vegtilsynet

Tilsynsrapport - sak 2026-01

Styring av sikkerhet i digitale systemer i Nye Veier AS

vegtilsynet

Saksnummer	2026-01
Publiseringsdato	30.04.2026
Tilsynslag	Thomas Ruud Sollien, tilsynsleder Iver Fiksdal, ekstern revisor, Deloitte AS
Tilsynspart	Nye Veier AS
Tilsynsform	Tilsynsmøte

Om rapporten

Rapporten er basert på tilsyn i Nye Veier AS. Tilsynssaken omhandler styring av sikkerhet i digitale systemer med betydning for sikkerheten i veginfrastrukturen.

Vegard Hansen
direktør

Thomas Ruud Sollien
tilsynsleder

Rapporten er godkjent elektronisk og har ingen signatur.

Sammendrag

Digitalisering og ny teknologi i vegsektoren gir både muligheter og nye risikoer, inkludert trusler mot trafikksikkerheten. Derfor er det viktig å ha kontroll på digitale systemer som styrer trafikk og beredskap.

Målet med tilsynssaken har vært å undersøke om Nye Veier AS har et styringssystem som sikrer oppfyllelse av krav til digital sikkerhet knyttet til veginfrastrukturen.

Tilsynet ble gjennomført som et tilsynsmøte etter revisjonsprinsippene i NS-EN ISO 19011:2018 *Retningslinjer for revisjon av ledelsessystemer*. Bevisinnhentingen i tilsynssaken var avgrenset til informasjon fra møtet og gjennomgang av relevante dokumenter i Nye Veier AS sitt styringssystem.

Hovedfunn i tilsynet har vært:

- Tilsynspart sitt arbeid for å identifisere risiko synes å være betryggende for de IT-systemer som tilsynspart benytter.
- Vegtilsynet stiller spørsmål om i hvilken grad det ligger systematiske risikovurderinger/-analyser til grunn for tilsynspart sine vurderinger av risikoer, trusler og sårbarheter i OT[1]-systemer selskapet benytter i sitt arbeid.
- Tilsynspart sitt arbeid med å vurdere risiko, iverksette risikoreduserende tiltak og evaluere effekten av de risikoreduserende tiltakene synes å være systematisk når det gjelder IT-systemer.
- Tilsynspart bør sikre at den systematikken som er etablert knyttet til identifisering og håndtering av risiko når det gjelder IT, også utvides til å omfatte OT-systemer og OT-sikkerhet. Dette vil særlig være viktig fremover når det forventes en større grad av integrasjon mellom IT og OT.

Vegtilsynet har i saken gitt to observasjoner:

1. Nye Veier AS bør gjennomføre systematiske risikovurderinger knyttet til digital sikkerhet som også dekker OT-systemer og OT sikkerhet. Dette for å sikre et

[1] OT – Operasjonell teknologi, refererer gjerne til maskinvare- og programvaresystemer som benyttes til å overvåke, kontrollere og administrere fysiske prosesser.

oppdatert og helhetlig bilde av trusler, sårbarheter og sikkerhetsmessige konsekvenser av uønskede hendelser.

2. Nye Veier AS bør sikre helhetlig systematisk for vurdering av risiko, iverksettelse av risikoreduserende tiltak og evaluering av tiltakenes effekt som også dekker OT-systemer og OT-sikkerhet.

Innhold

1. Bakgrunn

Digitalisering av vegsektoren og innføring av ny teknologi gir økte muligheter. Samtidig skaper digitalisering også nye og ukjente sårbarheter og risikoer – også for trafikantene sin sikkerhet. Å ha kontroll på de digitale systemene er viktig for at verdikjeden skal fungere, bl.a. knyttet til trafikkstyring og beredskap ved hendelser. I Nasjonal strategi for digital sikkerhet[2] framheves viktigheten av forebyggende arbeid ved å foreta risikovurderinger og gjennomføre tilstrekkelige tiltak for å beskytte seg mot uønskede hendelser.

Forskrift om vegdata, trafikkinformasjon, trafikkberedskap og trafikkstyring m.m. for offentlig veg (vegdata- og trafikkinformasjonsforskriften), med ikrafttredelse 01.04.2025, stiller i § 6-1 ulike typer krav til aktører i vegsektoren knyttet til digital sikkerhet.

Et styringssystem for informasjonssikkerhet skal gjennom en prosess for risikostyring bidra til at konfidensialiteten, integriteten og tilgjengeligheten til informasjon bevares.[3]

- Konfidensialitet dreier seg om at informasjon ikke blir kjent for uvedkommende.
- Integritet handler om at informasjon ikke blir endret av uvedkommende, eller på en utilsiktet måte.
- Tilgjengelighet betyr at informasjon skal være tilgjengelig for autoriserte brukere ved behov.

Vegtilsynet ønsker å undersøke sikkerhetsstyringen i digitale systemer i Nye Veier AS med betydning for sikkerheten i veginfrastrukturen.

[2] Nasjonal strategi for digital sikkerhet - regjeringen.no
[3] Jf. ISO/IEC 27001:2023 Ledelsessystemer for informasjonssikkerhet

2. Mål

Målet med tilsynet har vært å undersøke om Nye Veier AS har et styringssystem for å sikre at krav til digital sikkerhet knyttet til veginfrastrukturen blir oppfylt.

3. Metode og gjennomføring

Metode

Tilsynssaken er gjennomført som et tilsynsmøte. Dette er en av tilsynsformene Vegtilsynet har etablert for å føre tilsyn med at Statens vegvesen og Nye Veier AS. Tilsynsformen bygger på alminnelige revisjonsprinsipp, jf. ISO 19011:2018[4].

Vegtilsynet benytter tilsynsmøter for å skaffe kunnskap om og ha dialog med tilsynspart om utvalgte trafikksikkerhetsmessige forhold. Tilsynsformen blir også benyttet innenfor andre områder, der Vegtilsynet ser at det kan være hensiktsmessig å gjennomføre et mer overordnet og dialogpreget tilsyn.

Vegtilsynet vil gjøre oppmerksom på at bruk av tilsynsmøte som tilsynsform innebærer at det ikke er gjennomført et fullstendig systemtilsyn av Nye Veier AS sitt system og rutiner for styring av sikkerhet i digitale systemer. Det er heller ikke undersøkt om etablerte system og rutiner blir etterlevd, eller om de har tilsiktet effekt for alle digitale systemer. Tilsynet utgjør derfor ingen fullstendig verifikasjon av om Nye Veier AS ivaretar digital sikkerhet for alle IT- og OT-systemer med relevans for trafikksikkerheten knyttet til riksveg.

For denne tilsynssaken er det er fastsatt fem tilsynskriterier[5], utledet fra vegdata- og trafikkinformasjonsforskriften, jf. kap. 1.

Saken er avgrenset til sikkerhetsstyringen i digitale systemer i Nye Veier AS med betydning for sikkerheten i veginfrastrukturen. Bevisinnhenting i saken er avgrenset til informasjon som kom fram i tilsynsmøtet og gjennomgang av utvalgte dokumenter i Nye Veier AS sitt styringssystem.

Digitale systemer med betydning for sikkerheten i veginfrastrukturen omfatter blant annet (ikke uttømmende liste):

- Digitale systemer som umiddelbart kan endre objekter og veginfrastruktur

[4] ISO 19011:2018 Retningslinjer for revisjon av ledelsessystemer
[5] Se kap. 4 Tilsynsresultat

- Digitale systemer som er en del av en beredskapsfunksjon
- Digitale systemer som er nødvendig for å ivareta veginfrastruktur
- Digitale systemer som er nødvendig for utføre og følge opp drift av veginfrastruktur.

Gjennomføring

Vegtilsynet sendte varsel om tilsyn 26.01.2026 og gjennomførte tilsynsmøtet 03.02.2026. Representasjon fra tilsynspart sin side i tilsynsmøtet framgår av tabell 1.

Tilsynet har hatt slik framdrift:

Dato	**Framdrift**
26.01.2026	Varsel om tilsyn
03.02.2026	Åpningsmøte
03.02.2026	Tilsynsmøte der representanter fra følgende deler av Nye Veier AS sin organisasjon deltok: - Økonomi, finans og virksomhetsstyring - Sikkerhet, organisasjon og digitalisering - Utbedring og drift - Juridisk
13.04.2026	Rapportutkast oversendt for faktasjekk.
30.04.2026	Endelig tilsynsrapport

Tabell 1: Gjennomføring og framdrift av tilsynssaken

Utkast til rapport ble sendt tilsynspart for faktasjekk 13.04.2026. Tilsynspart meldte i oversendelse datert 24. april 2026 at de ikke hadde kommentarer eller forslag til justeringer i det oversendte utkastet til rapport eller behov for sluttmøte i saken.

Vegtilsynet opplever at det har vært god dialog mellom partene, der tilsynspart har lagt forholdene til rette for en effektiv og god gjennomføring av tilsynet.

4. Tilsynsresultat

Symboler som er brukt for å illustrere tilsynsfunnene i rapporten går fram av tabellen under.

Symbol	Vurdering av samsvar med tilsynskriterium
🔴	Avvik: Manglende samsvar med krav
🟡	Observasjon: Forhold der man gjennom tilsynet har sett at det er potensial for forbedring hos tilsynspart
🟢	Undersøkelsen har ikke avdekket avvik eller observasjoner

Tabell 2: Illustrasjon på tilsynsfunn

Tilsynskriterium (TK):
Virksomheten skal ha et styringssystem for digital sikkerhet. Sentrale krav knyttet til et slikt system for styring av digital sikkerhet vil være:
TK 1: Virksomheten skal identifisere risiko
TK 2: Virksomheten skal vurdere identifiserte risikoer
TK 3: Virksomheten skal iverksette risikoreduserende tiltak/kontrollaktiviteter
TK 4: Virksomheten skal evaluere effekten av iverksatte tiltak
TK 5: Virksomheten skal justere/tilpasse risikoreduserende tiltak/kontrollaktiviteter

Utledning av tilsynskriterium:
Virksomheten må kjenne til eksterne krav for å kunne ha kontroll med at styringssystemet er innrettet slik at det sikrer oppfylling av relevante eksterne krav. Plikten til å sikre sammenheng mellom eksterne krav og styringssystemet går fram flere steder i Prop. 160 L (2015-2016) *Endringar i veglova (Vegtilsynet)* bl.a. kap. 2.2. I dette punktet er det presisert at et styringssystem skal «innehalde ei beskriving av aktivitetar for å nå dei mål og for å sikre etterleving av dei krav som er satt til tryggleiken knytt til riksveg».

For denne saken betyr dette at vegdata- og trafikkinformasjonsforskriftens krav til digital sikkerhet må være operasjonalisert og beskrevet i Nye Veier AS sitt styringssystem på en slik måte at det legges til rette for at forskriften etterleves.

Det følger av forskriften § 6-1 første ledd at Nye Veier AS gjennom planlagte og systematiske tiltak skal, i henhold til nasjonale og europeiske sikkerhetsstandarder, normer og regelverk, sørge for tilfredsstillende behandling av data og informasjon. Av Vegdirektoratets veileder til forskriften[6] framgår det at dette medfører at «Det skal foreligge risikovurderinger av de digitale systemene som er i eller tilknyttet vegnettet og av systemene og løsningene for de nasjonale tjenestene.»

Av forskriften § 6-1, andre ledd framgår det at Nye Veier AS skal stille krav til sikkerhet og beskyttelse, inkludert tilgangsstyring, i henhold til sikkerhetsstandarder og normer for datasystemer og tjenester, samt til tilknytningspunkt, kommunikasjonsinfrastruktur og utstyr. I nevnte veileder trekkes ISO 2700-serien og IEC 62443-standardene fram som relevante sikkerhetsstandarder og normer.

På bakgrunn både av kjent risiko og sannsynlig fremtidig risiko, legger Vegtilsynet til grunn at tilsynsparts styringssystem for å være tilstrekkelig og effektivt, bør omfatte digital sikkerhet i både IT- og OT-systemer.

Om **innretning og bruk av informasjonsteknologi (IT) og operasjonell teknologi (OT) i Nye Veier AS**

Nye Veier AS benytter en rekke ulike IT-systemer og -applikasjoner i sitt daglige arbeid, både i sentraladministrative operasjoner (ERP-system, ulike kommunikasjons- og arbeidsapplikasjoner under Microsoft-paraplyen mv.), og ved utførelse av veirelaterte arbeidsoppgaver. Nye Veier AS har eksempelvis anskaffet et digitalt forvaltnings-, drifts- og vedlikeholdssystem (FDV-system), der alle objekter som selskapet skal drifte og vedlikeholde legges inn (f.eks. skilt, skjæringer, konstruksjoner og utstyr i tunneler). Nye Veier AS benytter videre operasjonell teknologi (OT) i form av eksempelvis sensorer og IoT-teknologi (Internet of Things), for å samle informasjon som er relevant for drift og vedlikehold, og som inkluderes i FDV-systemet.

I tilsynsmøtet informerte Nye Veier AS og at det på sikt er planlagt at informasjon om objekter i FDV-systemet skal kobles mot inspeksjon- og vedlikeholdsplaner, slik at man skal kunne få automatiske varsler om når objekter skal kontrolleres, og registrere ev. avvik

[6] Veiledning til forskrift om vegdata, trafikkinformasjon, trafikkberedskap og trafikkstyring m.m. på offentlig veg, datert 02.05.25

og oppfølgingsbehov i sanntid når kontrollene gjennomføres. I tilsynsmøtet viste imidlertid tilsynspart til at systemet per i dag er frittstående og ikke koblet direkte mot objektene, og at utstyr/OT ute på veg ikke er påvirkbart gjennom systemet. Selv om det i systemet ligger informasjon om utstyr som har betydning for trafikksikkerhet, peker Nye Veier AS på at endringer/justeringer på utstyret som faktisk påvirker sikkerheten på veg, ikke kan gjøres via nett av Nye Veier AS, men må foretas fysisk på stedet.

I forlengelsen av dette viste tilsynspart i møtet til at Nye Veier AS heller ikke for andre systemer/områder har noe selvstendig informasjonssikkerhetsansvar for OT/utstyr som har direkte betydning for trafikksikkerhet. Tilsynspart pekte på at de kun har lesetilganger til de systemer og det OT-utstyr de oppfatter at har sikkerhetsmessige betydning (f.eks. systemer som styrer bommer, vifter og veikantutstyr), og at ansvar for informasjonssikkerheten for system/utstyr ligger hos andre, eksempelvis Vegtrafikksentralene (VTS-ene) og entreprenører. Nye Veier AS opplyser samtidig at dette er i endring slik at OT-systemene i fremtiden vil måtte åpnes for mer fjerntilgang og økt styring/kontroll fra Nye Veier AS direkte. Dette for i større grad å kunne hente ut de verdier og den operasjonelle effektiviteten som er forventet av selskapet. Det ble fra tilsynspart påpekt at en slik utvikling vil medføre et endret risikobilde.

I Nye Veier AS sin årsrapport for 2024 blir det videre vist til at Nye Veier AS er eksponert for angrep mot selskapets IT- og OT-systemer og forsøk på økonomisk kriminalitet. Vegtilsynet forstår dette som at Nye Veier AS har risiko i sine systemer knyttet til mulig kompromittering av informasjon i systemer ved cyberangrep, herunder også informasjon som ligger i OT-systemer og som potensielt kan ha betydning for sikkerhet på vei. Vegtilsynet registrerer også at det i internrevisjonsrapport fra 2025 om OT-sikkerhet fremkommer observasjoner og anbefalinger knyttet til risikostyring, internkontroll og tekniske kontroller, for å styrke OT-sikkerheten.

Organisering av arbeid med digital sikkerhet i Nye Veier AS

I tilsynsmøtet ble tilsynspart innledningsvis bedt om å redegjøre kort for den overordnede organiseringen av arbeidet med sikkerhet i digitale systemer/informasjonssikkerhet, herunder roller, ansvar og oppgaver både i det overordnede informasjonssikkerhets-arbeidet og med hensyn til enkeltvise systemer Nye Veier AS benytter. I tilknytning til

disse spørsmålene, opplyste tilsynspart at det per i dag opereres med to forskjellige organisasjoner for å håndtere sikkerhet innen henholdsvis IT og OT, men at tilsynspart i styringsdokumenter forsøker å håndtere IT og OT innenfor samme rammeverk i de samme styrende dokumenter. Det vises også til at man ser at OT i stadig større grad blir en del av IT-strukturen i virksomhet, og at det fremover vil være viktig å se IT og OT i tydelig sammenheng.

Samtidig opplyser tilsynspart at det per i dag ikke eksisterer koblinger mellom IT- og OT-systemer som medfører risiko for at manglende ivaretakelse av digital sikkerhet vil medføre redusert sikkerhet på vei. Tilsynspart opplyser at:

- Nye Veier AS kun har lesetilgang i systemer som styrer bommer, vifter og veikantutstyr. Nye Veier AS har ansvar for at sikkerheten knyttet til drift av denne infrastrukturen ivaretas, men opererer ikke som styrende og definerende part for systemene som styrer skilting, bommer mv. Dette blir håndtert av VTS-ene, og Nye Veier AS sitt ansvar blir opplyst å begrense seg til å respondere på og håndtere meldinger fra VTS-ene sine IT-systemer tilknyttet driftsmessige forhold.
- Nye Veier AS har ingen egne OT-systemer de har ansvar for, og som har nettilgang og dermed må sikres i henhold til anerkjente digitale sikkerhetsprinsipper for å unngå at systemer kompromitteres og sikkerhet på vei reduseres.

Tilsynspart legger til at de tror ovennevnte situasjon vil endre seg fremover. Nye Veier AS jobber aktivt med å optimalisere arbeidet med drift av de veistrekninger selskapet har ansvar for, herunder med å ta i bruk teknologi i både styring og utførelse av arbeidet. Tilsynspart ser derfor for seg at integrasjonen mellom IT og OT vil bli vesentlig større i tiden som kommer, og at Nye Veier AS selv vil ha ansvar for flere OT-løsninger der digital sikkerhet også må ivaretas. Dette kan eksempelvis handle om økt digitalisering i innretning og bruk av FDV-systemet til Nye Veier AS, slik at dette blir mer effektivt og økonomisk i bruk. I dag har selskapet et objektbasert, frittstående FDV-system der de har samlet informasjon av sine vegstrekninger. Systemet er basert på import av data, og er ikke koblet direkte mot anleggene, noe som innebærer at informasjonen som ligger i systemet om utstyr av sikkerhetsmessig betydning, ikke er direkte påvirkbart gjennom systemet (men at man for å kompromittere utstyret må ut fysisk *on-site)*.

Når det gjelder den spesifikke organiseringen av arbeidet med sikkerhet i digitale systemer/informasjonssikkerhet, herunder roller, ansvar og oppgaver for henholdsvis IT- og OT-sikkerhet, viser tilsynspart til at det er et tydelig skille mellom IT- og OT-miljøene i organisasjonen, med begrenset samarbeid, for eksempel i forbindelse med risikovurderinger av informasjonssikkerhetsrisikoer. Det er utarbeidet stillingsbeskrivelser for relevante roller i sikkerhetsarbeidet for begge de to miljøene. Videre er det utarbeidet en rekke styringsdokumenter knyttet til digital sikkerhet, og som er ment å dekke både IT og OT, herunder bl.a.:

- Overordnet styringsdokument for risikostyring
- Overordnet styringsdokument for informasjonssikkerhet
- Informasjonssikkerhetsinstruks
- Instruks for sikker bruk av informasjonsteknologi
- Instruks og prosedyre for tilgangsstyring

Tilsynskriterium 1: Virksomheten skal identifisere risiko

Bevis

Vegtilsynet stilte i tilsynsmøtet spørsmål ved om det har blitt gjennomført systematiske risikovurderinger for å identifisere og vurdere informasjonssikkerhetsrisikoer for alle systemer som er vesentlige for trafikksikkerheten på vegene, både IT- og OT-systemer. Nye Veier AS informerte om følgende:

- Det gjennomføres kvartalsvise risikovurderinger i IT-avdelingen, i henhold til styringsdokument og tilhørende prosedyrer og maler for risikovurdering, opp mot avdelingens målbilde (som omfatter IT-sikkerhet). Dersom det i kvartalsvurderingene/-kartleggingene blir oppdaget forhøyet IT-sikkerhetsrisiko, blir dette fulgt opp og tatt tak i jf. de prosedyrer som er etablert i de styrende dokumentene.
- Det pågår i tillegg kontinuerlig arbeid med å vurdere risiko i driftsbildet i IT-systemene, blant annet gjennom monitorering av ivaretakelse av etablerte sikkerhets-KPIer (som f.eks. en Microsoft Secure Score på 85, et mål som viser den prosentvise sikkerhetsgraden (0-100 %) i en virksomhets IT-sikkerhet, sammenliknet med relevant industristandard).

- Arbeid med vurdering og oppfølging av risiko er også inkorporert i drift av IT-systemporteføljen og hvert enkelt IT-system, og skjer blant annet gjennom kjøp av tjenester fra ulike selskap (månedlig patching, tetting av sikkerhetshull mv).
- Når det gjelder OT, blir det gjennomført prosjektspesifikk og/eller tematiske risikovurderinger, eksempelvis vurderinger knyttet til fysisk sikring av styringsskap.

Vurdering

Vegtilsynet vurderer, på grunnlag av informasjonen som fremkom i tilsynsmøtet og dokumentasjon gjort tilgjengelig av Nye Veier AS, at tilsynspart sitt arbeid for å identifisere risiko synes å være betryggende for de IT-systemene som tilsynspart benytter. Prosessbeskrivelser, instrukser og prosedyrer som foreligger, indikerer god systematikk i arbeidet med vurdering av risiko i disse systemene, og det synes å være høy bevissthet i IT-organisasjonen om vurdering og oppfølging av risikoer og sårbarheter i systemene.

I tilsynsmøtet ble det i liten grad presentert noen systematisk tilnærming til å holde oversikt over risikoer, trusler og sårbarheter i OT-systemer Nye Veier AS benytter i driftsarbeid. Videre ble det i tilsynsmøtet ikke fremlagt informasjon som tilsier at det er gjennomført helhetlige risikovurderinger av de aktuelle systemene, eller på annet vis arbeides med å sikre fullstendig og oppdatert informasjon om risiko, trusler og sårbarheter knyttet til alle OT-systemer i Nye Veier AS.

Vegtilsynet registrerer at Nye Veier AS vurderer at selskapet i liten grad har ansvar for og styrer sikkerheten i OT-systemer selskapet benytter i sitt arbeid. Videre registrerer Vegtilsynet at selskapet vurderer at det er lav risiko for at mangelfull sikkerhetsstyring i digitale systemer i Nye Veier AS skulle medføre brudd på krav til konfidensialitet, integritet og tilgjengelighet til informasjon av betydning for sikkerheten i veginfrastrukturen.

Vegtilsynet stiller spørsmål ved hvor fullstendig denne vurderingen er, og vurderer at det som grunnlag for å konkludere på denne måten bør gjennomføres systematiske risikovurderinger/-analyser av alle OT-systemer som benyttes, hvilke sårbarheter som finnes i systemene og hvordan de kan være eksponert mot relevante trusler som cyberangrep, uautoriserte påloggingar mv. Dette vil være viktig for å kunne vurdere risikoen selskapet er eksponert for korrekt, og dermed kunne iverksette hensiktsmessige og effektive risikoreduserende tiltak.

Funn 1 – observasjon

Nye Veier AS bør gjennomføre systematiske risikovurderinger knyttet til digital sikkerhet som også dekker OT-systemer og OT-sikkerhet. Dette for å sikre et oppdatert og helhetlig bilde av trusler, sårbarheter og sikkerhetsmessige konsekvenser av uønskede hendelser.

Tilsynskriteriene 2-5: Oppfølging av gjennomførte risikokartlegginger

Bevis

Som det fremgår under tilsynskriterium 1, har tilsynspart etablert flere ulike styringsdokumenter knyttet til digital sikkerhet, ment å dekke både IT og OT. Dette omfatter blant annet overordnet styringsdokument for risikostyring, med underliggende støttende dokumenter for gjennomføring av risikovurdering, analyse og vurdering av identifiserte risikoer, iverksettelse av risikoreduserende tiltak og oppfølging og vurdering av effekten av iverksatte risikoreduserende tiltak. Disse styrende dokumentene blir lagt til grunn ved utførelse og oppfølging av risikokartlegginger av IT-systemene Nye Veier AS benytter. Dette innebærer at det for de ulike systemene også skal:

- Gjennomføres vurderinger av de risikoer som identifiseres (jf. TK2),
- Iverksettes risikoreduserende tiltak i tilfeller der den identifiserte risikoen vurderes som større enn hva virksomheten kan akseptere (jf. TK3),
- Gjennomføres evaluering av effekten av de tiltakene som iverksettes (jf. TK4), som grunnlag for justering/tilpasning dersom den ønskede effekten ikke oppnås (jf. TK5).

I tilsynsmøtet ble det fra tilsynspart vist til at når det gjelder vurderinger av identifiserte risikoer som gjelder IT-systemer, blir det gjort hvert kvartal i henhold til de etablerte styrende dokumentene. Der uakseptabel risiko avdekkes, er det etablert praksis at risikoreduserende tiltak iverksettes. Det vises til at dette i stor grad handler om veletablerte, anerkjente IT-sikkerhetstiltak som patching (oppdatere, rette feil og lukke sikkerhetshull i programvare), bruk av multifaktorautentisering (MFA), back-up av data, kjøp av døgnkontinuerlige sikkerhetsovervåknings-, trusseldeteksjons- og hendelseshåndteringstjenester (MDR), tilgang på incident response team (IRT) med 24 h support mv. Det ble i tilknytning til dette også vist til at det i forkant av alle planlagte endringer i etablerte systemer, gjennomføres risikovurderinger som grunnlag for å vurdere

om det er spesifikke tiltak som må gjennomføres for å ivareta sikkerheten når endringene gjøres.

Tilsynspart viser videre til at det ved anskaffelser av IT-systemer gjennomføres risikovurderinger av hva som er risikoene ved å implementere nytt system, og at det i tilknytning til dette arbeides med å identifisere tiltak for å håndtere og ved behov redusere risiko. Eksempel på slike tiltak kan være å stille krav i konkurranser om system hos leverandører for å sikre ivaretakelse av grunnprinsipper fra både ISO og NSM, slik at de tvinger leverandørene til å ivareta og dokumentere sikkerhet når nye systemer vurderes og anskaffes.

I tilsynsmøtet stilte Vegtilsynet spørsmål om hvordan det arbeides med å måle og evaluere om informasjonssikkerhetsarbeidet knyttet til de ulike systemer fungerer tilfredsstillende. Tilsynspart opplyste da om at:

- IT-sikkerhetsarbeidet i Nye Veier AS benchmarkes mot krav i standardene ISO27001 og ISO27002 gjennom jevnlige modenhetsanalyser, for å identifisere ev. svakheter og forbedringspunkter.
- Det er gjennomført cyber resilience-undersøkelser for å kartlegge hvor motstandsdyktige Nye Veier AS er mot f.eks. cyberangrep.

Tilsynspart vurderer at de selv har en høy grad av modenhet på IT-sikkerhet, og at Nye Veier AS på mange områder av ISO-standardene holder høy nok kvalitet til at man kunne ha blitt sertifisert etter standardene. Samtidig finnes andre områder der man vet at man ikke helt holder sertifiseringskvalitet, eksempelvis personellsikkerhet (on-/offboarding av personell). Økt modenhet på enkelte slike punkter kan imidlertid være krevende sett opp mot overholdelse av andre regulatoriske krav (GDPR og norsk personvernlovgivning).

Tilsvarende som for gjennomføring av risikokartlegginger (se TK1), viser tilsynet at det i liten grad arbeides helhetlig og systematisk med vurdering av identifiserte risikoer, iverksettelse av risikoreduserende tiltak og evaluering av iverksatte tiltak for de OT-systemer Nye Veier AS benytter og forholder seg til i sin drift. I tilsynsmøtet ble det imidlertid vist til at det har vært gjennomført noe testing av ivaretakelse av sikkerhet i OT-systemer ut mot leverandører, eksempelvis testing av hvilken informasjon man kan hente ut ved å koble seg inn i fysisk skap ute på anlegg.

Vurdering

Undersøkelsen har vist at tilsynspart sitt arbeid med å vurdere risiko, iverksette risikoreduserende tiltak og evaluere effekten av de risikoreduserende tiltakene, synes å være systematisk når det gjelder IT-systemer og IT-sikkerhet.

Tilsvarende som under tilsynskriterium 1, er det heller ikke for tilsynskriterium 2-5 presentert en helhetlig systematikk for å sikre at risikoer som knytter seg til OT-systemer blir vurdert, at risikoreduserende tiltak blir iverksatt der behov eller at effekten av eventuelle tiltak blir evaluert (og tiltak justert ved behov). Vegtilsynet mener Nye Veier AS bør sikre at den systematikken/prosessen som er etablert for dette når det gjelder IT, også utvides til å omfatte OT-systemer og OT-sikkerhet. Dette vil særlig være viktig fremover når integrasjonen mellom IT og OT blir større, og tilgang til og bruk av OT-systemer i større grad digitaliseres, og dermed eksponeres for digitale trusler og sårbarheter.

Funn 2 – observasjon

Nye Veier AS bør sikre helhetlig systematikk for vurdering av risiko, iverksettelse av risikoreduserende tiltak og evaluering av tiltakenes effekt som også dekker OT-systemer og OT-sikkerhet.

5. Konklusjon

Tilsynspart sitt arbeid for å identifisere, vurdere og håndtere risiko synes etter Vegtilsynet sin vurdering å være betryggende og systematiske for de IT-systemer som virksomheten benytter.

Når det gjelder sikkerheten knyttet til de OT-systemene som tilsynspart benytter i sitt arbeid, registrerer Vegtilsynet at tilsynspart vurderer at de i liten grad har ansvar for og styrer sikkerheten i disse systemene. Tilsynspart fremholder også at det er lav risiko for at mangelfull sikkerhetsstyring i digitale systemer i Nye Veier AS skulle medføre brudd på krav til konfidensialitet, integritet og tilgjengelighet til informasjon av betydning for sikkerheten i veginfrastrukturen. Vegtilsynet stiller spørsmål om i hvilken grad det ligger systematiske risikovurderinger /-analyser til grunn for disse vurderingene og dermed hvor robuste vurderingene faktiske er.

Vegtilsynet mener Nye Veier AS bør sikre at den systematikken som er etablert for identifisering, vurdering og håndtering av risiko når det gjelder IT, også utvides til å omfatte OT-systemer og OT-sikkerhet. Dette vil særlig være viktig fremover når integrasjonen mellom IT og OT forventes å bli større, og tilgang til og bruk av OT-systemer i større grad digitaliseres, og dermed eksponeres for digitale trusler og sårbarheter.