NIS2-status 2026

En skandinavisk markedsanalyse for ledere
og beslutningstakere

Den nye europeiske cybersikkerhetsstandarden:
Trender, utfordringer og strategisk gjennomføring

Innholdsfortegnelse

1. Innledning: Nye krav til digital sikkerhet

Innføringen av EUs NIS2-direktiv (Network and Information Security Directive) innebærer et grunnleggende skifte i hvordan europeiske virksomheter håndterer digital risiko.

NIS2 innebærer juridiske krav til styre og ledelse i virksomheter som omfattes av regelverket, blant annet et direkte ansvar for å føre tilsyn med og godkjenne virksomhetens cybersikkerhetstiltak. Etter det nye direktivet kan ledelsen holdes personlig ansvarlig ved manglende etterlevelse. Det betyr at ledelsen aktivt må delta i risikovurderinger, sikre implementering av robuste sikkerhetsrammeverk og gjennomføre obligatorisk opplæring for å forstå et trusselbilde i stadig utvikling.

Denne rapporten bygger på en markedsundersøkelse gjennomført i februar 2026 av Opinion på vegne av House of Control. Med data fra 462 relevante virksomhetsledere og beslutningspåvirkere i Norge, Sverige og Danmark belyser analysen konkrete beredskapsgap og trender i Skandinavia, med særlig relevans for norske virksomheter som må, eller forventes å måtte, dokumentere etterlevelse overfor kunder og styre, samt følge opp dokumentasjon fra leverandører.

I tillegg til undersøkelsesdataene har vi inkludert House of Controls refleksjoner basert på samtaler med nordiske kunder som forventes å bli berørt av NIS2. Disse delene er merket som «Vårt perspektiv» gjennom rapporten.

Nøkkeldata fra undersøkelsen

Formål: Å kartlegge markedets kjennskap til og den strategiske betydningen av NIS2, samt undersøke hvordan selskaper planlegger å håndtere kommende regulatoriske krav.

Metode: Kvantitativ nettbasert undersøkelse gjennomført i februar 2026 av Opinion.

Målgruppe: Sentrale beslutningstakere i skandinaviske selskaper med mer enn 50 ansatte.

Utvalgsstørrelse: 462 respondenter totalt.

- Norge: 150
- Sverige: 218
- Danmark: 94

Respondentprofil:

- Omtrent seks av ti respondenter har avgjørende, høy eller ganske høy innflytelse på beslutninger innen IT, rapporteringssystemer eller compliance.
- Primærrollene omfatter IT-ledere/CTO (31%) og administrerende direktører/CEOer (16%).
- Utvalget representerer et bredt spekter av sektorer, inkludert offentlig sektor, digital infrastruktur og energi.

2. Oppsummering av hovedfunn

Undersøkelsen fra 2026 viser et skandinavisk marked der kjennskapen er høyere enn den operative beredskapen.

Følgende funn beskriver dagens situasjon i regionen:

- Blant respondentene som kjenner til eller har hørt om NIS2, svarer 62% at direktivet har eller sannsynligvis vil få konsekvenser for selskapet deres. Dette tilsvarer rundt halvparten av totalmarkedet.

- 55% av respondentene kjenner direktivet godt eller til en viss grad. Blant respondentene som sier at NIS2 har eller sannsynligvis vil få konsekvenser for dem, har 15% etablert systemer og prosedyrer for dette arbeidet, og 45% vurderer selskapet sitt som forberedt på NIS2-kravene i dag.

- Manuell compliance-oppfølging er fortsatt tidkrevende. Blant berørte respondenter som kan anslå tidsbruk, rapporterer organisasjonene et gjennomsnitt på **54 timer per måned** på manuell oppfølging. Norge rapporterer det høyeste gjennomsnittet med **83 timer per måned.**

- NIS2 påvirker mer enn virksomheter som er direkte regulert. Blant organisasjoner som opplever konsekvenser av direktivet, er 46% kun indirekte berørt gjennom kunde- eller leverandørkrav, mens ytterligere 14% er både direkte og indirekte berørt. House of Control tolker dette som et tegn på at krav til kunde- og leverandørrapportering kan skape et kommersielt dokumentasjonspress i B2B-relasjoner.

- Implementering av sikkerhetstiltak og dokumentasjon er de mest ressurskrevende aktivitetene. Blant berørte respondenter peker 52% på implementering av sikkerhetstiltak, mens 47% viser til dokumentasjon og oppfølging av hvordan de beskytter IT-systemer og data. Formalisering av krav til leverandører og underleverandører er også betydelig, med 30%.

3. Markedskjennskap: Høy kunnskap, lav beredskap

Undersøkelsen kartla kunnskapsnivået og den opplevde betydningen av NIS2 i Skandinavia.

3.1. Forståelse av direktivet

- **Markedskjennskap:** 55% av respondentene kjenner NIS2-direktivet godt eller til en viss grad.
- **Dyp kunnskap:** 21% av alle respondentene oppgir at de kjenner direktivet godt.
- **Regional variasjon:** Sverige har høyest nivå av dyp kunnskap med 24%, etterfulgt av Danmark med 23% og Norge med 13%.
- **Ledelsesinnsikt:** Blant dem med «betydelig» eller «avgjørende» innflytelse over IT og compliance, kjenner 34% direktivet godt.

3.2. Beredskapsgapet

- **Forberedelse:** Blant respondentene som sier at NIS2 har eller sannsynligvis vil få konsekvenser for selskapet deres, vurderer 45% selskapet sitt som forberedt.
- **Status i dag:** Blant respondentene som sier at NIS2 har konsekvenser for dem, har 15% etablert systemer og prosedyrer for å håndtere dette arbeidet.

3.3. Vårt perspektiv: Gapet mellom å vite og å gjøre

Selv om et flertall kjenner til NIS2, viser undersøkelsen at 55% kjenner direktivet godt eller til en viss grad, 26% har bare hørt om det, og 19% har ikke hørt om det.

I tillegg til undersøkelsesdataene ser House of Control en tydelig trend i dialoger med nordiske selskaper som forbereder seg på å rapportere på NIS2. Mange kjenner til NIS2, men mangler fortsatt en klar og operativ plan for hvor de skal begynne. Kompleksiteten i de nye kravene fører ofte til usikkerhet, noe som gjør det krevende for ledere å omsette juridiske krav til daglige rutiner.

Etter House of Controls erfaring er det en stor hindring at leverandørdata ofte er spredt på tvers av ulike systemer. Dermed finnes det ingen samlet kobling mellom kontrakter og faktiske sikkerhetsrisikoer. I tillegg bruker mange selskaper generiske spørreskjemaer som fungerer som enkle avkrysningsøvelser uten å gi reell innsikt i hva en leverandør faktisk leverer.

4. Omfang og påvirkning: Direkte vs. indirekte ansvar

NIS2 gjelder primært mellomstore og store virksomheter i kritiske sektorer, men rekkevidden strekker seg langt utover direkte regulering.

4.1. Kritiske sektorer i det skandinaviske markedet

Undersøkelsen rettet seg mot relevante ledere i selskaper med mer enn 50 ansatte. Mange respondenter representerer NIS2-relevante sektorer, mens 31% valgte «ingen av disse» på sektorlisten.

- **Offentlig sektor:** 19% av totalutvalget.
- **Digital infrastruktur:** 12% av utvalget.
- **Energi og transport:** Begge sektorer representerer henholdsvis 11% og 10% av utvalget.
- **Klassifisering:** Blant respondentene som fikk dette klassifiseringsspørsmålet, sier 56% at de er en «Important Entity», og 27% sier at de er en «Essential Entity».

4.2. Leverandørkjedens ringvirkninger

- **Indirekte påvirkning:** Blant selskapene som opplever konsekvenser av NIS2, mener 46% av selskapene som er berørt av NIS2, at de er indirekte berørt fordi kunder eller leverandører krever rapportering på NIS2-nivå.
- **Regionale forskjeller:** Danmark har høyest andel som rapporterer indirekte påvirkning (61%), etterfulgt av Norge (50%) og Sverige (39%).
- **Strategisk risiko:** For mange virksomheter kan NIS2-relatert dokumentasjon bli stadig viktigere i B2B-relasjoner, særlig der kunder eller leverandører må rapportere på krav på NIS2-nivå.

4.3. Vårt perspektiv: Dokumentert sikkerhetsarbeid blir stadig viktigere i B2B-relasjoner

Selv om organisasjoner kan ha kontroll på sine direkte leverandører, mangler de ofte innsyn i underleverandører lenger ned i leverandørkjeden. Vi mener at reell robusthet krever en visuell kartlegging av hele leverandørkjeden som identifiserer avhengigheter og vurderer kritikalitet for hver leverandør. For leverandører som er indirekte berørt, vil det være en stor fordel å kunne dokumentere NIS2-statusen sin én gang i en portal og dele den med alle kunder. Dette fjerner behovet for å fylle ut de samme manuelle rapportene gjentatte ganger.

Utover undersøkelsesdataene viser House of Controls dialoger med nordiske selskaper at mange blir overrasket over hvordan NIS2 påvirker dem indirekte. Selv om virksomheten din ikke er direkte regulert, kan kunder be om mer dokumentasjon fra leverandører som del av NIS2-relatert risikostyring i leverandørkjeden.

Vi hører i økende grad om selskaper som møter strenge dokumentasjonskrav bare for å opprettholde eksisterende B2B-kontrakter. Vår erfaring viser at NIS2-relatert dokumentasjon i enkelte B2B-prosesser er i ferd med å bli en forutsetning for å bli vurdert som leverandør. Virksomheter som ikke kan dokumentere at de har god kontroll på sikkerheten, kan stille svakere i kommersielle prosesser.

5. Compliance-belastningen: Sammenligning av manuelt arbeid

Et hovedfunn i rapporten er den høye mengden manuelt arbeid som i dag brukes på compliance.

5.1. Timer brukt på manuelt arbeid

Blant berørte selskaper der respondentene kunne anslå manuell etterlevelsesoppfølging, er de rapporterte gjennomsnittene:

- **Regionalt gjennomsnitt:** 54 timer per måned.
- **Norge:** 83 timer per måned.
- **Danmark:** 53 timer per måned.
- **Sverige:** 45 timer per måned.

5.2. Aktiviteter med høyt ressursbruk

Blant respondenter som sier at NIS2 har konsekvenser for selskapet deres, er de mest ressurskrevende aktivitetene:

- **Sikkerhetstiltak:** 52% mener implementering av tiltak som risikovurderinger, tilgangskontroll og kryptering er mest krevende.

- **Dokumentasjon:** 47% oppgir dokumentasjon og oppfølging av beskyttelse av IT-systemer som en vesentlig belastning.

- **Leverandørstyring:** 30% mener det er svært ressurskrevende å formalisere krav til leverandører og underleverandører.

5.3. Vårt perspektiv: Hvor bærekraftige er manuelle prosesser?

Blant berørte norske respondenter som kunne anslå manuell etterlevelsesoppfølging, er det rapporterte gjennomsnittet 83 timer per måned. Dette er en utfordring vi kjenner igjen fra våre dialoger med markedet. Å basere seg på regneark og manuell oppfølging er ikke bare kostbart og tidkrevende; det skaper også en betydelig risiko for menneskelige feil.

Fra House of Controls perspektiv er konklusjonen klar: manuelle prosesser er ikke lenger bærekraftige. Under NIS2, der ledelsen kan møte personlig ansvar, blir én felles kilde til sannhet stadig viktigere for å opprettholde kontroll, sporbarhet og trygghet.

6. Praktiske neste steg for berørte organisasjoner

Basert på funnene fra Opinion-undersøkelsen og House of Controls dialoger med nordiske selskaper som forventes å bli berørt av NIS2, anbefaler House of Control at berørte organisasjoner prioriterer fire tiltak:

1. Avklar NIS2-eksponeringen
Finn ut om organisasjonen er direkte berørt, indirekte berørt gjennom kunde- eller leverandørkrav, eller begge deler.

2. Kartlegg kritiske leverandører og underleverandører
Etabler innsyn i leverandører, tjenester og avhengigheter som kan skape operasjonell risiko eller etterlevelsesrisiko.

3. Etabler dokumenterte compliance-prosesser
Få på plass strukturerte prosesser for risikovurdering, innsamling av dokumentasjon, leverandøroppfølging og hendelsesrapportering.

4. Reduser avhengigheten av manuelle regneark og fragmentert dokumentasjon
Velg en mer strukturert og sporbar måte å håndtere NIS2-relatert dokumentasjon og oppfølging på.

7. Veien videre: Forenkle NIS2-etterlevelse med House of Control

House of Controls vurdering er at berørte selskaper har kunnskapen, men ofte mangler de spesialiserte verktøyene som trengs for å møte de strenge kravene i det nye direktivet.

For å møte dette behovet utvikler House of Control nå neste generasjon programvare for NIS2-etterlevelse. Løsningen skal gjøre komplekse juridiske krav enklere å håndtere i praksis, også for organisasjoner uten dedikerte sikkerhetseksperter.

Den kommende plattformen skal fungere som et felles informasjonsgrunnlag for hele organisasjonen. Ved å automatisere viktige dokumentasjonsprosesser, gi ledelsen bedre innsikt i digitale risikoer og gjøre det enklere å følge opp leverandørkjeden, hjelper vi virksomheter med å håndtere regulatoriske krav mer effektivt og styrke sin konkurransekraft.

Vi inviterer nå til dialog med organisasjoner som ønsker å være godt forberedt. Vi deler gjerne mer informasjon om løsningen og viser hvordan funnene fra undersøkelsen kan være relevante for din bransje.

Kontakt House of Control for en uforpliktende samtale om NIS2, behov for leverandørdokumentasjon og muligheter for å redusere manuelt compliance-arbeid.

Viktig informasjon: House of Control er et programvareselskap. Vi tilbyr ikke rådgivningstjenester innen NIS2-etterlevelse. Å følge veiledningen eller anbefalingene i denne rapporten garanterer derfor ikke etterlevelse av alle juridiske NIS2-krav.

Innholdet i denne rapporten bygger på undersøkelsesdata samlet inn av Opinion på vegne av House of Control, vår egen research på NIS2-krav og vår erfaring med etterlevelse av regelverk og kundedialoger i det nordiske markedet.

Vi påtar oss ikke ansvar for eventuell manglende etterlevelse av NIS2-krav eller for forhold som måtte oppstå som følge av bruk av denne veiledningen.

HOUSE OF CONTROL

Takk for din interesse for **House of Control!**

Kontakt

House of Control AS
O.H. Bangs vei 70 1363 Høvik, Norge
mops@houseofcontrol.com

www.houseofcontrol.com
Følg oss: Linkedin