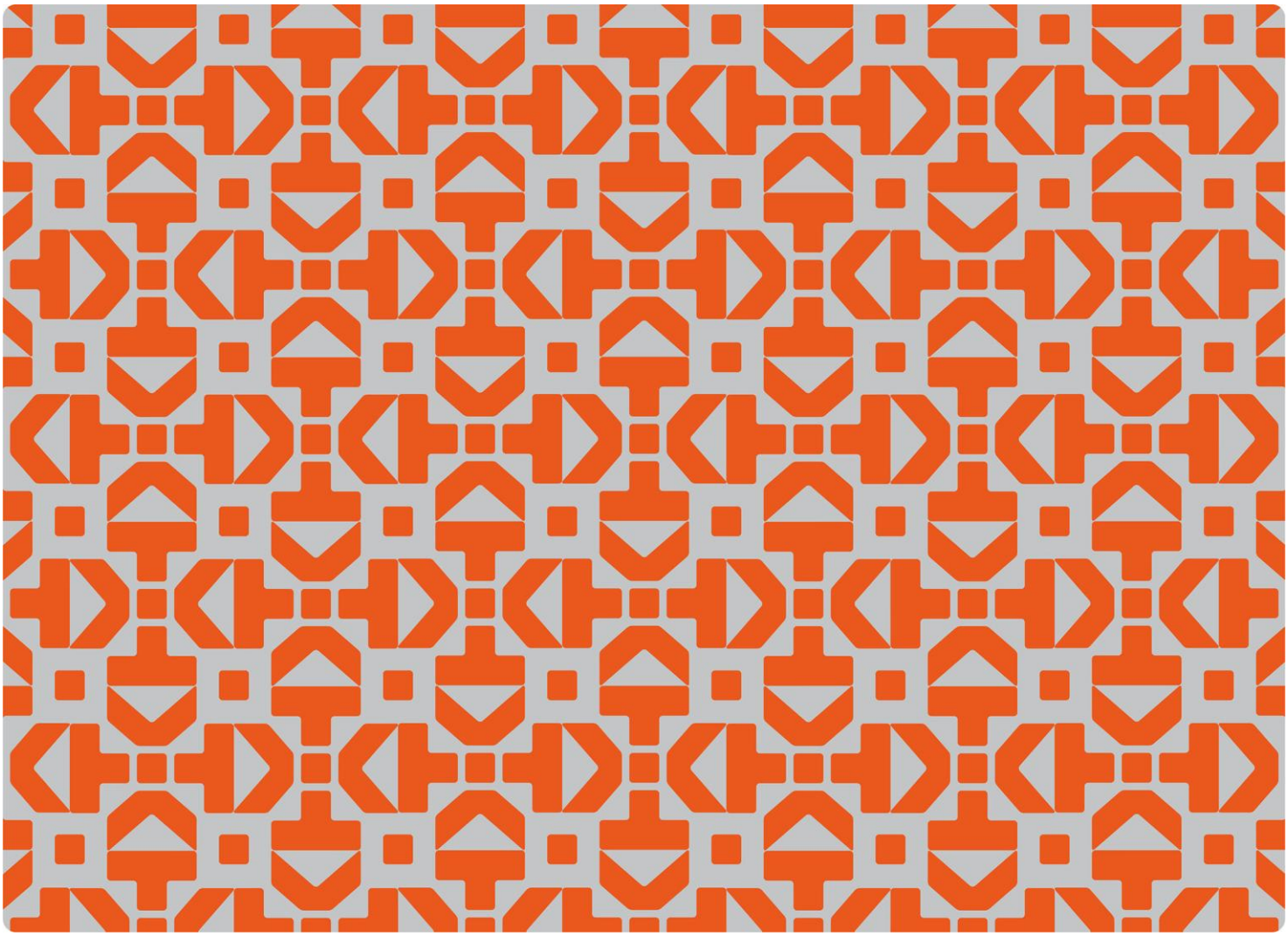
Direktoratet for høyere utdanning og kompetanse

Rapport nr. 09/2026

Tilstands- og risikovurdering 2026

Arbeidet med sikkerhet og beredskap i høyere utdanning og forskning



Tilstands- og risikovurdering 2026

Arbeidet med sikkerhet og beredskap i høyere utdanning og forskning

Redaktør:
Kristin Selvaag

Forfattere:
Agnethe Sidselrud
André Gaustad
Tommy Tranvik
Annette Grande Furset
Lars Bjønnes
Stine Rønnes

ISSN: 2703-9102

Innholdsfortegnelse

Sammendrag

Årets rapport viser at trusselbildet i universitets- og høyskolesektoren fortsatt er utfordrende. Nasjonale sikkerhetsmyndigheter peker for eksempel på at sektoren kan være et mål for utenlandsk etterretning. Det pekes også på risiko knyttet til digitale angrep, radikalisering og samarbeid med land som Kina, Russland og Iran. Også våre egne data om uønskede hendelser i sektoren indikerer at virksomhetene må forebygge, oppdage og håndtere mange ulike typer trusler og trusselaktører. Dette stiller høye krav til det lokale sikkerhetsarbeidet.

Sett i lys av trusselbildet, er det gledelig at sektoren arbeider mer systematisk med sikkerhet. Vi ser blant annet at informasjonssikkerhet er bedre samordnet med andre deler av sikkerhets- og beredskapsarbeidet, beredskapsplaner er ofte utarbeidet og overordnet ROS-analyse blir i stor grad gjennomført. Det er imidlertid svakheter i hvordan sikkerhet inngår i den øvrige virksomhetsstyringen. I deler av sektoren blir derfor sikkerhet i begrenset utstrekning prioritert i de viktigste styrings- og planleggingsprosessene. Det innebærer en fare for at sikkerhetsarbeidet verken får den oppmerksomheten eller de ressursene som kreves.

Årets kartlegging avdekker også områder hvor en del av virksomhetene har et tydelig forbedringspotensial. Det gjelder spesielt mangelfulle kontinuitetsplaner og varierende oppfølging av risikoreduserende tiltak etter ROS-analyser. Disse funnene betyr at sektoren fortsatt er sårbar for både kjente og mer avanserte trusler. Avhengighet av nøkkelpersoner og begrenset oppfølging av læringspunkter etter øvelser, bidrar til å gjøre deler av sektoren sårbar for uønskede hendelser og trusler fra nettkriminelle grupper eller statlige aktører. Særlig manglende oppfølging av risikoreduserende tiltak etter ROS-analyser og av læringspunkter etter øvelser, kan innebære at kontinuerlig forbedring i sikkerhetsarbeidet ikke oppnås i tilstrekkelig grad.

Rapporten anbefaler at sektoren iverksetter flere tiltak for å styrke sikkerhetsarbeidet, redusere sårbarheter og håndtere trusselbildet. For det første bør sektoren styrke koblingen mellom sikkerhet og virksomhetsstyringen, blant annet gjennom plan- og budsjettprosesser og ved å bruke etablerte styringsarenaer mer aktivt. Det anbefales også at tiltak etter overordnet ROS-analyse følges opp, at kontinuitetsplanverket forbedres, og at øvelser evalueres og eventuelle læringspunkter følges opp. Til slutt anbefaler vi at virksomhetene arbeider videre med sikkerhetstiltak for mobile dataenheter som benyttes til jobbformål.

Hovedfunn

Nedenfor presenterer vi de viktigste funnene fra kartleggingen av arbeidet med samfunnssikkerhet, nasjonal sikkerhet og informasjonssikkerhet i høyere utdanning og forskning i 2025.

Hendelser i sektoren

- De vanligste fysiske sikkerhetshendelsene i 2025, var trusler og vold uten alvorlige konsekvenser, og innbrudd og tyveri.
- De vanligste digitale sikkerhetshendelsene var nettfiske (phishing), bedrageriforsøk og datainnbrudd.
- Antallet brudd på personopplysningssikkerheten som ble varslet til Datatilsynet, økte noe i 2025.

Styring og samordning av sikkerhetsarbeidet

- 21 av 28 virksomheter oppga å ha etablert dokumenterte styringssystemer for sikkerhet, en økning på 5 sammenliknet med 2024.
- Samordningen mellom styringssystemer for sikkerhet og ledelsessystemer for informasjonssikkerhet er forbedret.
- 15 av 28 virksomheter opplyste om at sikkerhetsarbeidet er mangelfullt inkludert i den øvrige virksomhetsstyringen.

ROS-analyser og risikoreduserende tiltak

- 22 virksomheter har utarbeidet en overordnet ROS-analyse. De resterende 6 har delvis utarbeidet en slik analyse.
- 15 virksomheter oppga at iverksatte tiltak har hatt ønsket effekt på sikkerheten. 13 virksomheter mente at effekten av tiltakene enten hadde vært noe begrenset eller liten.
- 11 av 28 oppga å ha mangler i tiltaksplaner for oppfølging av risikoer med middels og høy risiko.

Beredskapsplaner og -øvelser

- 22 virksomheter oppga å ha utarbeidet beredskapsplaner. De siste 6 virksomhetene hadde delvis utarbeidet slike planer.
- 10 virksomheter oppga å ha utarbeidet kontinuitetsplaner for å opprettholde kritiske funksjoner ved høyt personellfravær. Hos de øvrige 18 virksomhetene manglet dette helt eller delvis.
- 12 virksomheter oppga å ha utarbeidet kontinuitetsplaner for å opprettholde kritiske IT-funksjoner ved alvorlige digitale sikkerhetshendelser. Hos de øvrige 16 virksomhetene manglet dette helt eller delvis.
- Virksomhetene gjennomfører øvelser. Skrivebordøvelser er den mest utbredte typen øvelsestypen.

Sårbarhetsstyring hos tre utvalgte virksomheter

Alle de tre virksomhetene arbeider godt med sikkerhetsoppdateringer og reduksjon av sårbarheter i sine digitale systemer. Følgende forbedringspunkter ble avdekket:

- Ytterligere tiltak for mobile dataenheter som brukes til jobbformål, spesielt private enheter hvor sikkerhetstiltak ikke kan kreves.
- Videre arbeid med kontroll på hvilke nettlesere som brukes, og særlig bruk av tillegg til nettlesere.

Risikovurdering på sektornivå og anbefalinger

På bakgrunn av kartleggingen har vi identifisert og vurdert risiko for 7 ulike risikoscenarioer (uønskede hendelser) i sektoren. Vi har vurdert disse slik:

- Høy risiko: Studenter eller ansatte opplever trusler, trakassering og psykososial utrygghet.
- Middels risiko: Alvorlige digitale angrep som fører til svikt i viktige tjenester; brudd på personopplysningssikkerheten som skyldes menneskelige eller tekniske feil og uhell; PLIVO på campus; innsiderisiko og misbruk av tilganger i kritiske systemer som medfører tap av skjermingsverdig informasjon.
- Lav risiko: Langvarig svikt i felles IKT-tjenester som fører til bortfall av tjenestene i hele eller deler av sektoren; svikt i kritisk infrastruktur og svikt i strømforsyning som innebærer avbrudd i kjerneoppgaver (undervisning, forskning, osv.).

I det videre sikkerhetsarbeidet bør sektoren fokusere særlig på risikoscenarioer med høy og middels risiko.

1 Innledning

Årets tilstands- og risikovurdering oppsummerer hovedfunn fra HK-dir sin kartlegging av arbeidet med samfunnssikkerhet, nasjonal sikkerhet og informasjonssikkerhet i høyere utdanning og forskning. Kartleggingen omfatter 28 universiteter, høyskoler og andre forvaltningsorganer og selskaper underlagt Kunnskapsdepartementet.[1]

Kartleggingen tar utgangspunkt i kravene som departementet stiller til virksomhetene i «Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor» og i «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».

Datainnsamlingen som ligger til grunn for funn og konklusjoner i denne rapporten foregikk i perioden oktober 2025 til januar 2026.

1.1 Om gjennomføringen

For å få en samlet oversikt over sikkerhetsarbeidet i sektoren, sendte vi et spørreskjema til og mottok svar fra samtlige 28 virksomheter. Spørsmålene handlet om hvordan virksomhetene etterlever kravene i styringsdokumentet for sikkerhet og beredskap og i policyen for informasjonssikkerhet og personvern. I tillegg ble det stilt spørsmål om blant annet sikkerhetshendelser, sårbarheter og iverksatte sikkerhetstiltak.

Videre har vi gjennomført intervjuer med ni utvalgte virksomheter.[2] Intervjuene ble avholdt i november 2025, og formålet var å fremskaffe supplerende informasjon om forhold som det ble spurt om i spørreskjemaet.

I tillegg ble det innhentet utfyllende informasjon om det digitale sikkerhetsarbeidet i sektoren. Det skjedde gjennom stedlige besøk hos tre universiteter og høyskoler. Temaet for årets stedlige besøk var sårbarhetsstyring, det vil si hvordan institusjonene jobber med sikkerhetsoppdateringer av programvare, og hva de gjør for å redusere angrepsflaten på sine IT-systemer. Vi gjennomgikk også hvilke tekniske tiltak som er etablert for å håndtere digitale trusler og skadevare.

---

[1] Dette er de 21 statlige universitetene og høyskolene, og følgende forvaltningsorganer og selskaper: Norges forskningsråd; Nasjonalt organ for kvalitet i utdanningen; Sikt – kunnskapssektorens tjenesteleverandør; Norsk utenrikspolitisk institutt; Simula Research AS; De nasjonale forskningsetiske komiteene og Universitetssenteret på Svalbard.

[2] Intervjuene ble gjennomført på Microsoft Teams og varte i ca. 1,5 timer.

Til slutt ble det avholdt møter med cybersikkerhetssenteret hos Sikt og med BOTT-universitetene. I møtene ble det innhentet data om digitale sikkerhetshendelser og det digitale trusselbildet i sektoren.

Vedlegg 1 redegjør for arbeidet med datainnsamling og datagrunnlaget som rapporten baserer seg på.

1.2 Bruk av kunstig intelligens

Vi har benyttet kunstig intelligens – Microsoft Copilot – som støtteverktøy i arbeidet med rapporten. KI ble særlig brukt til å strukturere data fra intervjuer og spørreskjema sett opp mot kravene i styringsdokument for sikkerhet og beredskap og i policy for informasjonssikkerhet og personvern. Hensikten var å fange opp relevante opplysninger eller sammenhenger som vi kunne ha oversett. Alle KI-analyser ble kvalitetssikret manuelt.

1.3 Kapitteloversikt

I kapittel 2 drøfter vi trusselbildet i sektoren basert på vurderinger fra EOS-tjenestene, og våre egne data om sikkerhetshendelser i sektoren.

I kapittel 3–5 drøfter vi resultatene fra spørreundersøkelsen, supplert med data fra intervjuene. Her gir vi en samlet oversikt over sektorens etterlevelse av krav til sikkerhetsarbeidet. Vi drøfter ulike krav i hvert kapittel: styring og samordning av sikkerhetsarbeidet i kapittel 3, ROS-analyser og tiltak etter ROS i kapittel 4, og beredskapsplaner og -øvelser i kapittel 5.

I kapittel 6 oppsummerer vi viktige funn fra de stedlige besøkene, det vil si hvordan utvalgte virksomheter jobber med sårbarhetsstyring.

I kapittel 7 vurderer vi risikoen for sikkerhetshendelser på sektornivå. Vurderingene baserer seg på funn og konklusjoner i de tidligere kapitlene.

I kapittel 8 skisserer vi anbefalinger til tiltak for virksomhetene i sektoren. Formålet med disse er å redusere risikoen for alvorlige hendelser vurdert i kapittel 7, og å styrke etterlevelsen av departementets krav til sikkerhetsarbeidet.

2 Trusselbildet i sektoren

EOS-tjenestene peker på at det generelle trusselbildet fortsatt er krevende, særlig på grunn av etterretningsaktivitet, cyberoperasjoner og påvirkningsforsøk fra stater som Russland, Kina og Iran. Tjenestene mener også at høyere utdanning og forskning er attraktive etterretningsmål, blant annet på grunn av tilgang til teknologi, kompetanse og internasjonalt samarbeid. EOS-tjenestene er i tillegg bekymret for terror, ekstrem vold og radikalisering. Dette er trusler som har relevans i vår sektor.

De vanligste fysiske sikkerhetshendelsene i høyere utdanning og forskning i 2025, var trusler og vold uten alvorlige konsekvenser, og innbrudd og tyveri. De vanligste digitale sikkerhetshendelsene var nettfiske (phishing), bedrageriforsøk og datainnbrudd. Hendelsene hadde begrensede eller ingen skadevirkninger. Menneskelige feil eller uhell var den vanligste årsaken til slike hendelser.

Antallet brudd på personopplysningssikkerheten som ble varslet til Datatilsynet har økt noe i 2025. Økningen skyldtes i hovedsak feil hos eksterne IT-leverandører.

Samlet sett er vår vurdering at trusselbildet i sektoren fortsatt er komplekst, spesielt fordi sektoren må forebygge og håndtere mange ulike typer trusler, både fysiske og digitale. Samtidig kan sikkerhetshendelser skyldes alt fra manglende digital kompetanse hos ansatte til nettkriminell aktivitet og statlig etterretning. Dette stiller høye krav til det lokale sikkerhetsarbeidet.

2.1 Det generelle trusselbildet

Politiets sikkerhetstjeneste (PST) mener at utenlandske etterretningstjenester, spesielt fra Russland, Kina og Iran, kan forsøke å rekruttere forskere og fagpersoner innenfor relevante fagmiljøer. Rekrutteringsforsøk kan skje både i det fysiske og digitale rom, for eksempel på seminarer, konferanser og andre møteplasser (PST 2026, s. 25).

Land som Kina og Iran kan tilegne seg teknologi ved å skaffe seg tilgang til norske forsknings- og utviklingsmiljøer. PST forventer at dette kan skje gjennom gjesteforelesningsordninger og tilgang til spesialisert forskningsinfrastruktur, samt ved misbruk av sensitiv informasjon delt i internasjonale forskningssamarbeid. Etterretningstjenesten (E-tjenesten) peker på at norskprodusert maritim teknologi og kommunikasjons- og navigasjonsteknologi er attraktivt for Russland, Kina og Iran (E-tjenesten 2026, s. 49).

Nordområdene er av særlig interesse for Russland og Kina (PST 2026, s. 13–14), og kinesiske aktører forventes å styrke sin tilstedeværelse på Svalbard (E-tjenesten 2026,

s. 15). PST mener at for Kina er forsknings- og utdanningssektoren i nordområdene en av få arenaer som er åpne for kultivering og samarbeid. Fremstøtene forventes utført av kinesiske forskningsinstitusjoner og personer som opptrer på vegne av kinesiske myndigheter (PST 2026, s. 19). Fagmiljøer i høyere utdanning og forskning som har spesialisert seg på nordområdespørsmål er av interesse for russisk etterretning.

Videre forventer PST at autoritære stater vil gjennomføre påvirkningsoperasjoner i Norge i 2026, som også inkluderer proxyaktører[3] (PST 2026, s. 26). De siste årene har disse statene blant annet gjort forsøk på påvirkning og overvåkning av diaspora (E-tjenesten 2026, s. 37–39). Det kan bety at studenter eller ansatte i høyere utdanning og forskning med bakgrunn fra Russland, Kina eller Iran er mulige mål for slik påvirkning og overvåkning.

Kunstig intelligens

I rapportene fra EOS-tjenestene blir kunstig intelligens løftet frem som en særskilt trussel.

PST forventer at statlige cyberaktører vil gjennomføre cyberoperasjoner i 2026, hvor KI-verktøy benyttes. Det kan skje ved at KI gjør sosial manipulasjon, slik som nettfiske, mer overbevisende og målrettet, men også ved at KI-verktøy benyttes i alle faser av et datainnbrudd. Kunstig intelligens kan i tillegg brukes til å fremstille bilder, videoer, tekst eller lyd som underbygger falske identiteter (PST 2026, s. 22).

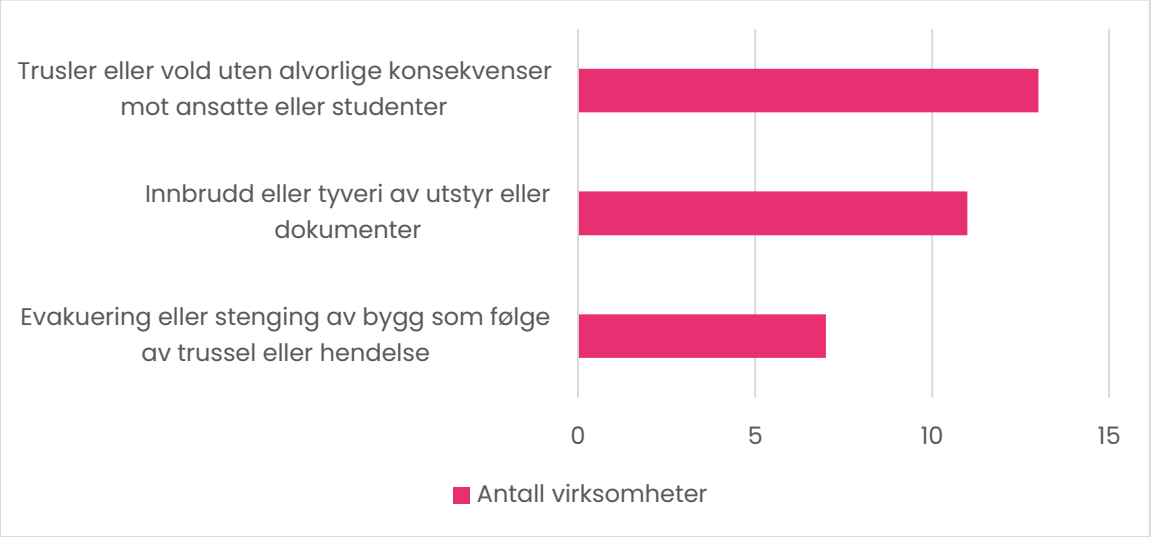
EOS-tjenestene vurderer også terrortrusler og risiko for politisk motivert vold. PST er for eksempel bekymret for at enkeltpersoner radikaliseres ved å bli eksponert for ekstrem ideologi, voldsmateriale eller et miljø som ser på vold som en legitim aksjonsform. Eventuelle personlige sårbarheter, som psykisk uhelse, utenforskap eller livskriser, kan medvirke til dette. PST peker videre på at personer som radikaliseres finner inspirasjon i voldsforherligende ideer uten en tydelig ideologi, blant annet gjennom nettfora.

Selv om vurderingene av ekstrem voldsutøvelse ikke gjelder spesielt for høyere utdanning og forskning, er dette likevel forhold som også universiteter og høyskoler bør være oppmerksomme på.

[3] Proxyaktører er personer eller organisasjoner uten formell tilknytning til etterretnings- og sikkerhetstjenester eller andre myndighetsorganer, men som utfører aktivitet på oppdrag fra, eller til støtte for, sine lands myndigheter. Aktiviteten kan være politisk, ideologisk eller økonomisk motivert (PST 2026, s. 13).

2.2 Fysiske sikkerhetshendelser

I årets kartlegging har vi fulgt opp PSTs vurderinger av fysiske sikkerhetshendelser, inkludert volds- og trusselhendelser. Vi spurte derfor virksomhetene om hvilke slike hendelser de hadde registrert.



Figur 1: De vanligste fysiske sikkerhetshendelsene i 2025 (N=16)

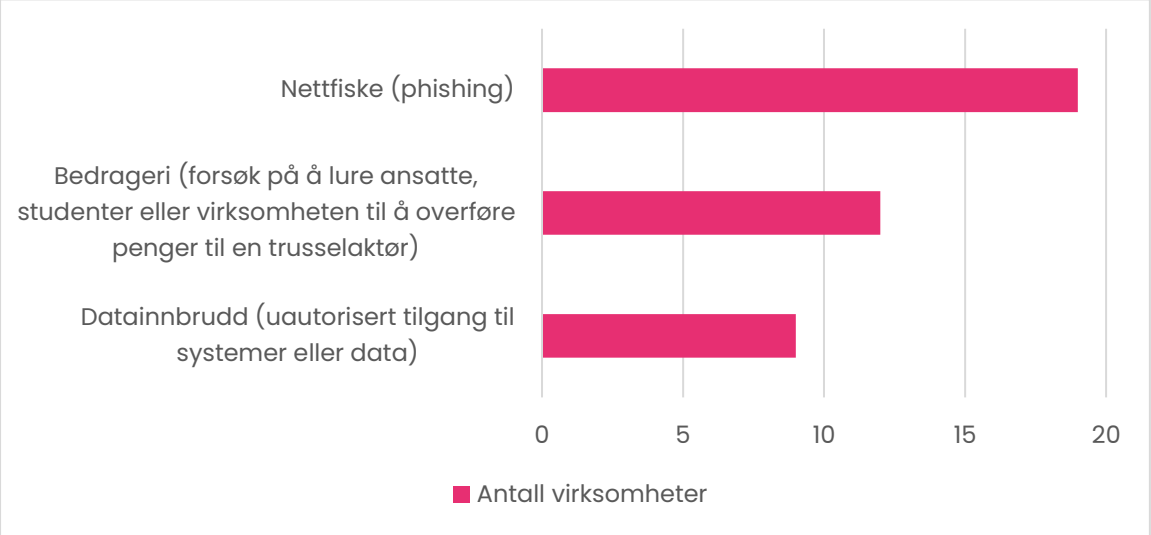
16 virksomheter rapporterte om fysiske sikkerhetshendelser i 2025. Figur 1 viser de 3 vanligste hendelsestypene. Den vanligste hendelsestypen var trusler og vold mot studenter eller ansatte, men uten alvorlige konsekvenser. Eksempler på slike hendelser var blant annet truende atferd og bæring av kniv på campus, personforfølgelse (stalking) av ansatte/studenter og hendelser knyttet til psykisk uhelse.

Den nest vanligste hendelsestypen var innbrudd eller tyveri av utstyr eller dokumenter. Det handlet typisk om skadeverk og tyveri av datamaskiner, og tilfeller hvor ansatte ble frastjålet PC/telefon på reise. Kun én virksomhet rapporterte om at tyveri av utstyr førte til mistanke om at data var kommet på avveie.

7 virksomheter rapporterte om hendelser som førte til evakuering eller stenging av bygg. Det ble blant annet opplyst om evakuering grunnet «kjemikaliehendelser» og «granatkasting» i nærhet til campus. Det ble også rapporterte om manglende tilgjengelighet til bygninger på grunn av demonstrasjon på utsiden.

2.3 Digitale sikkerhetshendelser

22 virksomheter opplyste å ha registrert digitale sikkerhetshendelser i 2025. Figur 2 viser de 3 vanligste hendelsestypene som disse virksomhetene rapporterte om.



Figur 2: De vanligste digitale sikkerhetshendelsene i 2025 (N=22)

Den vanligste hendelsestypen i 2025 var nettfiske (phishing). Enkelte virksomheter opplyste for eksempel at nettfiske var vanlig eller pågikk kontinuerlig, men at forsøkene ikke hadde lyktes og derfor heller ikke hadde fått nevneverdige konsekvenser. To virksomheter rapporterte om forsøk som hadde lyktes, men hvor rask håndtering forhindret alvorlige konsekvenser.

Kun én av virksomhetene som var utsatt for forsøk på bedrageri rapporterte om økonomisk tap på grunn av dette. Når det gjaldt datainnbrudd, opplyste 9 virksomheter om dette. Den alvorligste hendelsen handlet om utnyttelse av sikkerhetshull i tjeneste hos ekstern leverandør.

Virksomhetene ble i tillegg bedt om å oppgi årsaker til de uønskede hendelsene. 19 virksomheter svarte at uønskede hendelser skyldes menneskelige feil eller uhell. 11 virksomheter rapporterte teknisk svikt eller feil oppsett av IT-systemer (feilkonfigurasjon) som årsak. Manglende kompetanse/opplæring og sårbarheter/feil hos IT-leverandører ble angitt som årsak av 10 virksomheter.

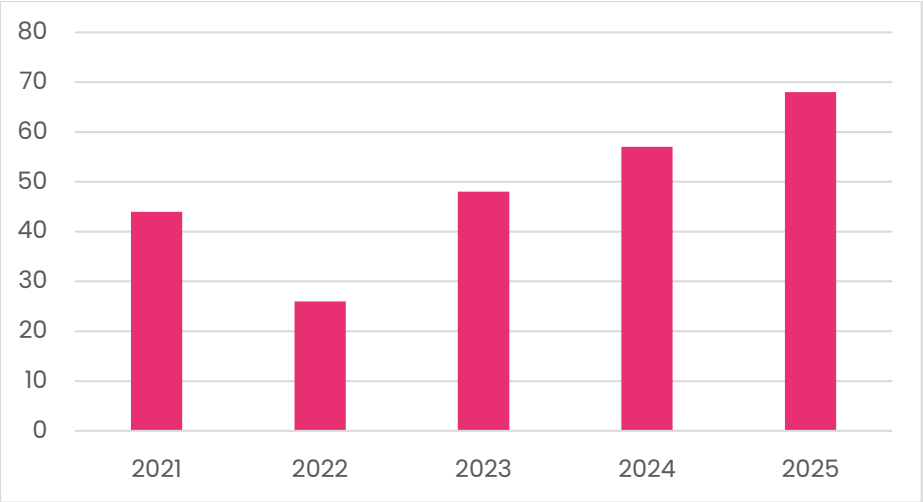
Digitale sikkerhetshendelser registrert hos Sikt

Cybersikkerhetssenteret for forskning og utdanning (eduCSC) hos Sikt rapporterte om en liten økning i antall digitale sikkerhetshendelser og sårbarheter i 2025.

Den største andelen av hendelser registrert hos eduCSC gjaldt sårbare datasystemer, hvor det er en marginal økning fra i fjor. Deretter kommer kompromitterte brukerkontoer og datamaskiner, som også har økt noe i forhold til 2024.

2.4 Brudd på personopplysningssikkerheten

I kartleggingen rapporterte virksomhetene om varsling til Datatilsynet ved brudd på personopplysningssikkerheten. 21 virksomheter sendte til sammen 68 varsler til Datatilsynet om slike brudd i 2025. Figur 3 viser at det har vært en jevn økning i antall varslinger til Datatilsynet de siste 4 årene.



Figur 3: Saker meldt til Datatilsynet, 2019–2025

Virksomhetene oppga også årsak til hendelser som ble varslet Datatilsynet. En relativt stor andel kan tilskrives feil på fellestjenester i sektoren. Også menneskelige feil eller uhell ble angitt som viktige årsaker til slike hendelser.

Flere virksomheter mente at ansatte fortsatt rapporterer for få sikkerhetsbrudd, og at det derfor er tenkelig at flere hendelser burde vært varslet til Datatilsynet. Manglende kompetanse om hva som skal rapporteres og liten kjennskap til rutiner for rapportering, ble pekt på som mulige årsaker.

3 Styring og samordning av sikkerhetsarbeidet

Trusselbildet i sektoren forutsetter at virksomhetene jobber systematisk med å forebygge, oppdage og håndtere truslene. Departementet krever derfor at virksomhetene etablerer et styringssystem for sikkerhet. I tillegg kreves det at styringssystemet for sikkerhet samordnes med ledelsessystemet for informasjonssikkerhet og med den øvrige virksomhetsstyringen. Styringssystemet skal dokumenteres, gjennomgås årlig og revideres ved behov.

Årets kartlegging viser en positiv utvikling når det gjelder etablering av dokumenterte styringssystemer for sikkerhet. Vi ser dessuten en viss positiv utvikling når det gjelder graden av samordning mellom styringssystemer for sikkerhet og ledelsessystemer for informasjonssikkerhet.

Videre ser vi at resultatene er svakere med hensyn til sikkerhetsarbeidets plass i den øvrige virksomhetsstyringen, med svært liten fremgang siden 2024. I intervjuene pekes det på mulige årsaker, spesielt at denne formen for samordning kan være et komplekst og tidkrevende arbeid. Virksomhetene som opplever disse utfordringene bør vurdere hvordan etablerte prosesser – ledelsens gjennomgang, rapporteringer til styret og arbeidet med årsrapporter – kan benyttes for å integrere sikkerhetsarbeidet sterkere i virksomhetsstyringen.

3.1 Styringssystem for sikkerhet – status for etablering

Figur 4: Etablering av dokumentert styringssystem for sikkerhet – endring fra 2024 til 2025 (N=28)

Også i 2025 ble virksomhetene spurt om de hadde et ferdig etablert og dokumentert styringssystem for sikkerhet. Som resultatene i figur 4 viser er kravet om etablering av et dokumentert styringssystem bedre ivaretatt i sektoren i 2025 enn i 2024. Det var 21 virksomheter som svarte at de i stor eller svært stor grad har dette på plass, en økning med 5 virksomheter fra fjorårets kartlegging.

De 9 virksomhetene vi intervjuet ble spurt om hvordan styringssystemet er utformet og forankret i ledelsen. Flere av dem opplyste om at styringssystemet er godt forankret i toppledelsen. Det er også vanlig at styringssystemet er behandlet og godkjent av universitets- eller høyskolestyret.

3.2 Samordning med ledelsessystemet for informasjonssikkerhet

Virksomhetene ble spurt om de hadde samordnet styringssystemet for sikkerhet med ledelsessystemet for informasjonssikkerhet.[4] Slik samordning styrker systematikken i det samlede sikkerhetsarbeidet.

Figur 5: Samordning av styringssystemet for sikkerhet og ledelsessystemet for informasjonssikkerhet (N=28)

[4] Forskjellen mellom systemene handler hovedsakelig om formål og omfang. Styringssystemet for sikkerhet skal omfatte alle aktiviteter med betydning for forebyggende sikkerhetsarbeid. Ledelsessystemet for informasjonssikkerhet har et snevrere omfang og formål ved at det begrenser seg til styring og kontroll med tilgjengeligheten, integriteten og konfidensialiteten til informasjon. Se Etabler styringssystem for sikkerhet - Nasjonal sikkerhetsmyndighet. Se også Internkontroll/ styringssystem/ ledelsessystem for informasjonssikkerhet | Digdir.

Som figuren viser var det 21 virksomheter som svarte at styringssystemet for sikkerhet i stor eller svært stor grad er samordnet med ledelsessystemet for informasjonssikkerhet. Dette er 6 flere enn i 2024.

Flere av virksomhetene vi intervjuet oppga at samordningen skjedde ved at styringssystemet for sikkerhet ble utformet basert på strukturen i ledelsessystemet for informasjonssikkerhet. Det innebærer for eksempel at eksisterende policyer for informasjonssikkerhet bygges ut til å bli et felles styringssystem som også dekker de øvrige sikkerhetsområdene.

Ledelsens gjennomgang og systemrevisjon

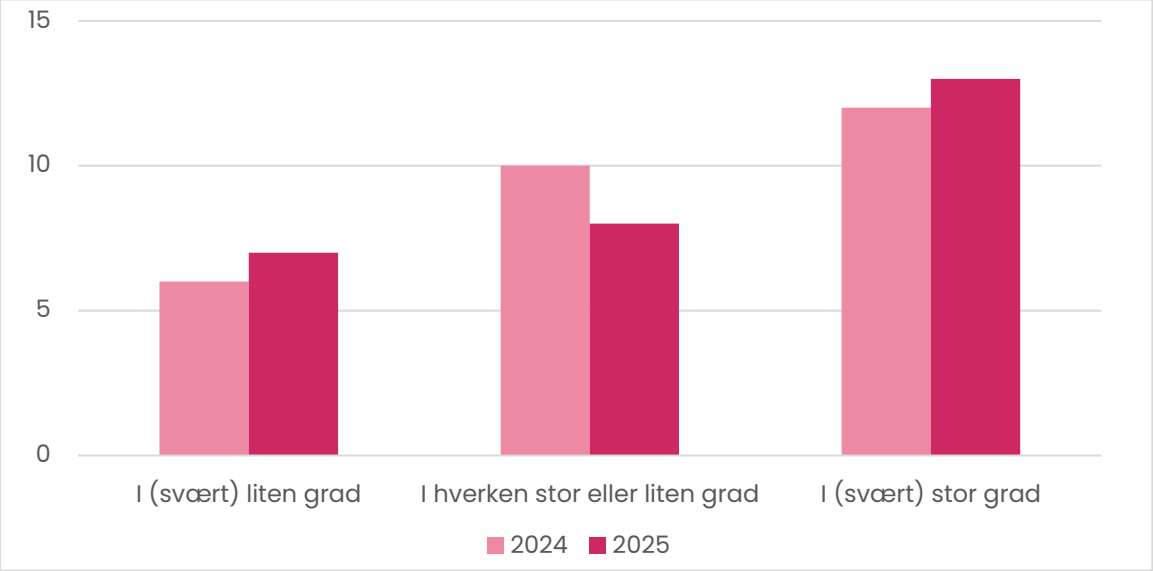
I intervjuene fremkom det at flere av virksomhetene følger opp styringssystemet for sikkerhet gjennom ledelsens gjennomgang. To virksomheter opplyste om at de bruker ledelsens gjennomgang til å revidere og oppdatere styringssystemet.

Også ved en tredje virksomhet har ledelsen vedtatt at sikkerhetsdokumentene skal gjennomgås jevnlig (hvert kvartal). Sikkerhetsteamet i virksomheten utfører det praktiske arbeidet, mens ledergruppen får full gjennomgang av og vedtar endringer i styringssystemet.

To virksomheter opplyste om at revisjonsrutiner er beskrevet i styringssystemet for sikkerhet, og at de jobber videre med å forbedre prosesser for styring og internkontroll på sikkerhetsområdet.

3.3 Samordning med den øvrige virksomhetsstyringen

Virksomhetens ledelse har ansvar for sikkerhetsarbeidet, og arbeidet skal inngå i den øvrige virksomhetsstyringen, for eksempel plan- og budsjettprosessen. Derfor ble virksomhetene spurt om styringen av arbeidet med samfunnssikkerhet, nasjonal sikkerhet og informasjonssikkerhet var samordnet med andre styringsprosesser internt. Svarene fremgår av figur 6.



Figur 6: Samordning av sikkerhetsstyringen med den øvrige virksomhetsstyringen (N=28)

13 virksomheter oppga at styringssystemet for sikkerhet er godt eller svært godt samordnet med andre styringsprosesser i virksomhetene, en beskjeden forbedring siden 2024. Flertallet – 15 av 28 virksomheter – oppga imidlertid at styringssystemet for sikkerhet ikke er samordnet med den øvrige virksomhetsstyringen på en god nok måte, eller at samordningen er fraværende.

3.4 Utfordringer i arbeidet med sikkerhetsstyring

Resultatene for samordning av styringssystemet for sikkerhet med den øvrige virksomhetsstyringen avviker noe fra de andre resultatene i dette kapitlet. Vi ser en viss forbedring både når det gjelder etablering av dokumentert styringssystem for sikkerhet, og samordning med ledelsessystemet for informasjonssikkerhet. Forbedringene er langt mer moderate med hensyn til sikkerhetsarbeidets plass i den øvrige virksomhetsstyringen. Det kan tyde på at store deler av sektoren fortsatt har utfordringer med å sørge for at sikkerhet ses i sammenheng med, og vurderes som en del av, virksomhetenes øvrige oppgaver.

I intervjuene opplyste flere av virksomhetene om at de har en god forståelse for hva samordning av sikkerhetsstyring og den øvrige virksomhetsstyringen innebærer. Noen virksomheter pekte imidlertid på at det finnes utfordringer som må løses før dette kan skje. Det ble blant annet vist til at ulike administrative områder har sine egne styrings- og kvalitetssystemer (studieadministrasjon, eiendomsforvaltning, IT-drift, osv.). Flere forskjellige styrings- og kvalitetssystemer bidrar til å komplisere arbeidet med å integrere sikkerhetsstyringen i den øvrige virksomhetsstyringen.

I virksomheter som opplever å ha lyktes med å samordne arbeidet på tvers av sikkerhetsområder ser det ut til å være enklere å inkludere sikkerhetsstyring i den øvrige virksomhetsstyringen.

Det kan også virke som det er noe enklere for mindre virksomheter å inkludere sikkerhetsstyring i den øvrige virksomhetsstyringen enn hva det er for de større virksomhetene.

4 ROS-analyser og risikoreduserende tiltak

Risikostyring har en sentral plass i sikkerhetsarbeidet. Det er også krav som følger av departementets styringsdokument for sikkerhet og beredskap, hvor det blant annet forventes at virksomhetene vurderer risiko for hendelser som kan true deres verdier (helhetlig og overordnet ROS).

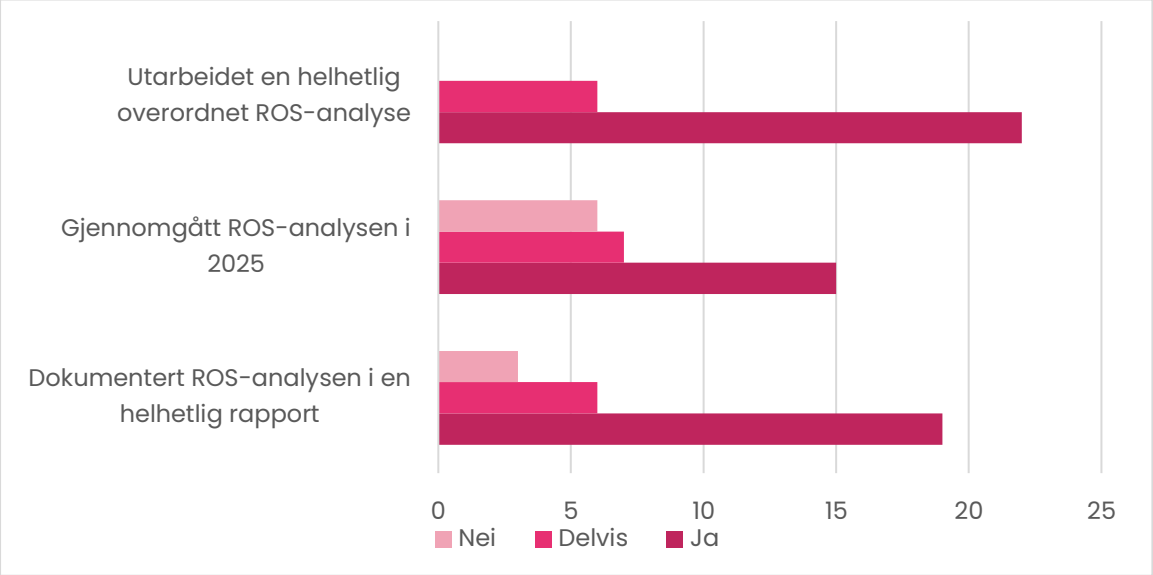
Resultatene fra kartleggingen tyder på at virksomhetene i sektoren arbeider systematisk med risikovurderinger. Ingen av dem oppga at de mangler en helhetlig og overordnet ROS-analyse. Det var imidlertid mangler i forhold til kravene i styringsdokumentet om å ha samlet analysen i en helhetlig rapport, og å ha gjennomgått ROS-analysen i 2025.

Kartleggingen viser at tiltak for å redusere risiko blir iverksatt hos de fleste virksomhetene. Likevel er det enkelte virksomheter som iverksetter tiltak uten først å ha utarbeidet en tiltaksplan for hendelser med høy eller middels risiko. Flere virksomheter jobber med oppfølging av tiltak, men det fremstår som mer usikkert om tiltakene har ønsket effekt.

I arbeidet med ROS-analyser har virksomhetene identifisert avhengighet av enkeltpersoner/nøkkelpersoner som den vanligste sårbarheten i sikkerhetsarbeidet. Samtidig viser karleggingen at de største virksomhetene har avsatt flere personellressurser (årsverk) til dette arbeidet enn de mindre. Det kan stilles spørsmålstegn ved om de små ressursoverslagene hos mange av de mindre virksomhetene, er tilstrekkelige til å videreutvikle sikkerhetsarbeidet vesentlig.

4.1 Overordnet og helhetlig ROS

En viktig del av risikostyringen er at virksomhetene har utarbeidet en helhetlig og overordnet ROS-analyse. Figur 7 viser status for arbeidet med ROS-analyser i 2025.



Figur 7: Gjennomført, gjennomgått og dokumentert ROS-analyse (N=28)

Det store flertallet av virksomhetene rapporterer at de har utarbeidet en overordnet ROS-analyse. De resterende 6 virksomhetene opplyser at de delvis har gjort det. Drøyt halvparten av virksomhetene (15) oppgir at ROS-analysen er gjennomgått i 2025.

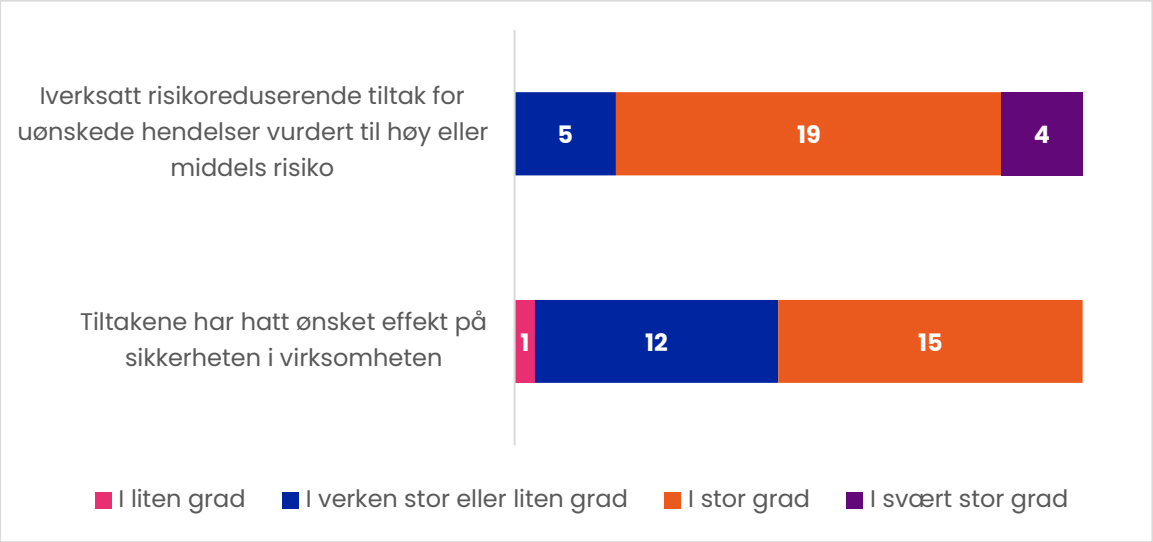
Når det gjelder å dokumentere ROS-analysen i en helhetlig rapport, var det 3 virksomheter som manglet dette, mens 6 virksomheter mente at de delvis oppfylte kravet. 19 virksomheter oppga at analysen er dokumentert på riktig måte.

I intervjudelen av kartleggingen fikk vi ytterligere innsikt i deres arbeid med overordnet ROS. Flere virksomheter oppga å bruke risiko- og trusselvurderinger fra sentrale aktører som kilde, for eksempel nasjonale sikkerhetsmyndigheter, i tillegg til innspill fra egne fagmiljøer. Hos enkelte virksomheter kunne ROS-analysen omfatte opp til 15 scenarioer. Det handlet blant annet om alvorlige arbeidsulykker, ulovlig kunnskapsoverføring, cyberangrep, hatefulle ytringer, trusler og vold, og ekstremvær.

4.2 Tiltaksplaner og tiltaksgjennomføring

Virksomhetene ble videre spurt om de har utarbeidet planer for å redusere risikoen for hendelser som, ifølge overordnet ROS, har middels eller høy risiko. På dette svarte 17 virksomheter at planer for reduksjon av risiko var utarbeidet, mens 11 virksomheter svarte at dette ikke eller bare delvis var gjort.

Vi spurte også virksomhetene om risikoreduserende tiltak for hendelser med høy eller middels risiko faktisk ble iverksatt og om tiltakene hadde ønsket effekt. Svarene fremgår av figur 8.



Figur 8: Gjennomføring av tiltak og ønsket effekt (N=28)

Her ser vi at 23 virksomheter oppgir å ha iverksatt risikoreduserende tiltak. De resterende 5 virksomhetene oppgir at dette i noen grad er gjort. Det er derfor flere virksomheter som har iverksatt tiltak enn som har laget planer for hvilke tiltak det er nødvendig å iverksette (11 virksomheter svarte at planverket var mangelfullt, se ovenfor). Dette kan indikere manglende systematikk i måten ROS-analyser følges opp på hos mange virksomheter. Samtidig antyder det at tiltaksaktiviteten er større enn hva planverket hos enkelte av virksomhetene gir inntrykk av.

På spørsmål om tiltakene har hatt ønsket effekt på sikkerheten, var det 15 som oppga at dette stemmer i stor grad, mens 12 oppga i hverken stor eller liten grad. 1 virksomhet oppga at dette stemmer i liten grad. Svarene antyder at selv om tiltaksaktiviteten er stor, mente nesten halvparten av virksomhetene at det er en viss usikkerhet knyttet til om tiltakene bidrar til å redusere risiko. Det kan bety at effekten av tiltak enten ikke måles eller er vanskelig å måle, eventuelt at det velges tiltak som er lite egnet til å redusere den aktuelle risikoen.

I intervjuene oppga likevel flere av virksomhetene at de har bevissthet om effekter av tiltak, for eksempel ved at tiltak utformes med tanke på at effekt skal kunne måles. Andre virksomheter oppga at ansvarlige for oppfølging av tiltak er identifisert og at det rapporteres jevnlig på status for gjennomføring.

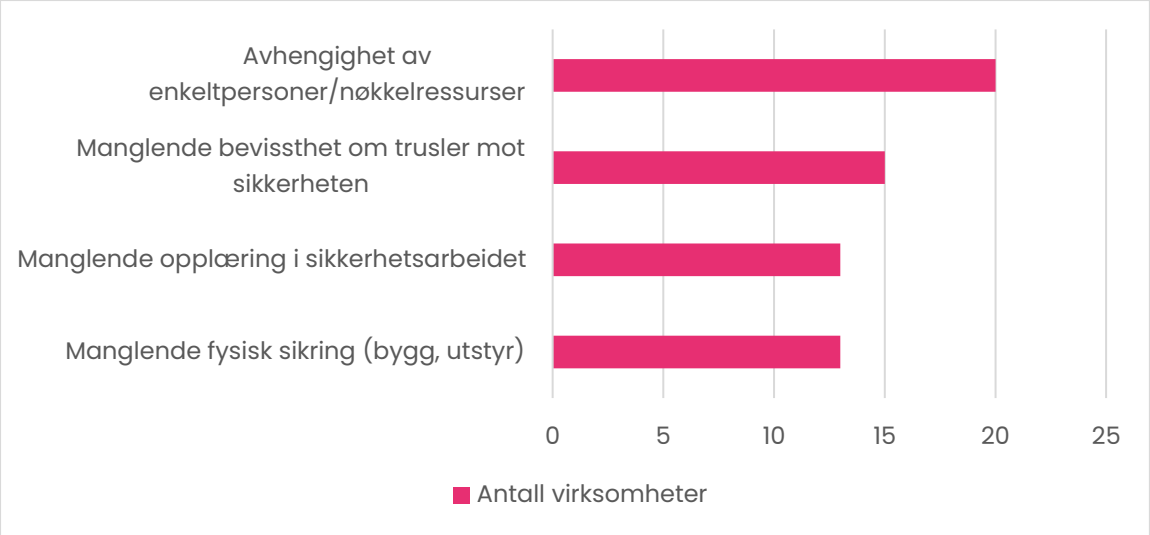
Sikkerhetskultur og risikoaksept

I intervjuene ble tiltak for å styrke sikkerhetskultur trukket frem som særlig viktige, blant annet for å styrke forståelsen for roller og ansvar. Ulike former for pedagogiske tiltak ble derfor vektlagt, eksempelvis opplæring i sikkerhet for nyansatte og kompetansehevende tiltak for ledere.

Det ble også fremhevet at enhver risiko ikke nødvendigvis skal møtes med tiltak – noe risiko må aksepteres. Dette ble begrunnet med at formålet er å redusere risiko så langt som mulig, men uten å legge for mange hindringer i veien for akademisk frihet.

4.3 Identifiserte sårbarheter

Virksomhetene ble spurt om hvilke sårbarheter i arbeidet med sikkerhet som var identifisert i ROS-analysene i 2025. Figuren nedenfor viser de 4 vanligste sårbarhetene som ble rapportert.



Figur 9: De 4 vanligste sårbarhetene identifisert i ROS-arbeidet i 2025 (N=28)

Den vanligste sårbarheten som er avdekket i ROS-arbeidet i sektoren, er avhengighet av noen få enkeltpersoner (eller nøkkelressurser). Det indikerer at relativt små personellendringer kan få store konsekvenser for sikkerhetsarbeidet hos de 20 virksomhetene som oppga dette som en sårbarhet. Deretter følger to sårbarheter som gjelder bevissthet om trusselbildet i sektoren og manglende sikkerhetsopplæring. Det er naturlig å se dette i lys av avhengigheten av enkeltpersoner: mangelfull bevissthet og opplæring kan øke avhengigheten av noen få kompetente nøkkelressurser.

Sårbarheter i arbeidet med personellsikkerhet

De 9 virksomhetene vi intervjuet rapporterte også om sårbarheter i arbeidet med personellsikkerhet. Det gjaldt særlig manglende kompetanse og mangelfulle rutiner. Mangel på felles praksis i sektoren for sikkerhetsvurderinger ved ansettelser – spesielt når det gjelder personer fra land som Norge ikke har et sikkerhetspolitisk samarbeid med – ble også rapportert som en sårbarhet.[5]

4.4 Kapasitet

Avhengighet av enkeltpersoner/nøkkelressurser viser at kapasitet, spesielt i form av personellressurser avsatt til sikkerhetsarbeidet, er en viktig utfordring i sektoren. Færrest årsverk finner vi hos de mindre virksomhetene. Vi ser det som bekymringsfullt at mange av de mindre virksomhetene har så få «hender i arbeid», og stiller spørsmål ved konsekvensene det kan ha for kvaliteten på sikkerhetsarbeidet.

Antallet årsverk gir likevel ikke en fullstendig oversikt over kapasiteten, da det også benyttes innleie av tjenester til gjennomføring av ulike sikkerhetsoppgaver. Hele 25 virksomheter opplyste om at de i 2025 kjøpte sikkerhetstjenester i markedet. Dette bidrar til å redusere konsekvensene av manglende egenkapasitet. Sikt var den mest brukte tjenesteleverandøren på sikkerhetsområdet. Deretter fulgte ulike private leverandører (Sikkerhetsledelse AS, Atea og PwC).

[5] HK-dir har utarbeidet retningslinjer for ansvarlig internasjonalt kunnskapssamarbeid (AIS). Retningslinjene ble utarbeidet som en oppfølgning av Panoramastrategien (2021-2027). For mer om AIS se Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid-Introduksjon | HK-dir.

5 Beredskapsplaner og -øvelser

I tillegg til iverksetting av tiltak mot hendelser med høy og middels risiko identifisert i overordnet ROS, må virksomhetene være forberedt på å håndtere hendelser når de oppstår. I departementets styringsdokument stilles det derfor krav om beredskaps- og kontinuitetsplaner basert på overordnet ROS.

Virksomhetene skal videre gjennomføre minst én øvelse i året på håndtering av hendelser identifisert i overordnet ROS. Hendelser som er vurdert til middels eller høy risiko skal prioriteres i valg av øvelsesscenario. I etterkant av øvelsene, skal virksomhetene lage en oppfølgingsplan. Planen skal inneholde læringspunkter fra øvelser, forslag til konkrete forbedringstiltak og tidsramme for gjennomføring av tiltak.

Store deler av sektoren rapporterer at de har utarbeidet beredskapsplaner basert på overordnet ROS, og at de har pandemiplan. Det foreligger også øvelsesplaner hos de aller fleste av virksomhetene, og årlige beredskapsøvelser blir vanligvis gjennomført. Det er likevel behov for forbedring når det gjelder evaluering av øvelser og utarbeidelse av planer for oppfølging av læringspunkter avdekket under øvelser.

Forbedringspotensialet i sektoren er klart størst når det gjelder kontinuitetsplaner for opprettholdelse av kritiske funksjoner ved høyt personellfravær, og tilsvarende planer for opprettholdelse av kritiske IT-funksjoner. Kontinuitetsplanene må beskrive hva som er kritiske IT-funksjoner, leveranser og avhengigheter, hvilke tiltak som kan og skal gjennomføres, og hvilke oppgaver som skal ivaretas.[6]

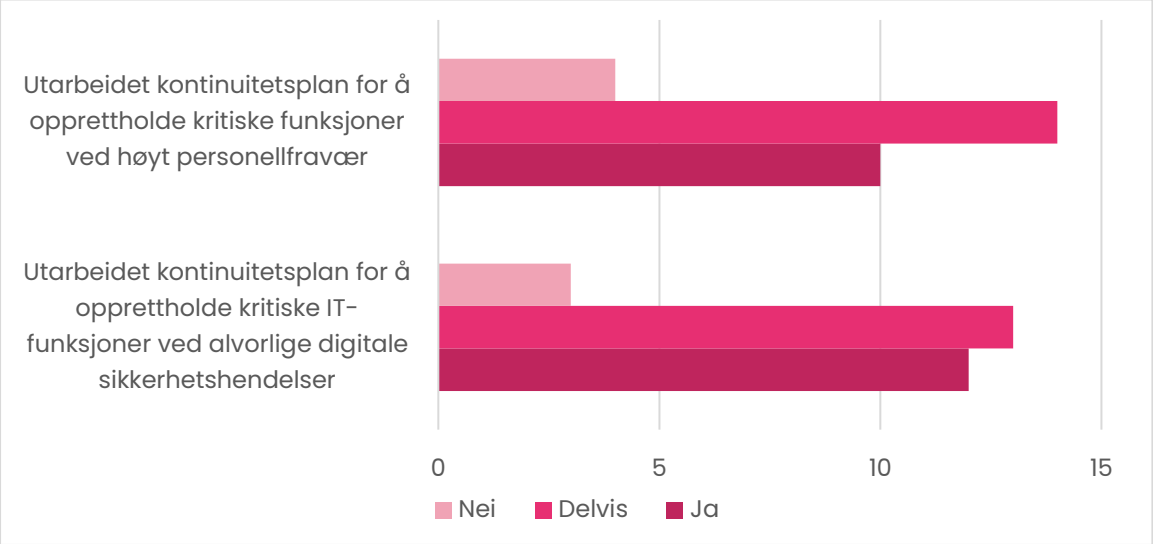
5.1 Beredskapsplaner

I spørreundersøkelsen oppga et stort flertall – 22 av 28 virksomheter – at de har utarbeidet beredskapsplaner. De resterende virksomhetene svarer at de delvis har utarbeidet slike planer. Dette er en liten forbedring sammenliknet med 2024.

20 virksomheter rapporterte om at de hadde gjennomgått sine beredskapsplanverk i 2025.

Resultatene i figuren nedenfor indikerer at det fortsatt er en del avvik fra kravene om kontinuitetsplaner for opprettholdelse av kritiske funksjoner ved høyt personellfravær.

[6] Tiltak som kan være aktuelle er opplæring av stedfortredere slik at stedfortredere enklere kan tre inn i en bestemt rolle ved høyt personellfravær, alternative løsninger for videre drift av IKT-systemer og krav til gjenopprettelsestid for systemene.



Figur 10: Etterlevelse av krav til kontinuitetsplanverk (N=28)

Kun 10 virksomheter svarte at dette er på plass, mens 14 sier at dette delvis er på plass. 4 virksomheter svarte at kontinuitetsplaner for høyt fravær mangler.

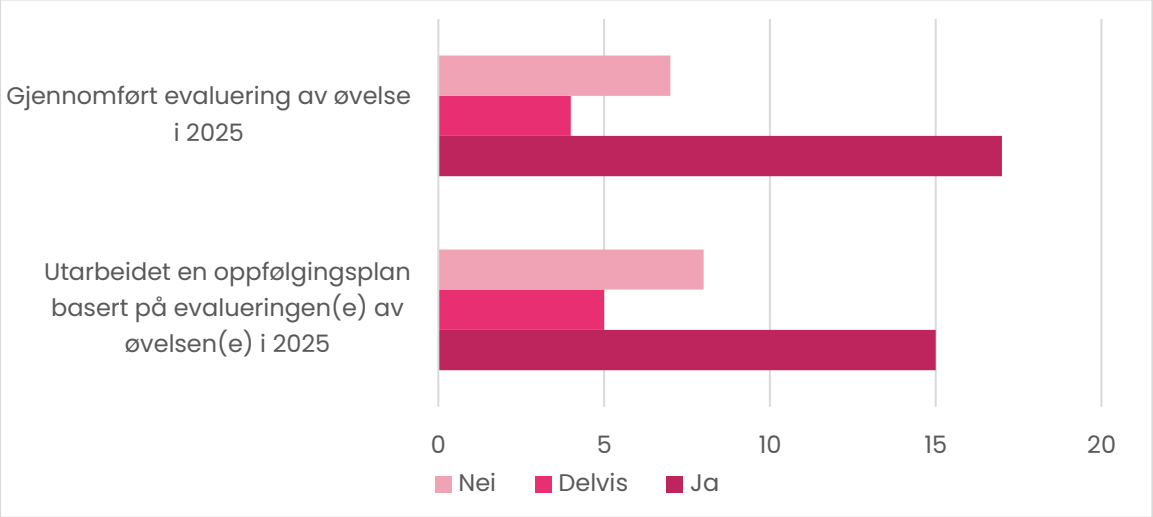
12 virksomheter svarte at de har kontinuitetsplan for kritiske IT-funksjoner, mens slike planer manglet helt eller delvis hos 16 virksomheter. 23 virksomheter opplyste om at de har en pandemiplan.

5.2 Øvelser

19 virksomheter svarte at beredskapsøvelser var gjennomført i 2025. De resterende virksomheter oppga at øvelse ikke ennå var gjennomført, men ville bli det i løpet av året (november eller desember 2025). Enkelte av disse virksomhetene ble intervjuet i etterkant av spørreundersøkelsen og bekreftet da at øvelsen var gjennomført.

De aller fleste virksomhetene oppga å ha utarbeidet en øvelsesplan. 5 virksomheter svarte at øvelsesplan delvis er utarbeidet, mens kun 2 virksomheter oppga å mangle en slik plan.

Det var imidlertid enkelte mangler knyttet til kravene om evaluering og oppfølging av øvelser.



Figur 11: Evaluering og oppfølging av beredskapsøvelser i 2025 (N=28)

17 virksomheter rapporterer at de har gjennomført evaluering, mens 11 virksomheter oppga at dette ikke eller bare delvis var gjort.

Svarene fra disse 11 virksomhetene må sees i sammenheng med at de ikke hadde øvd på kartleggingstidspunktet, og at de derfor heller ikke hadde evaluert øvelsene. Vi legger til grunn at alle virksomheter utførte evaluering etter gjennomført øvelse.[7]

Typer øvelser

I spørreskjema undersøkte vi for første gang hvilke typer øvelser virksomhetene i sektoren gjennomfører. Ut fra svarene ser vi at skrivebordøvelser er mest utbredt, med 17 virksomheter som oppga å ha gjennomført denne typen øvelse på kartleggingstidspunktet. Deretter følger spilløvelser, som ble oppgitt av 15 virksomheter, mens 11 virksomheter oppga å ha gjennomført funksjonsøvelser.

Videre svarte 15 virksomheter at de hadde utarbeidet oppfølgingsplaner basert på evaluering etter øvelser. De siste 13 virksomhetene hadde enten ikke laget oppfølgingsplaner eller hadde delvis gjort det. Også dette resultatet må sees i

[7] Direktoratet for samfunnssikkerhet og beredskap har veiledningsmateriell (Øvingsveiledning) for øvelser og evaluering av disse. I intervjudelen av kartleggingen nevnte enkelte virksomheter at de ser stor nytte i å ta utgangspunkt i dette veiledningsmaterialet i eget arbeid.

sammenheng med andelen virksomheter som på punktet for spørreundersøkelsen ikke hadde gjennomført øvelse enda.

Krisehåndteringsverktøy, innleie og samarbeid

I intervjudelen av kartleggingen oppga flere virksomheter at det er behov for å øve mer på bruk av krisehåndteringsverktøy. Enkelte virksomheter har de siste årene gått fra å bruke CIM til å benytte krisehåndteringsverktøyet RAYVN. Mange virksomheter har sluttført innføringen eller er i siste innføringsfase, og prioriterer nå å bli bedre kjent med verktøyet.

En del virksomheter opplyste om at de leier inn ekspertise for å planlegge og gjennomføre øvelser. Enkelte uttrykte også ønske om flere samarbeidsøvelser. Noen hadde allerede gjennomført slike øvelser, blant annet i regi av Sikt.

Med bakgrunn i resultatene ovenfor, ønsker vi å påpeke viktigheten av å gjennomføre evalueringer av øvelser og utarbeide oppfølgingsplaner. Gjennom dette får virksomhetene testet organisasjonen, avdekket svakheter i arbeidet og fulgt disse opp med konkrete forbedringstiltak.

5.3 Utfordringer i arbeidet med beredskapsplaner og -øvelser

Kartleggingen viser at sektoren har et betydelig forbedringspotensial med hensyn til kontinuitet. Store deler av sektoren mangler planverk for opprettholdelse av kritiske funksjoner ved høyt personellfravær. Samtidig ser vi at sektoren har behov for å kartlegge og dokumentere kritiske funksjoner og avhengigheter. Kartleggingen har også avdekket tilsvarende mangler når det gjelder planer for fortsatt drift ved bortfall av viktige IT-tjenester eller digital infrastruktur, for eksempel som følge av alvorlige digitale sikkerhetshendelser.

Videre viser kartleggingen at øvingsaktiviteten i sektoren er høy, men at det ofte dreier seg om skrivebordsøvelser. Virksomhetene bør variere mellom ulike typer øvelser – skrivebords-, spill- og funksjonsøvelser – og hva det øves på. Dette vil styrke læringseffekten av øvelsesaktiviteten. Det forutsetter imidlertid at øvelser evalueres og at eventuelle læringspunkter som avdekkes følges opp med tiltak. Også her ser vi at sektoren har et tydelig forbedringspotensial.

6 Sårbarhetsstyring hos utvalgte virksomheter

Som en del av våre årlige kartlegginger gjennomfører vi stedlige besøk hos et begrenset antall virksomheter (se tekstboks nedenfor). Her kontrollerer vi arbeidet med konkrete tekniske sikkerhetstiltak for å få innsikt i den reelle sikkerhetstilstanden. Vi har tatt utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet, men også tatt hensyn til funn i Riksrevisjonens undersøkelse av informasjonssikkerheten i forskningssystemer i UH-sektoren (Riksrevisjonen 2024).

Om dybdeundersøkelsen

I årets kartlegging av digital sikkerhet deltok tre virksomheter som representerer ulike deler av sektoren med hensyn til størrelse og faglig profil. Undersøkelsen ble gjennomført i form av fysiske møter hos de tre virksomhetene i desember 2025.

I forkant av møtene ble det oversendt informasjon om formålet med møtene, ønsket deltakelse og andre praktiske forhold knyttet til undersøkelsen. Virksomhetene mottok også informasjon om fokusområdet for undersøkelsen, og om spørsmål vi var særlig interessert i å finne svar på.

Årets kartlegging ser på hvordan virksomhetene arbeider med sårbarhetsstyring, det vil si sikkerhetsoppdateringer av programvare og reduksjon av sårbarheter i systemer og programvare. Angripere utnytter ofte sårbarheter i operativsystemer og programvare for å få tilgang til IT-systemer.

Våre resultater tyder på at de tre utvalgte virksomhetene ivaretar oppgaven på en god måte. Gjennom dette arbeidet hindrer de angripere i å utnytte sårbarheter i digitale tjenester som er tilgjengelig fra internett og tjenester internt i sine datanettverk. Det gjøres også en god jobb med sikring av klienter, servere og infrastruktur. Det er rom for forbedring når det gjelder sikring av mobile dataenheter som benyttes til jobbformål, og kontroll med sikkerheten i nettlesere.

6.1 Metodikk og kontrollkriterier

Vi vurderte virksomhetenes sårbarhetsstyring opp mot kriteriene fra NSMs (NSM 2021) grunnprinsipper for IKT-sikkerhet, nærmere bestemt grunnprinsipp 2.3 «Ivareta en sikker konfigurasjon» og 3.1 «Oppdag og fjern kjente sårbarheter og trusler». Vi hadde spesiell oppmerksomhet på disse anbefalte sikkerhetstiltakene:

- Etabler et sentralt styrt regime for sikkerhetsoppdatering (tiltak 2.3.1 i NSMs grunnprinsipper).

- Konfigurer klienter slik at kun kjent programvare kjører på dem (tiltak 2.3.2 i NSMs grunnprinsipper).
- Deaktiver unødvendig funksjonalitet (tiltak 2.3.3 i NSMs grunnprinsipper).
- Endre alle standardpassord på IKT-produktene før produksjonssetting (tiltak 2.3.7 i NSMs grunnprinsipper).
- Gjennomfør jevnlig sårbarhetskartlegging (tiltak 3.1.1 i NSMs grunnprinsipper).
- Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare) (tiltak 3.1.3 i NSMs grunnprinsipper).

6.2 Sentrale funn

Alle tre virksomheter har etablerte rutiner for gjennomføring av regelmessige sikkerhetsoppdateringer på klienter[8] og servere.

Styring og oppdatering av mobile enheter fremstår som et område med potensial for forbedring. I tilfeller hvor de ansatte har mulighet til å benytte mobiltelefoner til jobbrelaterte formål, for eksempel jobbmail, bør det etableres et sentralt styrt regime med muligheter for å sikre jevnlige oppdateringer av telefonene og fjernsletting av innholdet på dem.

En utfordring med dette er at styring av mobile dataenheter veldig raskt kan oppleves som en inngripen i brukernes private sfære. Dette gjelder særlig dersom enhetene er privateide, men allikevel benyttes til enkelte jobbrelaterte formål. Ved slik bruk er det en risiko for at sårbare enheter utnyttes av angripere på samme måte som en hvilken som helst annen dataenhet i virksomhetens IT-miljø. Dersom virksomheten mangler mulighet for fjernsletting er det også en risiko for at data kommer på avveie hvis enheten blir stjålet eller mistes.

[8] Klienter i denne sammenhengen dreier seg i all hovedsak om PC-er med Windows operativsystem, men vi undersøkte også hvordan virksomhetene håndterer Linux-PC-er og Mac.

Beskyttelse av mobile dataenheter

NSMs temarapport «Mobilapplikasjoner på tjenesteenheter» (NSM 2025) påpeker at mobile enheter er en del av den digitale infrastrukturen og har samme behov for sikring som andre datamaskiner. De anbefaler at det ikke overlates til den enkelte ansatte å vurdere hvilke applikasjoner som kan lastes ned på tjenesteenheter.

Et generelt råd til alle med smarttelefon er å være kritisk til hvilke tillatelser og informasjon man gir den enkelte applikasjon, og kun gi midlertidige tillatelser der det er mulig. Alle bør ha et bevisst forhold til applikasjonene som er installert på en tjenesteenhet eller en privat dataenhet.

I enkelte tilfeller ble det beskrevet behov for ulike former for unntak fra oppdateringsregimet, eksempelvis for teknisk utstyr i laboratorier som ikke kan oppdateres på normalt vis. Det ble da innført risikoreduserende tiltak for å begrense sårbarheter som dette medfører, vanligvis gjennom segmentering av nettverket.[9]

Alle virksomhetene har mulighet for kontroll av programvare som installeres på klientmaskiner. Samtlige oppga imidlertid at de mangler tilstrekkelig styring på hvilke tillegg som kan installeres i nettlesere. Dette oppleves som en sårbarhet som det er utfordrende for virksomhetene å håndtere. Ingen av virksomhetene gir brukere lokale administratorrettigheter på egne klientmaskiner.

For å sikre klientmaskiner ytterligere mot angrep anbefales det å begrense eller blokkere kjøring av makroer og scriptfiler. Disse kan inneholde skjulte kommandoer som utnytter sårbarheter, eller gjennomfører ondsinnede operasjoner, for eksempel datatyveri. Alle virksomhetene hadde etablert blokkering av dette med utgangspunkt i Microsofts anbefalinger for sikring av klientmaskiner. Der det var behov for unntak måtte unntakene godkjennes av sentral IT.

På servere og annen IT-infrastruktur har samtlige virksomheter etablert hensiktsmessige tiltak og rutiner for å redusere sårbarheter[10]. Det inkluderer blant

[9] Nettverkssegmentering er inndeling av virksomhetens nettverk i flere logiske soner. Trafikkflyt mellom ulike soner kan da overvåkes, begrenses eller sperres. På denne måten kan tilgang til sensitive data sikres, og man begrenser potensielle angriperes tilgang til virksomhetens sentrale tjenester.

[10] En av virksomhetene skilte seg ut ved å ikke ha teknisk gjeld i sin IT-infrastruktur, noe som var nedfelt i deres styringssystem. På denne måten har de besluttet at alt IT-utstyr som brukes skal være innenfor leverandørenes støtteperiode, slik at det blant annet mottar sikkerhetsoppdateringer som lukker nye sårbarheter som oppdages.

annet aktivering av lokal brannmur og stenging av unødvendige tjenester. Det er videre etablert ulike nettverkssegmenter for å administrere slikt utstyr.

Eksternt sårbarhetsskann

Digitale tjenester som er tilgjengelige fra internett er spesielt sårbare for angrep fra ondsinnede aktører. God praksis tilsier derfor at man begrenser antallet internetteksponerte tjenester til et minimum. Samtidig bør de tjenestene som er eksponert på internett sikres ekstra nøye.

Et viktig tiltak for å sikre disse tjenestene er sårbarhetsskann som leveres av cybersikkerhetssenteret hos Sikt (eduCSC). Her letes det etter sårbarheter i digitale tjenester i sektoren, og oppdagede sårbarheter rapporteres til den enkelte virksomhet. Cybersikkerhetssenteret følger også opp viktige funn slik at sikkerhetshull blir lukket. De tre virksomhetene som ble undersøkt i år hadde gode rutiner for oppfølging og utbedring av funn fra disse sårbarhetsskannene.

Internt i virksomhetenes nettverk kan det være sårbarheter som skanning av internetteksponerte tjenester ikke vil oppdage (se tekstboks ovenfor). To av virksomhetene gjennomfører sårbarhetsskann i ulike deler av sitt interne datanettverk. Den tredje oppga at de ikke har noe internt skann, men har benyttet en ekstern leverandør til penetrasjonstesting for å avdekke sårbarheter i internt datanettverk.

De tre virksomhetene som ble undersøkt hadde alle tatt i bruk avanserte brannmurer, såkalt applikasjonsbrannmur, som ble brukt til segmentering av nettverk og kontroll på trafikk mot internett. Arbeidet med å etablere korrekt sikkerhetsnivå er en stor oppgave, og to av virksomhetene opplyste om at det fremdeles pågår justeringer av brannmuroppsettet.

6.3 Utfordringer i arbeidet med sårbarhetsstyring

Kartleggingen avdekket to forbedringspunkter:

- Håndtering av mobile dataenheter som benyttes til arbeidsformål.
- Kontroll av nettlesere og brukeres muligheter til å installere tillegg.

En mobil dataenhet som benyttes i jobbsammenheng er en del av virksomhetens digitale infrastruktur og har behov for sikring. Det oppstår imidlertid utfordringer når enheten er privateid og sikkerhetstiltak ikke kan kreves.

En mulig tilnærming til denne problemstillingen kan være å vise til NSMs råd for bedre sikkerhet på mobile enheter (NSM 2024). Virksomhetene bør legge ekstra vekt på NSMs råd 13. Dette rådet anbefaler å skille mellom jobb og privatliv gjennom å kreve bruk av dedikerte applikasjoner til jobbrelaterte formål. På den måten kan virksomheten skaffe seg muligheter til å stenge tilganger og fjernslette informasjon i tilfelle enheten blir mistet eller stjålet. Bruk av dedikerte applikasjoner kan også bidra til å ivareta skillet mellom jobb og privatliv, og redusere risikoen for at data utilsiktet deles med uvedkommende.

Manglende kontroll på hvilke nettlesere som brukes, og ukontrollert bruk av tillegg til nettlesere, kan utgjøre en sikkerhetsrisiko. Utfordringen knyttet til nettlesere og tillegg har for øyeblikket ingen enkel og tydelig løsning. Noen sikkerhetsløsninger, for eksempel fra Microsoft, kan brukes til å overvåke hvilke tillegg som installeres i enkelte nettlesere. Her bør sektoren samarbeide gjennom å dele erfaringer og finne måter å håndtere dette på i tiden fremover.

7 Risikovurdering på sektornivå

I dette kapitlet vurderer vi risiko for utvalgte risikoscenarioer, det vil si uønskede hendelser som representerer trusler mot samfunnssikkerheten, nasjonal sikkerhet og informasjonssikkerheten i sektoren. Scenarioene er hendelser det er viktig at virksomhetene er forberedt på og iverksetter tiltak for å forebygge, oppdage og håndtere. Rammeverket for vurdering av risiko finnes i vedlegg 2.

Risikoscenarioene og vurderingene av dem baserer seg på funn og konklusjoner i kapittel 2-7. Vurderingene av våre utvalgte risikoscenarioer oppsummeres i matrisen nedenfor. Scenarioene benevnes S1–S7:

- S1 = Alvorlig digitalt angrep
- S2= Langvarig svikt i felles IKT-tjenester
- S3 = Brudd på personopplysningssikkerheten
- S4 = Svikt i kritisk infrastruktur og svikt i strømforsyning
- S5 = PLIVO-hendelse på campus
- S6 = Innsiderisiko og misbruk av tilganger i kritiske systemer
- S7 = Trusler, trakassering og psykososial utrygghet

Konsekvenser						
	Svært alvorlig		**S5**			
	Alvorlig		**S1**			
	Middels		**S2, S4**		**S6**	**S7**
	Små					**S3**
	Ubetydelig					
		Usannsynlig	**Lite sannsynlig**	**Mindre sannsynlig**	**Sannsynlig**	**Meget sannsynlig**
		Sannsynlighet				

Figur 12: Risikomatrise

Risikoscenario 1: Alvorlig digitalt angrep

Vår vurdering er at det er en **middels risiko** for alvorlige digitale angrep som medfører at en virksomhet blir ute av stand til å levere sentrale tjenester i en periode på 1-3 dager.

Beskrivelse av scenarioet:
Alvorlige digitale angrep forbindes ofte med såkalte APT-aktører.[11] Angrepene starter gjerne med phishing for å få tilgang til virksomhetens datanettverk. Angriperne benytter deretter avanserte metoder for å skaffe seg kontroll over nettverket. Målet kan være å stjele informasjon, sabotasje eller økonomisk vinning. Løsepengeangrep er et eksempel på det siste, hvor angriperen gjør data utilgjengelig og forlanger betaling for å gjenopprette tilgangen til dem. Angriperne kan også være grupper som opererer på vegne av fremmede stater. Her kan formålet være kunnskapsspionasje eller politisk motivert sabotasje.

Vurdering av sannsynlighet – lite sannsynlig
I årets kartlegging oppga ingen av virksomhetene å ha vært utsatt for forsøk på løsepengeangrep, og det var heller ingen som hadde tydelige indikasjoner på aktivitet fra APT-aktører. APT-angrep er imidlertid relativt vanlige både internasjonalt og nasjonalt, og NSM omtaler løsepengeangrep som en av de mest vanlige digitale angrepene som norske bedrifter utsettes for.

Flere av virksomhetene rapporterer å ha gjennomført hensiktsmessige tiltak for å forebygge, oppdage og håndtere slike angrep. Det er i tillegg iverksatt tiltak for å gjenopprette normal drift dersom de skulle bli rammet. Det gjelder tiltak som segmentering av datanettverk og strenge autentiseringskrav til administratorer.

Vurdering av konsekvenser – alvorlig
Skadevirkningene av et alvorlig digitalt angrep vil i de aller fleste tilfelle være omfattende. Angrep kan medføre at tjenester, for eksempel sentral lagring, blir utilgjengelig. Det kan også ramme sluttbrukeres PC-er slik at de ikke kan koble seg opp mot digitale tjenester. I begge disse tilfellene vil det være behov for gjenoppretting, noe som er ressurskrevende.

Slike angrep medfører i mange tilfeller betydelige økonomiske tap, både i form av oppryddingskostnader og tjenesteavbrudd (oppgaver som ikke utføres). Det kan også oppstå tap av blant annet forskningsdata dersom det er mangler i oppsettet for

[11] Avanserte vedvarende trusler (Advanced Persistent Threats, APT) betegner aktører som er ressurssterke, bruker avansert skadevare og opererer langsiktig. Dette kan være statlige eller statsstøttede aktører, men også nettkriminelle grupper.

lagring og sikkerhetskopiering. Større angrep kan dessuten medføre medieoppslag som kan påvirke omdømme og tilliten til virksomheten.

Risikoscenario 2: Langvarig svikt i felles IKT-tjenester

Vår vurdering er at det er en **lav risiko** for angrep eller en hendelse som medfører bortfall av felles IKT-tjenester i sektoren i en periode på 1-2 dager.

Beskrivelse av scenarioet:
Sektorens kjernevirksomhet er avhengig av felles IKT-tjenester levert av et begrenset antall leverandører. Avbrudd i tilgangen på disse tjenestene over en lengre periode vil kunne medføre at virksomhetene ikke er i stand til å utføre sin kjernevirksomhet. Sektoren har for eksempel utstrakt bruk av amerikanske skytjenester og er sårbare når disse opplever driftsforstyrrelser. En lignende situasjon kan oppstå dersom sektorens fellestjeneste for pålogging, Feide, blir utilgjengelig.

Vurdering av sannsynlighet – lite sannsynlig
Flere av virksomhetene opplyste om hendelser som førte til kortvarige driftsforstyrrelser, spesielt såkalte tjenestenektangrep mot nettsider og en av fellestjenestene i sektoren. I sine egne risikovurderinger er det også flere virksomheter som har identifisert leverandørkjeder og tredjeparter som sårbarheter, og har trukket frem bortfall av tjenester som et høyrisiko-scenario.

De hendelsene som har forekommet i sektoren er imidlertid av kort varighet, og det tar typisk 1-5 timer før normal drift er gjenopprettet. Samtidig har internasjonale skytjenester høy robusthet, leverandørene har stor oppmerksomhet på å unngå driftsforstyrrelser og tjenestene har i de aller fleste tilfeller høy tilgjengelighet. Det samme gjelder tjenester levert av Sikt. Dette omfatter både hvordan tjenestene er etablert, samt rutiner for beredskap, for eksempel ved bortfall av strøm.

Vurdering av konsekvenser – middels
Avhengig av tidsrommet hvor driftsforstyrrelser inntreffer, kan konsekvensene være relativt omfattende. Dersom brukere mister muligheten for pålogging til felles IKT-tjenester kan dette medføre stans eller store forstyrrelser i viktige aktiviteter, for eksempel forskning, undervisning eller gjennomføring av eksamen. I ytterste konsekvens kan dette føre til at det må etableres manuelle nødløsninger. Slike nødløsninger kan øke risikoen for brudd på sikkerhetsrutiner eller personvernet.

Risikoscenario 3: Brudd på personopplysningssikkerheten

Vår vurdering er at det er **middels risiko** for brudd på personopplysningssikkerheten som skyldes utilsiktede menneskelige eller tekniske feil og uhell.

Beskrivelse av scenarioet:
Denne typen hendelser varierer fra feilsending av e-poster og dokumenter eller feil i tilgangsstyring til uautorisert bruk av tredjepartsapplikasjoner i nettlesere og Office-applikasjoner. Det kan blant annet føre til at personopplysninger blir tilgjengelige for ansatte uten tjenstlige behov for tilgang til opplysningene. Dokumenter med sensitivt innhold kan bli lagret på lagringsområder uten tilgangsbegrensning.

Vurdering av sannsynlighet – meget sannsynlig
Det er meget sannsynlig at brudd på personopplysningssikkerheten vil forekomme, også brudd som innebærer varslingsplikt til Datatilsynet. Vi er imidlertid ikke kjent med hendelser som har medført overtredelsesgebyr fra Datatilsynet i 2025. Selv om vår vurdering er at brudd på personopplysningssikkerheten er meget sannsynlig, mener vi hendelsene trolig vil ha begrenset skadevirkning. Vi mener derfor at alvorlige brudd på personopplysningssikkerheten, for eksempel uautorisert tilgang til store mengder særlige kategorier opplysninger, er mindre sannsynlig.

Vurdering av konsekvenser – små
Konsekvensene av slike hendelser fremstår som mindre alvorlige, for eksempel at egne ansatte får innsyn i en begrenset mengde personopplysninger de ikke har tjenstlige behov for tilgang til. I tilfeller hvor hendelsen dreier seg om lagring på feil lagringsområder kan opplysninger bli endret eller slettet. Dette vil i så fall øke alvorlighetsgraden.

Hendelsene medfører brudd på personvernet til de registrerte. Dersom slike hendelser innebærer risiko for personers rettigheter og friheter, skal bruddet varsles til Datatilsynet, noe som kan medføre gebyrer. Hendelser med høy alvorlighetsgrad vil også omtales i media, og det kan påvirke virksomheters omdømme. Vi har likevel ikke indikasjoner på at brudd på personopplysningssikkerheten i 2025 har påvirket omdømme til virksomhetene eller til sektoren som helhet.

Risikoscenario 4: Svikt i kritisk infrastruktur og svikt i strømforsyning

Vår vurdering er at det er **lav risiko** for at virksomhetene utsettes for svikt i strømforsyning, som fører til avbrudd i teknisk drift, og opphold i undervisning og forskning.

Beskrivelse av scenarioet:
Sabotasje eller brann i en trafostasjon kan ramme deler av sektoren og føre til svikt i strømforsyning til læresteder og myndigheter.. Svikt i forsyning kan føre til uregelmessig og uforutsigbar driftssituasjon i 1-2 døgn, med alvorlige konsekvenser for avvikling av undervisning, eksamen, opptak, og kan utgjøre også risiko for tap av forskningsresultater.

Vurdering av sannsynlighet – lite sannsynlig
De nasjonale trusselvurderingene beskriver et trusselbilde som gir dette scenarioet økende relevans. Resultater fra årets kartlegging viser at det allerede skjer hendelser med utfall av kritisk infrastruktur, men disse hendelsene har ikke vært av et slikt omfang at det har påvirket virksomhetenes kjerneoppgaver i særlig grad.

Vurdering av konsekvenser - middels
En faktor som påvirker vurdering av konsekvens, er UH-sektorens avhengighet av digitale løsninger. En hendelse med forsyningssvikt og utfall av kritisk infrastruktur vil ha store konsekvenser for virksomheten, ansatte og studenter. Hendelsen vil ramme flest studenter og ansatte dersom den inntreffer i eksamens- eller opptaksperioden. Samtidig kan strømutfall og en påfølgende ustabil driftssituasjon ha negative konsekvenser for drift av laboratorier med fysiske forskningsdata som er avhengig av kjøling. Som nevnt ovenfor, er det likevel få virksomheter i vår sektor som rapporterer om alvorlige skader eller langvarig nedetid. Dette kan redusere vurdering av konsekvens.

Risikoscenario 5: PLIVO-hendelse på campus

Vår vurdering er at det er **middels risiko** for at ansatte eller studenter utsettes for en PLIVO-hendelse (pågående livstruende vold) på campus som innebærer tap av liv og helse.

Beskrivelse av scenarioet:
Trusler og vold i form av en PLIVO-hendelse på campus som rammer studenter eller ansatte, kan føre til tap av liv og helse, utløse evakuering, akutt politibistand og samvirke mellom nødetater. Et PLIVO-scenario kan derfor innebære en dramatisk situasjon for ansatte og studenter, en uklar trusselsituasjon, og et presset beslutningsmiljø ved virksomheten.

Vurdering av sannsynlighet – lite sannsynlig
De nasjonale trusselvurderingene beskriver et trusselbilde som gir dette scenarioet økende relevans. Studenter og andre unge mennesker kan la seg påvirke til å utføre voldshandlinger på campus.

Resultater fra årets kartlegging viser at det skjer hendelser med trusler og fysisk vold på campus. Slike hendelser kan eskalere til en PLIVO-hendelse. En annen sårbarhet som påvirker vurdering av sannsynlighet er UH-sektorens særpreg, dvs. stor åpenhet både i fysisk campusinfrastruktur, men også som prinsipp for samarbeid, mange publikumsflater og få fysiske barrierer. Det er ofte store folkemengder på campus og dette kan tiltrekke aktører som ønsker masseskade.

Faktorer som reduserer sannsynligheten, er lavt antall faktiske PLIVO-hendelser. Når det gjelder terrortrusselen, peker EOS-tjenestene på mål knyttet til samfunnskritiske funksjoner snarere enn utdanningsinstitusjoner. Også dette bidrar til å redusere sannsynligheten.

Vurdering av konsekvens – svært alvorlig
En PLIVO-hendelse på campus kan ha store konsekvenser for liv og helse. Hendelsen kan få særlig høy konsekvens dersom den inntreffer ved aktiviteter der mange deltar, for eksempel åpne arrangementer eller eksamener. Avhengig av utløsende årsak for hendelsen, kan en voldshendelse på én campus ha flere følgehendelser med like store konsekvenser.

Risikoscenario 6: Innsiderisiko og misbruk av tilganger i kritiske systemer

Vår vurdering er at det er **middels risiko** for at virksomhetene og verdiene de forvalter utsettes for innsidevirksomhet, hvilket innebærer risiko for tap av skjermingsverdig informasjon.

Beskrivelse av scenarioet:
Innsidere i UH-sektoren kan få tilganger som blir utnyttet over en lengre tidsperiode til påvirkning, etterretning eller ulovlig kunnskapsoverføring. Disse innsiderne kan videre bli bedt om å fremskaffe informasjon om sårbarheter i sikkerhetstiltak, rutiner og teknisk infrastruktur. Innsidere kan også utføre sabotasje eller forstyrrende aktiviteter. De kan også rekruttere andre personer til å utføre slike handlinger.

Vurdering av sannsynlighet – sannsynlig
Trusselvurderingene fra EOS-tjenestene peker på at virksomhetene bør legge til grunn at rekrutteringsforsøk vil skje. Sektoren forvalter viktige verdier, og innsidevirksomhet kan føre til tap av skjermingsverdig informasjon.

En annen sårbarhet som påvirker vurdering av sannsynlighet, er at det gjennomføres få tiltak som styrker arbeidet med personellsikkerhet i sektoren. Uavklart juridisk handlingsrom ved ansettelser, det vil si avveininger knyttet til kvalifikasjonsprinsippet og adgangen til lovlig forskjellsbehandling, utgjør en utfordring. Dette kan, sammen med begrensede styringsmuligheter i forsker-til-forsker-samarbeid, bidra til å gjøre sektoren sårbar for innsiderisiko.

Vurdering av konsekvenser - middels
Konsekvens av innsidevirksomhet kan ramme virksomheten på ulikt nivå og over en lengre tidsperiode. Uautorisert tilgang til informasjon kan muliggjøre gjennomføring

av sabotasjeaksjoner på campus eller i det digitale rom. Det kunne ramme virksomhetens forskning, økonomi og omdømme.

Innsidevirksomhet kan også gi fremmed etterretning tilgang til personopplysninger om diasporamiljøer. Dette kan innebære alvorlige konsekvenser for sikkerheten til disse personene eller deres familier (jf. «students at risk»). Videre kan innsidevirksomhet innebære kompromittering av skjermingsverdig informasjon, eksempelvis ved å føre til tap av teknologisk forsprang.

Risikoscenario 7: Trusler, trakassering og psykososial utrygghet

Vår vurdering er at det er **høy risiko** for at studenter og ansatte utsettes for trusler, trakassering og psykososial utrygghet, men også risiko for integritet til informasjonsverdier som virksomhetene forvalter.

Beskrivelse av scenarioet:
Forskere, undervisere eller administrativt ansatte utsettes for verbale trusler, sjikane, e-posttrusler, personforfølgelse (stalking) eller trakassering. Trusler og sjikane i det fysiske og digitale rom kan forsterke hverandre. Det kan føre til psykisk uhelse, sykemeldinger, utfordre den akademiske friheten, og svekke evnen til å beskytte integriteten til viktige informasjonsverdier og forskningsresultater.

Vurdering av sannsynlighet – meget sannsynlig
Både trusselvurderingene og årets kartlegging bekrefter at ansatte og studenter i vår sektor opplever trusler og psykososial utrygghet. Rapporteringen viser at slike hendelser skjer ved halvparten av virksomhetene.

Arbeid med forebyggende tiltak kan redusere sannsynligheten for slike hendelser Tiltakene som iverksettes dreier seg likevel mer om reduksjon av konsekvenser og i mindre grad om reduksjon av sannsynligheten for at slike hendelser skjer.

Vurdering av konsekvenser - middels
Trusler og press mot ansatte og studenter kan ha alvorlige konsekvenser for samfunnet og for den enkelte forsker/student. Det kan for eksempel få forskere eller ledere til å unngå kontroversielle temaer. Det kan også føre til at de avstår fra å komme med ytringer, avstår fra arrangementer og trekker seg fra verv. Dette kan påvirke kvaliteten eller integriteten til forskningen.

Fysiske hendelser som dreier seg om rusede og truende studenter, og uro som fører til stenging av bygg, kan skape utrygghet blant studenter og ansatte. Trusler og press kan også føre til at ansatte eller studenter forlater sektoren.

Sektorens innsats for å styrke arbeidet med hendelseshåndtering og beredskap kan redusere konsekvensene av slike hendelser. Årets kartlegging viser at virksomhetene arbeider systematisk med beredskapsplanverk for å håndtere vold og trusselsituasjoner. Flere virksomheter tar disse scenarioene inn i sine øvingsplaner og gjennomfører relevante øvelser.

8 Anbefalinger til videre arbeid

I dette kapitlet oppsummerer vi anbefalinger for det videre sikkerhetsarbeidet i sektoren. Våre anbefalinger baserer seg på funn fra årets kartlegging, og er ment å bidra til forbedret etterlevelse av kravene i departementets styringsdokument for sikkerhet og beredskap. De har i tillegg til hensikt å redusere risikoen for uønskede hendelser vurdert i forrige kapittel.

Styrings- og ledelsessystem

Kartleggingen viser at integreringen mellom sikkerhetsarbeidet og den øvrige virksomhetsstyringen er svak hos mange av virksomhetene.

Vi anbefaler at virksomheter som har mangler i dette arbeidet benytter prosesser som for eksempel ledelsens gjennomgang for å styrke koblingen mellom sikkerhetsstyring og virksomhetsstyring. Viktige prioriteringer i arbeidet med sikkerhet bør videre tas inn i virksomhetens plan- og budsjettprosess.

Risikostyring og sårbarheter

Kartleggingen viser at virksomhetene i sektoren iverksetter og gjennomfører risikoreduserende tiltak, men det er usikkert om tiltakene har den ønskede effekten.

Vi anbefaler at risikoreduserende tiltak følges opp i forbindelse med rapportering til virksomhetens toppledelse. Iverksatte tiltak bør revideres og det bør vurderes om de har hatt den planlagte effekten.

God risikostyring er avhengig av at virksomhetene har oversikt over hvilke verdier de forvalter og har vurdert hvor viktige verdiene er. Som ressurser i arbeidet med verdioversikt og verdivurdering, vil en ny sektorstandard for klassifisering av informasjon bli ferdigstilt av Sikt i løpet av 2026. Det vil også bli publisert en veileder om personellsikkerhet i UH-sektoren. Vi anbefaler at virksomhetene benytter disse ressursene i arbeidet med verdioversikt og verdivurdering. Det finnes også andre ressurser som kan benyttes, for eksempel NSMs «Håndbok i verdivurdering av informasjon» (NSM 2020).

Mange av de mindre virksomhetene i sektoren oppgir at det er avsatt få personellressurser til sikkerhetsarbeidet. Vi anbefaler at virksomhetene sikrer at de som har roller i sikkerhetsorganisasjonen gjøres i stand til å ivareta sine oppgaver på en hensiktsmessig måte. Dette innebærer at det er tydelig hvilket ansvar rollen innebærer, at det settes av tid til å utføre oppgavene og at rolleinnehaverne har nødvendig kompetanse.

Planverk og øvelser

Kartleggingen viser at virksomhetene i stor grad har utarbeidet krise- og beredskapsplaner, men at det ofte mangler kontinuitetsplan for ivaretakelse av kritiske funksjoner ved høyt personellfravær og tilsvarende planer for opprettholdelse av kritiske IT-funksjoner.

Vi anbefaler at virksomhetene beskriver de kritiske funksjonene, deres leveranser og avhengigheter, og hvordan de skal ivaretas i en beredskapssituasjon. Denne dokumentasjonen må gjøres kjent for de som har oppgaver i kontinuitetsarbeidet, og planverket må oppdateres ved behov.

Kartleggingen viser at samtlige virksomheter har gjennomført minst én øvelse, eller planla å gjennomføre en øvelse, i 2025. Det var imidlertid visse mangler når det gjelder evaluering av øvelsene og hvorvidt det ble utarbeidet en oppfølgingsplan basert på evalueringen.

Vi anbefaler at virksomhetene prioriterer å gjennomføre ulike typer øvelser og utarbeider en øvingsplan basert på overordnet ROS-analyse. Videre bør øvelsene involvere virksomhetens ledelse og ansatte både i planleggings- og evalueringsfasen.

Tekniske sikkerhetstiltak

De stedlige undersøkelsene av teknisk sikkerhet viser at virksomhetene som ble undersøkt gjør en god jobb med sårbarhetsstyring. Det er likevel rom for forbedring når det gjelder mobile dataenheter som benyttes til jobbformål. Disse enhetene kan inneholde informasjon og gi tilgang til virksomhetens tjenester, og har derfor behov for sikring.

Vi anbefaler at virksomhetene skaper et skille mellom jobb og privat bruk på mobile dataenheter ved å kreve bruk av dedikerte applikasjoner til jobbformål. På denne måten får virksomhetene bedre muligheter til å stenge tilganger og fjernslette informasjon dersom enheter kommer på avveie.

Referanseliste

Beredskapsrådet. (2022). *Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren.* https://www.uis.no/sites/default/files/2022-06/Risiko-%20og%20sa%CC%8Arbarhetsanalyse%20i%20kunnskapssektoren.pdf

Etterretningstjenesten. (2026). *Fokus 2026*. https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20NO%20-%20Weboppslag%20v4.pdf

Kunnskapsdepartementet. (2025). *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor.* https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeid-med-sikkerhet-og-beredskap-i-kunnskapsdepartementets-sektor/id3096694

Nasjonal sikkerhetsmyndighet. (2020). *Håndbok i verdivurdering av informasjon.* https://nsm.no/getfile.php/133657-1592813304/NSM/Filer/Dokumenter/Veiledere/handbok-i-verdivurdering-av-informasjon---032020.pdf

Nasjonal sikkerhetsmyndighet. (2021). *NSMs grunnprinsipper for IKT-sikkerhet (v2.1)*. NSMs Grunnprinsipper for IKT-sikkerhet v2.1.pdf

Nasjonal sikkerhetsmyndighet. (2024) *13 råd for bedre sikkerhet på mobile enheter.* https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/13-rad-for-bedre-sikkerhet-pa-mobile-enheter

Nasjonal sikkerhetsmyndighet. (2025) *Mobilapplikasjoner på tjenesteenheter.* https://nsm.no/getfile.php/1314053-1730352841/NSM/Filer/Dokumenter/Rapporter/NSM%20temarapport%202024%20Mobilapplikasjoner%20for%20tjenesteenheter.pdf

Nasjonal sikkerhetsmyndighet. (2026). *Risiko 2026*. NSM Risikorapport 2026

Politiets sikkerhetstjeneste. (2026). *Nasjonal trusselvurdering 2026* https://www.pst.no/wp-content/uploads/2026/02/Nasjonal-trusselvurdering-2026.pdf

Riksrevisjonen. (2024). *Informasjonssikkerhet i forskning innenfor kunnskapssektoren*. Sensitive forskningsdata kan komme på avveie

Figurliste

Vedlegg 1: Data og metode

Rapporten bygger primært på informasjon innhentet gjennom spørreskjema, intervju, dokumentkontroll og besøk i sektoren. Kartleggingsdata fra spørreskjema ble innhentet fra hver av de 21 statlig eide universitetene og høgskolene, og de sju øvrige forvaltningsorganer og selskaper, som omfattes av Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor, og Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i UH-sektoren.

Datainnsamlingen ble gjennomført i perioden 18. september til 9. desember 2025 på følgende måte:

- Spørreskjema til alle 28 virksomheter med svarfrist 15. oktober.
- Dokumentasjon fra 4 virksomheter innsendt med frist 20. november.
- Intervju med 9 virksomheter i perioden 7. til 21. november.
- Dybdeundersøkelser hos 3 virksomheter i perioden 1. til 9. desember.

Forberedelse og kontakt
Brev med informasjon om kartleggingen ble sendt ut til samtlige virksomheter 18. september.

Det ble gjennomført et felles videomøte for virksomheter i sektoren 8. oktober for å informere om kartleggingsopplegget.

For virksomheter utvalgt til intervju og dybdeundersøkelser ble et sett med spørsmål (kartleggingsskjema) oversendt minst to uker i forkant. Hensikten med møtene var å få svar på spørsmålene i skjemaet.

Deltakelse og deltakere
Deltakelsen fra virksomhetene i kartleggingsmøtene varierte noe. Den omfattet vanligvis tre til seks ledere og medarbeidere. Dette var primært sikkerhets- og beredskapsledere, informasjonssikkerhetsledere eller -rådgivere, rådgivere i forskningsadministrasjonen og personvernombud.

HK-dir stilte med to eller tre deltakere i intervjuene og to deltakere i dybdeundersøkelsene.

Gjennomføring og datainnsamling
Alle intervjuer ble avholdt som videokonferanser hvor det ble gjort opptak av møtet, og det var satt av 1,5 timer til besvarelse av spørsmålene i kartleggingsskjemaet.

Alle dybdeundersøkelser ble gjennomført som fysiske besøk hos virksomhetene, og det var satt av inntil fire timer til gjennomgang av spørsmålene i kartleggingsskjemaet.

Etterarbeid og tilbakemeldinger
I etterkant av møtene utarbeidet HK-dir et kartleggingsreferat som oppsummerte virksomhetenes svar. Referatene ble sendt tilbake til den enkelte virksomhet for kommentarer og kvalitetssikring. Vi mottak tilbakemeldinger – korreksjoner og utfyllende kommentarer – fra én virksomhet.

Med bakgrunn i kartleggingsreferatene, utarbeidet HK-dir anbefalingsbrev til den enkelte virksomhet. I brevene ble det gitt anbefalinger om hva vi mener virksomhetene bør legge vekt på i det videre sikkerhetsarbeidet.

Andre datakilder
Informasjon fra andre kilder enn kartleggingsmøtene inngår i datagrunnlaget for rapporten. Dette gjelder følgende datakilder:

- statistikk om IT-sikkerhetshendelser i forskningsnettet fra «Cybersikkerhetssenteret for forskning og utdanning» (eduCSC) hos Sikt,
- statistikk om IT-sikkerhetshendelser ved NTNU, UiB, UiO, og UiT,
- årsrapporter fra virksomhetene for 2025,
- risiko- eller trusselvurderinger fra nasjonale myndigheter.

Metodiske begrensninger
Den primære datakilden var svarene som virksomhetene ga på spørsmålene i spørreskjemaet og kartleggingsskjemaet for de 9 virksomhetene som deltok på intervju.

Det var administrativt ansatte som deltok på kartleggingsmøtene. Dersom fordelingen av deltakere hadde sett annerledes ut, for eksempel at vitenskapelig ansatte hadde deltatt i større grad, kan det tenkes at enkelte av svarene hadde blitt noe annerledes.

Med unntak av innsendt dokumentasjon og besøkene ble det ikke gjennomført kontroller eller testing av tiltak som virksomhetene opplyste om.

Vedlegg 2: Rammeverket for vurdering av risiko

Sannsynlighetsverdier (sannsynlighetsintervaller)
Sannsynlighet er vurdert ut fra sannsynlighetsintervaller basert på tilgjengelige data og vurdering av tilgjengelige kilder. Dette er uttrykt med følgende inndeling:

Sannsynlighetskategori	**Beskrivelse av sannsynlighetskategori**
Usannsynlig	Mindre enn 0.1%
Lite sannsynlig	Mellom 0.1% og 1%
Mindre sannsynlig	Mellom 1% og 10%
Sannsynlig	Mellom 10% og 50%
Meget sannsynlig	Mer enn 50%

Konsekvensverdier (skadevirkninger)
Konsekvensverdiene er inndelt i kategorier fra «Ubetydelig» til «Svært alvorlig». Tabellene under gir noen eksempler på konsekvenser i de ulike kategoriene.

Ubetydelig:

Områder	**Konsekvenser**
Liv og helse	Ingen fysiske eller psykiske skader
Driftssikkerhet/tjenesteyting	Ingen påvirkning på drift
Troverdighet og omdømme	Ingen påvirkning på troverdighet
Økonomiske og materielle verdier	Ingen økonomisk skade

Små:

Områder	**Konsekvenser**
Liv og helse	Få eller små fysiske eller psykiske skader
Driftssikkerhet/tjenesteyting	Driftsforstyrrelse/stans mindre enn 24 timer
Troverdighet og omdømme	Svekket lokalt samarbeid og troverdighet
Økonomiske og materielle verdier	Mindre økonomisk tap som kan gjenopprettes

Middels:

Områder	**Konsekvenser**
Liv og helse	Alvorlige fysiske eller psykiske skadde
Driftssikkerhet/tjenesteyting	Driftsforstyrrelse/stans i 1-2 døgn
Troverdighet og omdømme	Svekket regionalt samarbeid og troverdighet
Økonomiske og materielle verdier	Betydelig økonomisk tap som kan gjenopprettes

Alvorlig:

Områder	**Konsekvenser**
Liv og helse	1 dødsfall og/eller alvorlig fysisk skadet
Driftssikkerhet/tjenesteyting	Driftsforstyrrelse/stans i 2-7 døgn
Troverdighet og omdømme	Svekket nasjonalt samarbeid og troverdighet
Økonomiske og materielle verdier	Uopprettelig økonomisk tap

Svært alvorlig:

Områder	**Konsekvenser**
Liv og helse	Flere døde
Driftssikkerhet/tjenesteyting	Driftsforstyrrelse i mer enn 1 uke
Troverdighet og omdømme	Svekket internasjonalt og nasjonalt samarbeid og troverdighet
Økonomiske og materielle verdier	Betydelig og uopprettelig økonomisk tap

Risikonivåer og oppfølging

Høy risiko:
Hendelser som medfører uakseptabel risiko:

- Hendelser som er svært sannsynlige og som kan få mindre alvorlige, alvorlige eller meget alvorlige skadevirkninger.
- Hendelser som er sannsynlige og som kan få alvorlige eller meget alvorlige skadevirkninger.
- Hendelser som er lite sannsynlige og som kan få meget alvorlige skadevirkninger.

Oppfølging: Kunnskapsdepartementet og HK-dir må vurdere om eksisterende eller planlagte sektortiltak i risikohåndteringsplanen er egnet til å redusere risikoen, eventuelt om sektortiltakene må revideres for å styrke og målrette tiltakenes risikoreduserende effekt.

Middels risiko:
Hendelser som medfører behov for nærmere vurdering:

- Hendelser som er svært sannsynlige og som kan få lite alvorlige skadevirkninger.
- Hendelser som er sannsynlige og som kan få mindre alvorlige skadevirkninger.
- Hendelser som er lite sannsynlige og som kan få alvorlige skadevirkninger.
- Hendelser som er svært lite sannsynlige og som kan få alvorlige eller meget alvorlige skadevirkninger.

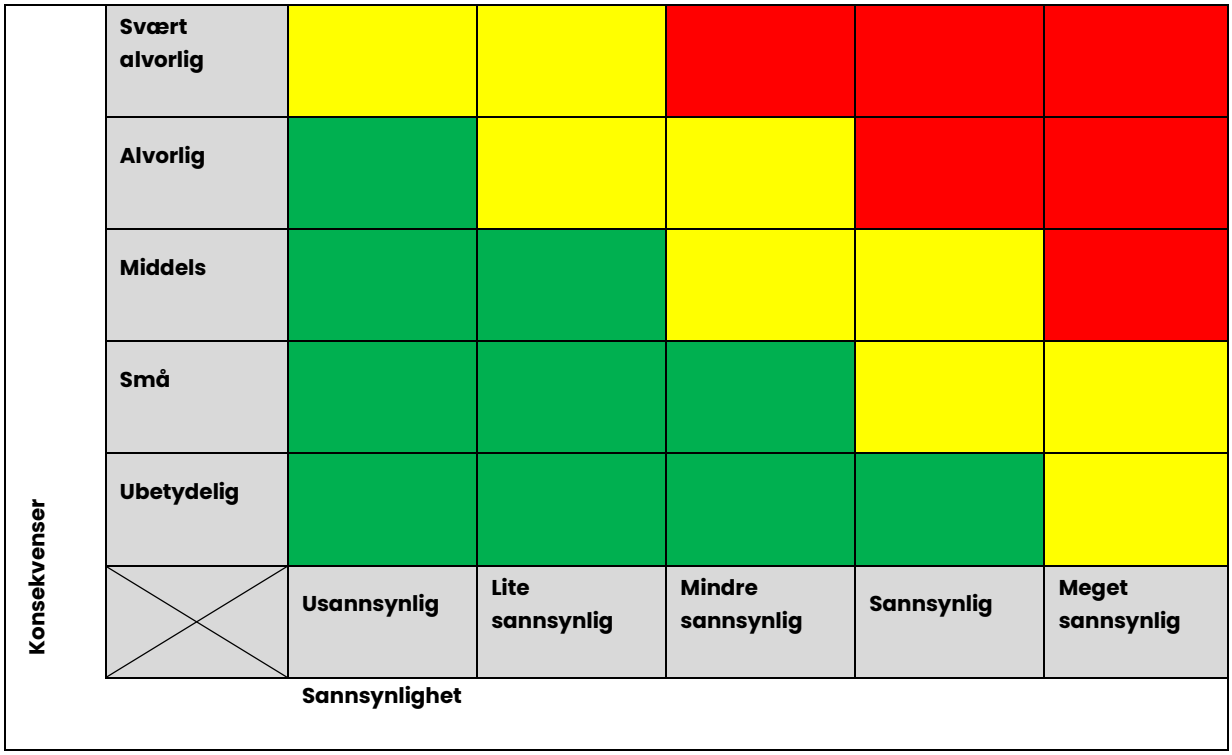
Oppfølging: Kunnskapsdepartementet og HK-dir bør ser nærmere på hendelsene. Det bør vurderes om risikoen kan aksepteres, særlig sett i lys av eksisterende eller planlagte tiltak i risikohåndteringsplanen, eventuelt at sektortiltakene revideres for å styrke og målrette tiltakenes risikoreduserende effekt.

Lav risiko
Risikoen aksepteres:

- Hendelser som er svært lite sannsynlige og som kan få lite eller mindre alvorlige skadevirkninger.
- Hendelser som er lite sannsynlige og som kan få lite eller mindre alvorlige skadevirkninger.
- Hendelser som er sannsynlige og som kan få lite alvorlige skadevirkninger.

Oppfølging: N/A.

Risikomatrise:



Om vurdering av konsekvens

Konsekvensene av en uønsket hendelse kan være sammensatte. Det betyr at når en hendelse har flere forskjellige skadevirkninger kan alvorlighetsgraden variere: noen av skadevirkningene kan være svært alvorlige mens andre kan være mindre eller lite alvorlige.

I slike situasjoner – når en hendelses alvorlighetsgrad varierer mellom skadekategorier – har vi valgt å legge den mest alvorlige skadevirkningen til grunn for vurderingen av hendelsens konsekvens. Det betyr for eksempel at dersom en hendelse innebærer alvorlig driftsavbrudd samtidig som andre skadevirkninger (økonomisk tap, omdømme, osv.) vurderes som middels eller små, vil konsekvensverdien for hendelsen bli alvorlig.

Dersom én eller flere av de andre skadevirkningene, for eksempel økonomisk tap og omdømme/tillit, også vurderes som alvorlige, vil hendelsens konsekvensverdi fortsatt være alvorlig. Hendelsen vil likevel innebære flere negative konsekvenser enn når det bare er skadevirkningene for tjenesteytelsen som vurderes som alvorlige. I slike tilfeller kan det være særlig viktig at det iverksettes risikoreduserende tiltak.

Direktoratet for
høyere utdanning
og kompetanse

post@hkdir.no hkdir.no