransjer omfattes

NIS1 gjaldt et relativt begrenset antall virksomheter innen kritisk infrastruktur. NIS2 utvider virkeområdet betydelig. Blant annet omfattes nå:

- Produksjonsbedrifter
- Helse- og omsorgssektoren
- Rransport og logistikk
- Energi og avfall
- Digitale tjenesteleverandører

Mange virksomheter som tidligere ikke har forholdt seg til regelverket, er nå direkte omfattet.

Ledelsens ansvar er tydeligere

NIS2 presiserer at virksomhetens øverste ledelse har ansvar for etterlevelse. Det betyr at:

- Sikkerhet ikke kan delegeres bort uten oppfølging
- Ledelsen skal godkjenne og følge opp tiltak
- Manglende etterlevelse kan få konsekvenser også på ledernivå

Dette er en tydelig endring fra NIS1, hvor ansvarsforholdene ofte var mer uklare.

Tydeligere krav til risikostyring

NIS2 stiller konkrete krav til hvordan risiko skal vurderes og håndteres. Dette gjelder ikke bare interne systemer, men også leverandørkjeden og tredjeparter. Det holder ikke lenger å anta at leverandører “har kontroll”.

Strengere sanksjoner

Myndighetene får sterkere virkemidler. Maksimale overtredelsesgebyrer avhenger av om virksomheten klassifiseres som vesentlig eller viktig. For *vesentlige* virksomheter kan bøtene være opptil 10 millioner euro eller 2 prosent av global årsomsetning, mens grensen for viktige virksomheter er opptil 7 millioner euro eller 1,4 prosent av global årsomsetning. Like viktig er muligheten for pålegg, tilsyn og krav om forbedringer.

Kort sagt: NIS2 er mer konkret, mer forpliktende og vanskeligere å ignorere enn NIS1.

3. Hvem omfattes av NIS2?

NIS2 deler virksomheter inn i to hovedkategorier:

- Vesentlige virksomheter
- Viktige virksomheter

Begge kategorier må oppfylle kravene i direktivet, men tilsynet er strengere for de vesentlige virksomhetene. For øvrig, krav til dokumentasjon under artikkel 21 varierer ikke bare fra sektor til sektor, men også fra land til land. Det siste innebærer at denne jobben er ekstra krevende for selskaper som opererer i flere EU-land.

Klassifiseringen avhenger blant annet av:

- Hvilken sektor virksomheten tilhører
- Virksomhetens størrelse
- Hvilken rolle virksomheten spiller i samfunnet og i verdikjeder

Et viktig poeng om leverandører

Selv om virksomheten din ikke er direkte underlagt NIS2, kan dere bli berørt indirekte. Dersom kundene deres er omfattet av direktivet, vil de stille krav til dere som leverandør. Dette gjelder særlig IT-tjenester, drift, programvare, infrastruktur og andre kritiske støttefunksjoner.

For mange virksomheter er dette første møte med formelle krav til dokumentert informasjonssikkerhet.

4. Artikkel 21: Krav til risikostyring og sikkerhetstiltak

Artikkel 21 er selve maskinrommet i NIS2. Den beskriver hvilke tiltak virksomheten skal ha på plass for å håndtere risiko knyttet til nettverks- og informasjonssystemer.

Kjernen i artikkelen er enkel: Virksomheten skal iverksette tekniske, operasjonelle og organisatoriske tiltak som står i forhold til risikoen dere står overfor.

Hva betyr det i praksis? Listen under er eksempler på tiltak som ofte er relevante:

Risikoanalyser: Har dere identifisert hvilke verdier som er kritiske, og hvilke trusler som kan påvirke dem?

Sikkerhetspolicyer: Finnes det skriftlige retningslinjer for informasjonssikkerhet, og er de kjent i organisasjonen?

Hendelseshåndtering: Har dere en plan for hva dere gjør når (ikke hvis) noe går galt?

Kontinuitets- og beredskapsplaner: Hvordan opprettholder dere drift ved et større IT-utfall eller sikkerhetsbrudd?

Leverandørsikkerhet: Har dere vurdert risiko knyttet til underleverandører og tredjeparter?

Opplæring og bevisstgjøring: Får ansatte og ledelse opplæring i digital sikkerhet og risikoforståelse?

Beskyttelse av data: Bruker dere for eksempel kryptering der det er nødvendig?

Sikker systemutvikling og anskaffelser: Har dere rutiner for å ivareta sikkerhet ved utvikling, innkjøp og vedlikehold av IT-systemer, inkludert håndtering og utbedring av sårbarheter?

Evaluering av sikkerhetstiltak: Har dere mekanismer for å kontrollere om sikkerhetstiltakene faktisk fungerer som forutsatt, og blir disse vurderingene brukt til forbedring?

Grunnleggende cyberhygiene: Følges grunnleggende sikkerhetsrutiner som oppdatering av systemer, sikring av endepunkter og bruk av sikre standardinnstillinger?

Tilgangsstyring og eiendelsoversikt: Har dere oversikt over hvilke systemer, data og enheter som er i bruk, og er tilganger begrenset til det som er nødvendig for den enkelte rolle?

Autentisering og sikker kommunikasjon: Bruker dere sterke autentiseringsmekanismer, som flerfaktorautentisering der det er relevant, og sikrer dere kommunikasjon i nettverk og systemer?

Dette er ikke ment som en sjekkliste som krysses av én gang. NIS2 forutsetter at arbeidet er **kontinuerlig**, og at tiltak vurderes og oppdateres over tid. Kravene i NIS2 skal anvendes forholdsmessig, basert på virksomhetens størrelse, risikoeksponering og betydning for samfunn og økonomi.

Et kjent gap i mange virksomheter

De fleste virksomheter har allerede noen tiltak på plass. Utfordringen er ofte at:

- Dokumentasjonen er spredt i Excel-ark og e-poster
- Ansvaret er uklart
- Oppfølging skjer uregelmessig
- Det er vanskelig å vise helhet

NIS2 krever at dere kan bevise etterlevelse over tid. Dette innebærer ikke bare å forklare hva dere *har tenkt* å gjøre, men å dokumentere hva dere faktisk gjør. Se vår guide til gap-analyse i kapittel 9.

5. Sikkerhet i leverandørkjeden: Du er ikke sterkere enn det svakeste leddet

Et av de mest diskuterte aspektene ved NIS2 er kravene til leverandørstyring. Tidligere har mange stolt blindt på at store skyleverandører eller lokale IT-partnere har "orden i syssakene". Med NIS2 er denne tilliten ikke lenger nok – den må dokumenteres.

Hvorfor er dette så viktig? De fleste moderne cyberangrep skjer ikke direkte mot målet, men via en underleverandør med svakere sikkerhet. Dersom en sikkerhetshendelse hos en leverandør får betydelig innvirkning på virksomhetens tjenester, er det virksomheten selv som har ansvar for å vurdere om hendelsen er rapporteringspliktig etter NIS2, og eventuelt rapportere den videre til myndighetene.

Slik følger du opp leverandører i praksis:

1. **Kategorisering:** Ikke alle leverandører er like viktige. Start med å identifisere hvem som er kritiske. Dette er de som, hvis de forsvinner, stopper din evne til å levere tjenester.

2. **Sikkerhetskrav i kontrakter:** Du må inkludere spesifikke krav om informasjonssikkerhet i alle nye avtaler, inkludert krav om at de varsler deg dersom de opplever et brudd.

3. **Kontinuerlig overvåking:** Det holder ikke med en årlig e-post. Sertifiseringer som ISO 27001 eller rapporter som SOC 2 er ikke eksplisitte krav i NIS2, men kan være nyttige former for dokumentasjon når virksomheten skal vurdere og følge opp leverandørers sikkerhetsnivå.

Ved å ha en strukturert tilnærming til dette, viser du ikke bare etterlevelse, men du reduserer den reelle risikoen for driftsstans dramatisk.

6. Artikkel 23: Varsling og rapportering av sikkerhetshendelser

Når en alvorlig hendelse inntreffer, er det sjelden mangel på aktivitet. Det som ofte mangler, er oversikt. Artikkel 23 i NIS2 er laget nettopp for disse situasjonene, det vil si når tidspresset er høyt, informasjonen ufullstendig og konsekvensene potensielt store.

Kjernen i artikkel 23 er at virksomheten skal kunne **rapportere raskt, strukturert og korrekt** til myndighetene.

Hva regnes som en signifikant hendelse?

En hendelse skal rapporteres dersom den har betydelig innvirkning på:

- Tilgjengeligheten av systemer eller tjenester
- Integriteten til data eller systemer
- Konfidensialiteten til informasjon
- Leveransen av virksomhetens tjenester

Dette kan være alt fra cyberangrep og løsepengevirus til større driftsavbrudd eller alvorlige leverandørfeil.

Tidslinjen i NIS2

NIS2 innfører en tydelig, trinnvis rapportering:

Tidlig varsel (innen 24 timer): En bekreftelse på at en alvorlig hendelse har inntruffet.

Oppdatering (innen 72 timer): Mer informasjon om hendelsens art, omfang og mulige konsekvenser.

Sluttrapport (senest innen én måned): En full gjennomgang av årsak, håndtering og tiltak som er iverksatt for å hindre gjentakelse.

Fristene regnes fra det tidspunktet virksomheten blir kjent med at en signifikant hendelse har inntruffet, og rapportering skal skje uten ugrunnet opphold.

Dersom hendelsen er pågående, kan det være nødvendig å sende oppdateringer underveis. NIS2 åpner også for mellomrapporter og fremdriftsrapporter før endelig rapport leveres når hendelsen er fullt håndtert.

Hvorfor dette er krevende i praksis

Mange virksomheter oppdager først i en krisesituasjon at:

- Roller og ansvar er uklare
- Beslutningslinjer ikke er definert
- Nødvendig informasjon er spredt på flere systemer
- Rapportering må gjøres manuelt under tidspress

Uten forhåndsdefinerte prosesser, ferdige maler og tydelig eierskap blir kravene i artikkel 23 svært krevende å etterleve.

7. Andre viktige krav i NIS2 du må få med deg

Selv om artikkel 21 og 23 er de mest sentrale, inneholder NIS2 flere andre krav som har stor praktisk betydning.

Ledelsens rolle og kompetanse (Artikkel 20)

NIS2 stiller eksplisitte krav til ledelsen. Det holder ikke lenger at styret "har fått en orientering". Ledelsen skal:

- Forstå risikoen virksomheten tar
- Godkjenne sikkerhetstiltak
- Følge opp etterlevelse
- Sørge for nødvendig kompetanse

Dette betyr i praksis at virksomheten må kunne dokumentere at sikkerhet og risiko er forankret på ledernivå.

NIS2 stiller også krav om at virksomhetens ledelsesorgan skal få opplæring i cybersikkerhet, slik at de er i stand til å forstå risiko, ta informerte beslutninger og følge opp etterlevelsen av regelverket. Det skal samtidig oppmuntres til opplæring for ansatte.

Tilsyn og myndighetskontroll

Myndighetene får utvidede fullmakter til å:
- Føre tilsyn
- Kreve dokumentasjon
- Pålegge konkrete forbedringstiltak

Virksomheter som ikke kan vise struktur og etterlevelse, risikerer både sanksjoner og pålegg som kan være ressurskrevende å etterkomme.

Sammenheng med andre regelverk

NIS2 står ikke alene. For mange virksomheter må det ses i sammenheng med:

- **GDPR**, spesielt der personopplysninger er involvert
- **DORA**, for finansielle aktører
- Interne krav til virksomhetsstyring og internkontroll

En fragmentert tilnærming fører ofte til dobbeltarbeid og uklare ansvarsforhold. En samordnet styringsmodell gir bedre oversikt – og lavere risiko.

8. Vanlige fallgruver i arbeidet med NIS2

Basert på erfaring ser vi noen typiske utfordringer hos virksomheter som jobber med NIS2:

- Compliance behandles som et engangsprosjekt
- Ansvar er uklart mellom IT, juridisk og ledelse
- Risiko vurderes, men følges ikke opp
- Dokumentasjon blir raskt utdatert
- Manuelle prosesser tar for mye tid og gir feil
- Vanskelig å holde oversikt over avhengigheter og risiko i leverandørkjeden

Resultatet er ofte at virksomheten *tror* de har kontroll – helt til de blir bedt om å dokumentere det.

9. Slik bygger dere en strukturert og bærekraftig NIS2-tilnærming

Virksomheter som lykkes med NIS2, jobber systematisk. Ikke fordi de må, men fordi det gir bedre kontroll.

En strukturert tilnærming kan se slik ut:

1. Kartlegg omfang og ansvar

Avklar hvilke deler av virksomheten som omfattes, og hvem som har ansvar for hva.

2. Gjennomfør en gap-analyse

Sammenlign dagens praksis med kravene i artikkel 21 og 23. Identifiser hvor det mangler tiltak, dokumentasjon eller eierskap. Se fremgangsmåte under.

3. Etabler tydelig ansvarsfordeling

Hvert kontrollpunkt må ha en eier. Uten eierskap blir oppfølging tilfeldig.

4. Digitaliser arbeidet

Manuelle prosesser i Excel og e-post er en av de største kildene til manglende etterlevelse. Samle krav, risiko, tiltak og dokumentasjon på ett sted.

5. Følg opp og forbedre kontinuerlig

NIS2 er ikke statisk. Risiko endrer seg, og det samme må sikkerhetsarbeidet gjøre.

Slik gjennomfører du en effektiv gap-analyse

En gap-analyse er rett og slett en sammenligning mellom hvor dere er i dag og hvor NIS2 krever at dere skal være. For mange er dette det første store steget i arbeidet.

Fremgangsmåte:

1. Gjennomgang av Artikkel 21: Gå gjennom de ti minimumskravene i artikkelen. For hvert punkt må dere spørre: "Har vi en skriftlig policy for dette? Er den implementert? Kan vi bevise det?".

2. Identifiser skuffevisjoner: Mange selskaper har fine beredskapsplaner som ligger i en skuff og støver ned. Hvis planen ikke er oppdatert eller testet det siste året, regnes det som et "gap" under NIS2.

3. Vurder teknisk vs. organisatorisk: Et gap er ikke alltid mangel på en brannmur. Ofte er det største gapet mangel på dokumentert opplæring av ansatte eller uklare ansvarsforhold mellom IT og ledelsen.

4. Prioriteringsliste: Når analysen er ferdig, vil dere sitte med en liste over mangler. Prioriter disse etter risiko: Hvilke hull er enklest for hackere å utnytte, og hvilke vil gi størst sanksjoner ved tilsyn?

10. Hvorfor struktur og verktøy er avgjørende

NIS2 stiller krav til sporbarhet, kontinuitet og dokumentasjon. Det betyr at virksomheten må kunne:

- Vise hvilke vurderinger som er gjort
- Forklare hvorfor tiltak er valgt
- Dokumentere at oppfølging skjer over tid

Dette er vanskelig å få til uten struktur og gode verktøy. Gode digitale løsninger kan strukturere og knytte sammen risiko, tiltak og ansvar. Med innebygde varslinger, blir det enklere å dokumentere at NIS2-kravene er gjennomført. På et mer strategisk nivå vil et digitalt verktøy gi ledelsen oversikt og et tilgjengelig beslutningsgrunnlag.

11. Avslutning: Fra regelverk til robust virksomhet

NIS2 representerer et tydelig skifte i hvordan digitale risikoer skal håndteres. Kravene er strengere, forventningene tydeligere og konsekvensene større.

Samtidig gir direktivet en klar retning. Virksomheter som jobber strukturert med risikostyring, sikkerhet og dokumentasjon står bedre rustet. Man blir mer robust ikke bare mot tilsyn, men mot faktiske hendelser.

Med riktig tilnærming kan NIS2 bli en naturlig del av virksomhetsstyringen. Ikke som en byrde, men som et rammeverk for bedre kontroll, høyere robusthet og tryggere drift.

HOUSE OF CONTROL | A COMPANY IN VISMA

Takk for interessen for **House of Control!**

Kontakt

House of Control AS
O.H. Bangs vei 70 1363 Høvik, Norge
+47 815 66 355

www.houseofcontrol.com
mops@houseofcontrol.com
Følg oss: **LinkedIn**