Hvordan praktiserer norske virksomheter NIS2-direktivet?

Av Kristian Foss og Sara Lamøy Engberg

Denne artikkelen er en del av artikkelserien om NIS2-direktivet og implemeneteringen i de nordiske landene. Tidligere artikler:

- *Agne Lindberg, Petri Dahlström, Klara Thyrén: Ny cybersäkerhetslag – den svenska regeringens förslag till införlivande av NIS2-direktivet Lov & Data nr. 163 3/2025*
- *Veikko Vauhkonen: Implementeing the NIS2 Directive in Finland: The New Cybersecurity Act, Lov & Data nr. 164 4/2025*

Kristian Foss

Sara Lamøy Engberg

NIS2-direktivet (direktiv (EU) 2022/2555) har ennå ikke blitt norsk lov, men flere virksomheter har begynt å forberede seg. Dette gjelder særlig private virksomheter og aller mest de som har kunder eller eiere i EU, hvor NIS2 allerede har trådt i kraft. I EU har 19 land så langt implementert NIS2.

Forberedelsene omfatter konkrete GAP-analyser, påbegynt tilpasning på teknisk og juridisk nivå, informasjon til ledelse og styrer mv. Vår erfaring er imidlertid at mange offentlige virksomheter enda ikke har kommet i gang med NIS2-forberedelsene.

Når man leser trussel- og risikovurderingene for 2026 lagt frem av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM), kan man lure på hvorfor ikke flere offentlige virksomheter er i gang:

> *Norge befinner seg i den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. (Nasjonal trusselvurdering 2026, PST, s. 4)*

NSM, som skal forvalte NIS2, følger opp dette i sin rapport:

> *Det som skaper motstandsdyktighet er langsiktig og systematisk sikkerhetsarbeid. Iverksett konkrete tiltak for å beskytte deres viktigste verdier. (Risikorapport 2026, NSM, s. 8)*

Rådene fra NSM er klare og praktiske:

> *Kjenn dine verdier. Reduser sårbarheter. Bygg reserveløsninger. Konsekvensene av en uønsket hendelse kan bli de samme, enten årsaken er en trusselaktør eller en tilfeldig, teknisk eller menneskelig feil. (Risikorapport 2026, NSM, s. 8)*

På mer overordnet nivå finner Nasjonal sikkerhetsstrategi og Nasjonal sikkerhetsplan for digital infrastruktur for digital infrastruktur, som peker samme vei. Totalberedsskapsmeldingen: Forberedt på kriser og krig, kan også nevnes. Alle tre er fra 2025.

Både vi og samarbeidspartnerne våre innenfor cybersikkerhet er overrasket over hvor få konkrete henvendelser vi har fått, særlig fra offentlig virksomheter. Vi tror at grunnen til dette er todelt. For det første er direktivet enda ikke norsk rett, slik at man ikke vet eksakt hvordan det vil bli implementert i norsk rett. For det andre er mange offentlige organer allerede omfattet av sikkerhetsloven.

Erfaringen vår er at private virksomheter er særlig motivert av to forhold når det kommer til cybersikkerhet, i tillegg til omdømmerisikoen ved cybersikkerhetsangrep. Virksomheter uten eksponering mot EU er særlig opptatt av ledelsens potensielle personlige ansvar. Virksomheter som har kunder og/eller eiere i EU, er opptatt av å oppfylle kravene allerede nå for å kunne være konkurransedyktige.

For virksomheter som er opptatt av ledelsens personlige ansvar, begynner prosessen typisk ved at vi rådgiver styret, gjerne med ledelsesgruppen til stede. Om ansvaret blir objektivt eller avhengig av skyld (uaktsomhet eller forsett), vet vi ikke før NIS2 blir norsk lov. At en-

keltpersoner kan bli personlig erstatningsansvarlige, virker imidlertid å være noe en del ledere kjenner til fra tradisjonelt styreansvar. En refleksjon i den forbindelse er at begrepet «styreansvar» er villedende. Vi opplever ofte at det kommer som en overraskelse på toppledere at også ledere langt ned i organisasjonen kan stilles personlig ansvarlig.

Ledere i det offentlige er muligens enda mindre bevisst på at også de kan bli personlig ansvarlige.

En nyvinning innført i digitalsikkerhetsloven (dsl.), som innfører NIS1 og deler av NIS2, er at det personlige ansvaret også kan omfatte overtredelsesgebyret. Det skal likevel noteres at terskelen antagelig vil være noe høyere, da forarbeidene til digitalsikkerhetsloven presiserer at fysiske personer kan ilegges overtredelsesgebyr «dersom det er nødvendig i det enkelte tilfelle».[1] Reguleringen viderefører trenden mot mer personlig ansvar, og det er ingen grunn til å tro at dette prinsippet vil fravikes når NIS2 implementeres i norsk rett sammen med CER (Direktiv om kritiske enheters motstandsdyktighet) .

Norske virksomheter har fortsatt tid fram til implementeringen av NIS2 (og CER) til å områ seg. For virksomheter som ønsker salg til kunder i Europa, er oppfyllelse av kravene sentralt for å kunne være konkurransedyktige. Dette gjelder uavhengig av implementering i Norge. For virksomheter som allerede har et fokus på og system for cybersikkerhet eller som oppfyller digitalsikkerhetsloven, skal det antagelig ikke så mye til for å oppfylle kravene i NIS2. Men veien til ansvar kan bli kort dersom man ikke engang har foretatt en vurdering av virksomhetens forhold til NIS2.

> For virksomheter som allerede har et fokus på og system for cybersikkerhet eller som oppfyller digitalsikkerhetsloven, skal det antagelig ikke så mye til for å oppfylle kravene i NIS2.

Disse regelverkene viderefører altså trenden mot mer personlig ansvar. Dette personlige ansvaret føres også oppover i selskapsstrukturen, til morselskapet (dsl. § 17 (2)). Sammen med risikoen for forstyrrelser i egen drift- og tjenesteleveranse og det potensielle omdømmetapet knyttet til sikkerhetsbrudd, antar vi risiko for personlig ansvar er motivasjon for de fleste virksomheter, både offentlige og private.

Med risiko for avledet ansvar oppover i konsernet, vil også konsernledere få et sterkt incitament til å sørge for etterlevelse i datterselskapene. Slik verden ser ut i dag, bør imidlertid både offentlige og private virksomheter være aller mest motivert av å unngå forstyrrelser av egen drift og tjenesteleveranse.

Hva gjør virksomhetene?

Som vi var inne på innledningsvis, har de mest profesjonelle virksomhetene begynt å forberede seg. Selskaper som allerede har god sikkerhetskultur jobber videre slik de tidligere har gjort. Andre selskaper starter med mer eller mindre blanke ark, og må lære seg mer om sikkerhet.
De viktigste aktivitetene vi ser er like lite banebrytende som de er fornuftige:

- Risikoanalyser. Uten å vite sikkerhetsstatus kan man heller ikke vite hva man må ta tak i.
- Gap-analyser. Med kjent status og ønsket mål, kan et gap - deltaen - fastsettes.
- Strategier. Basert på faktisk tilstand og det målet virksomheten setter seg - gapet - må en plan legges. Status, mål, tiltak, ansvarlige og øvrig plan blir strategien.
- Ansvarliggjøring. Uten ansvarlige roller blir lite gjort. Ansvarliggjøringen bør skje skriftlig, ved instrukser (internt) og avtaler (typisk med underleverandører), og støtte opp om strategien.
- Readiness-prosjekter. Vår samarbeidspartner Defendable melder om en del kunder som har kommet til konkret gjennomføring, i såkalte readiness-prosjekter.

Hva skal virksomhetene gjøre når NIS2 blir lov?

NSM uttaler i sin rapport at:

> *«Styringen må omfatte alle fagområder, fra digital og fysisk sikkerhet til personellsikkerhet og sikkerhetskultur. Sikkerhet er et lederansvar. (Risikorapport 2026, NSM, s. 8)*

Det er et godt sted å starte. Innføringen av DORA-loven, for finansiell sektor, kan trolig gi oss en pekepinn. Enda tydeligere enn for NIS2 krever DORA at finansvirksomhetene sikrer egne leveranseketjeder. Det betyr i praksis avtaler med underleverandører.

Normalgangen har så langt vært at finansforetakene sender en lang liste med krav til sine underleverandører. Kravene er ofte ganske generelle, uavhengig av hvor kritisk underleverandøren er. Vi mener dette er en for generell tilnærming. Når vi bistår en underleverandør, eller kundesiden, er første skritt å vurdere om underleverandøren støtter «kritiske og viktige funksjoner» hos finansforetaket. Ofte er det ikke tilfelle, slik at kravlisten kan fjernes eller trimmes kraftig ned.

Underleverandørenes svar på finansforetakenes lister med krav, er typisk å utarbeide et standard vedlegg

1 Prop. 109 LS (2022-2023) kap. 9.5.: «Etter forslaget kan imidlertid overtredelsesgebyr ilegges fysiske personer som opptrer på vegne av en tilbyder dersom det er nødvendig i det enkelte tilfellet.»

for finansielle underleverandørtjenester. De særlige kravene til sikkerhet og rapportering som følger med DORA, medfører en ekstra kostnad for underleverandørene, som de gjerne ønsker å ta seg betalt for.

For å skape en sikker leverandørkjede, er neste skritt å sikre seg videre nedover, overfor egne underleverandører.

Målet er, som NSM skriver i sin rapport:

> *Både små og store virksomheter på tvers av ulike sektorer må være forberedt på å håndtere hendelser i cyberdomenet. (Risikorapport 2026, NSM, s. 8)*

Endrer Digital Omnibus noe for NIS2?

19. november 2025 leverte EU-kommisjonen et forslag til en rekke forenklinger av EUs digitale regelverk. Formålet med Digital Omnibus er å styrke konkurranseevnen til europeiske virksomheter gjennom å forenkle og strømlinjeforme EUs mange regelverk innenfor det digitale området. En av hovedendringene som skal sikre strømlinjeforming, er innføringen av en enhetlig rapporteringsportal, som skal være et «single EU-wide entry point» for hendelsesrapportering. I tillegg har kommisjonen lagt frem et forslag om et direktiv knyttet til forenklinger i NIS2, hvor formålet er å gjøre regelverket tydeligere gjennom å forenkle reglene om jurisdiksjon (når en virksomhet er omfattet av regelverket), legge opp til mer effektiv innsamling av data om løsepengeangrep samt tilrettelegge for grensekryssende enheter og koordinering.

Forenklingspakken er ennå ikke vedtatt, og vi anbefaler å følge med på utviklingen. Men endringene som foreslås er uansett ikke av en slik karakter at virksomheter som omfattes av NIS2 bør tenke annerledes på hvordan man bør forberede seg til implementeringen av NIS2.

Sier NIS2 noe om digital uavhengighet?

I lys av at verdensordenen slik vi har kjent den siden andre verdenskrig er i ferd med å rakne, blir kravene til digital uavhengighet mer interessante. NSM forklarer:

> *Dersom virksomheter er avhengige av en enkelt leverandør, eller leverandører fra samme land, oppstår det som kalles konsentrasjonsrisiko. Norske virksomheter er på flere samfunnsområder avhengig av produkter, teknologi og tjenester fra andre land. Fornybar energi, moderne kjøretøy og skytjenester er noen få eksempler. Det er ikke den enkelte anskaffelsen som er problemet, men det er det samlede omfanget som er en nasjonal utfordring. (Risikorapport 2026, NSM, s. 8)*

Ifølge NSM er altså for mange virksomheter avhengig av noen få leverandører. Dette gir disse leverandørene, og i forlengelsen også landene de har sin hovedvirksomhet i, svært stor makt. Dermed er norsk næringsliv og infrastruktur svært sårbart, dersom tilgangen til disse leverandørenes tjenester, eller forutsetningene for fortsatt leveranse, skulle endre seg.

En endring vi derfor ser er at den tidligere refleksaktige «cloud first»-holdingen er på retur. Både private og offentlige virksomheter forstår risikoen ved å være avhengig av de store amerikanske skyleverandørene for kritiske systemer. En del private virksomheter begynner å forstå at norsk eller europeisk systemdrift kan gi et konkurransefortrinn.

NIS2 stiller krav til digital uavhengighet gjennom sitt krav til «tilgjengelighet» (art. 21 jf. art. 6). Kravet er at «security of network and information systems» skal være «passende» og «proposjonal» i forhold til risikoen.

I februar 2025 ble Karim Khan, sjefsaktor i Den internasjonale straffedomstolen (ICC), utestengt fra sin tilgang på Microsofts epost. Dette skjedde som følge av en arrestordre på den israelske statsministeren Benjamin Netanyahu for hans ansvar for overgrepene på Gaza. Microsoft, som har vært blant de mer kritiske til Trump, ble tvunget til å utestenge Khan gjennom et presidentdekret fra Trump. Khans britiske bankkonti ble også frosset. I tillegg fikk mange av de 900 ansatte i ICC innreiseforbud til USA.

ICC-saken viser at fullt lovlige og legitime aktiviteter kan rammes om Donald Trump ikke liker dem. Det betyr at en grunnleggende usikkerhet er introdusert til amerikanske IT-leverandører, som ikke tidligere var der. Det er nødt til å få konsekvenser for hvordan vi i Norge vurderer risikoen ved bruk av særlig amerikanske leverandører.

Et legitimt spørsmål norske virksomheter må vurdere er om det vil være forsvarlig å drifte systemer som er kritiske for det norske samfunnet på amerikanskkontrollert skyinfrastruktur. Hvor arbeidet med kartleggingen av slik sårbarhet står, er vi ikke kjent med. Vi ser imidlertid at flere kommuner begynner å se på muligheten for digital uavhengighet. En av de som har kommet lengst, er Larvik kommune, som over tid har jobbet aktivt for å sikre reell leverandørkontroll og valgmuligheter gjennom å frigjøre seg fra avhengigheten til de største, amerikanske leverandørene. Manglende vurderinger og tiltak i denne forbindelse vil, i lys av de regler som gjelder i dag og de som kommer, alene trolig kunne bety personlig ansvar for personer i offentlig sektor.

Kristian Foss, advokat, Bull & Co advokatfirma.

Sara Lamøy Engberg, senioradvokat i Advokatfirmaet Bulls avdeling for teknologi, personvern og IP.