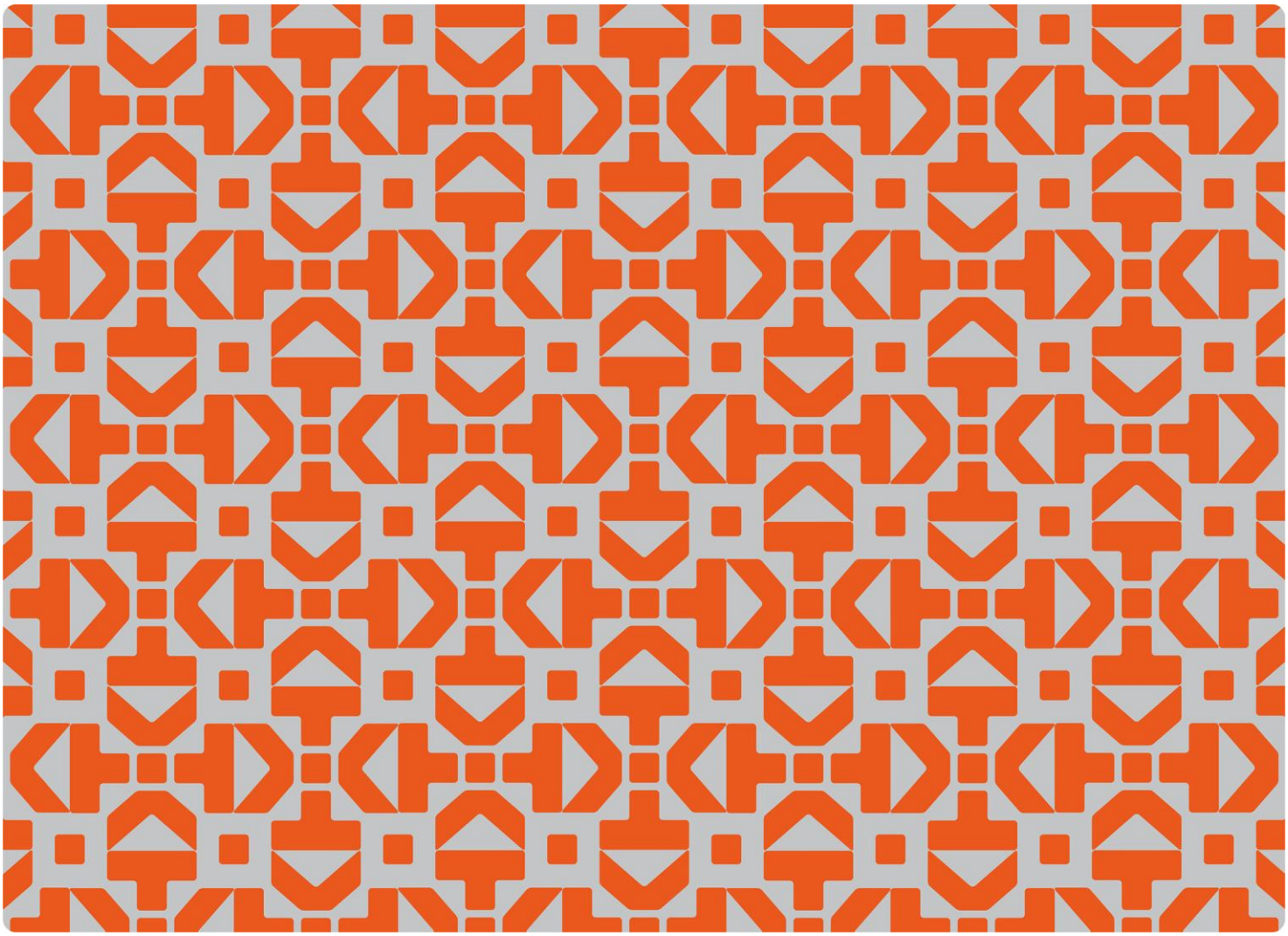
Rapport nr. 09/2025

Tilstands- og risikovurdering 2025

Arbeidet med sikkerhet og beredskap i høyere utdanning og forskning



Tilstands- og risikovurdering 2025

Arbeidet med sikkerhet og beredskap i høyere utdanning og forskning

Redaktør:
Kristin Selvaag

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

ISSN: 2703-9102

Innholdsfortegnelse

Sammendrag

Årets tilstands- og risikovurdering gir en samlet fremstilling av status for arbeidet med samfunnssikkerhet og beredskap, nasjonal sikkerhet, informasjonssikkerhet og personvern hos 28 virksomheter i forsknings- og høyere utdanningssektoren. Den presenterer også funn og anbefalinger fra dybdeundersøkelser (stedlige kontroller) av sikkerheten i viktige skytjenester hos utvalgte virksomheter i sektoren.

Avslutningsvis inneholder rapporten vurderinger av risikoscenarioer og anbefalinger til virksomhetene for det videre arbeidet med sikkerhet og beredskap.

Hovedfunn og anbefalinger

Trusler mot sektoren: Trusselbildet preges av økt geopolitisk spenning og mer krevende digitale sikkerhetsutfordringer. Statlige aktører som Russland og Kina, samt nettkriminelle grupper, utgjør de største truslene. Nettfiske er den vanligste sikkerhetshendelsen i sektoren.

Det er registrert en økning i personvernavvik som er meldt til Datatilsynet i 2024. Avvikene er særlig knyttet til utilsiktede feil og uhell hos ansatte, men også svakheter i tilgangsstyringen i sektorens IT-systemer.

Sikkerhetsledelse og -styring: Styring og ledelse av sikkerhetsarbeidet er styrket i 2024, men det er fortsatt et tydelig forbedringspotensial i sektoren. Det skyldes at litt over halvparten av virksomhetene er i ferd med å innføre styringssystem for sikkerhet, mens de øvrige virksomhetene ikke har kommet i gang med dette. 17 virksomheter har fortsatt enkelte viktige mangler i sitt ledelsessystem for informasjonssikkerhet.

Hos mange virksomheter er styrings- og ledelsessystemet i liten grad samordnet, og sikkerhetsledelse inngår i begrenset grad i den øvrige virksomhetsstyringen.

Oversikten over informasjonsverdier: Sektoren har relativt god oversikt over viktige IT-systemer og -tjenester som benyttes. Mange virksomheter har imidlertid ikke tilfredsstillende oversikt over informasjonsverdier underlagt sikkerhetsloven og eksportkontrollregelverket.

De fleste virksomhetene har kartlagt hvilke personopplysninger de forvalter (behandlingsprotokoll), men graden av opplysningsoversikt varierer mellom virksomhetsområder (utdanning, forskning og administrasjon). Samtidig er kjennskapen til hvilke personopplysninger som overføres til land utenfor EØS-området mangelfull hos nesten halvparten av virksomhetene.

Risikovurdering og tiltak: Vurderinger av risiko for uønskede sikkerhets- og personvernhendelser gjennomføres hos de fleste virksomheter i sektoren. Oppfølging av vurderingene med nødvendige sikkerhetstiltak er varierende, men alle virksomheter oppgir at de har iverksatt organisatoriske, tekniske eller pedagogiske tiltak i 2024.

Til tross for disse tiltakene, er det likevel sårbarheter i sektoren innen områder som tilgangsstyring, personellsikkerhet, beredskap og kontinuitet.

Beredskapsplaner og -øvelser: Overordnede beredskaps- og kontinuitetsplaner for håndtering av kriser og andre uønskede sikkerhetshendelser foreligger i stor grad. På den annen side er beredskaps- og kontinuitetsplanverket for digitale hendelser ofte utdatert eller ufullstendig.

Øvelsesaktiviteten i sektoren er høy. Systematikken i aktiviteten, både når det gjelder planlegging av øvelser og oppfølging av læringspunkter, er imidlertid mangelfull hos flere virksomheter.

Tilgangsstyring i skytjenester: Dybdeundersøkelser av tilgangsstyringen i skyløsninger avdekket store variasjoner i virksomhetenes sikkerhetsnivå. Særlig én virksomhet hadde betydelige svakheter i tilgangsstyringen.

På bakgrunn av dybdeundersøkelsene, har vi bedt samtlige virksomheter om å gjennomgå sine rutiner og praksis for håndtering av administrative tilganger i skytjenester. Eventuelle mangler bør utbedres i tråd med NSMs anbefalinger.

Risiko på sektornivå: På sektornivå vurderes risikoen for løsepengevirus og kunnskapsspionasje som høy. Sektoren bør derfor styrke sin evne til å forebygge, oppdage og håndtere disse hendelsene. For de øvrige sikkerhetshendelsene som vi har vurdert i år, mener vi at risikoen er middels.

Anbefalinger: Vi anbefalinger at virksomhetene i sektoren iverksetter flere forbedringstiltak. Disse omfatter blant annet ferdigstilling og samordning av styrings- og ledelsessystemer, forbedret risikostyring, etablering av beredskaps- og kontinuitetsplaner, og styrking av personellsikkerheten og tilgangsstyringen.

Kapittel 1: Innledning

Årets tilstands- og risikovurdering oppsummerer hovedfunn fra HK-dir sin kartlegging av arbeid med sikkerhet og beredskap hos 28 virksomheter i forsknings- og høyere utdanningssektoren. Rapporten gir en oversikt over virksomhetenes etterlevelse av kravene i Kunnskapsdepartementets styringsdokument for sikkerhet og beredskap (2025) og tilsvarende krav i policy for informasjonssikkerhet og personvern i høyere utdanning og forskning (HK-dir, 2025).[1]

Rapporten oppsummerer også viktige funn fra undersøkelser av tilgangsstyring i skytjenester hos utvalgte virksomheter.

Til slutt inneholder rapporten vurderinger av risikoen for konkrete sikkerhetsbrudd i sektoren, og anbefalinger til virksomhetene om hva de bør gjøre for å styrke sin evne til å forebygge, oppdage og håndtere uønskede sikkerhets- og personvernhendelser.

Definisjoner

Med sikkerhet menes både samfunnssikkerhet og beredskap, nasjonal sikkerhet og informasjonssikkerhet, inkludert sikring av personopplysninger.

Med forsknings- og høyere utdanningssektoren menes de 28 virksomhetene som omfattes av HK-dir sine kartlegginger av sikkerhet og beredskap. 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 utenrikspolitiske institutt; Simula Research AS; De nasjonale forskningsetiske komiteene og Universitetssenteret på Svalbard.

For definisjoner av andre sentrale begreper, se vedlegg 1.

Nytt kartleggingsopplegg

Dette er første gang HK-dir gjør en samlet kartlegging av forsknings- og høyere utdanningssektorens arbeid innen samfunnssikkerhet og beredskap, nasjonal sikkerhet, informasjonssikkerhet og personvern. Denne og kommende rapporter vil derfor gi et samlet bilde av tilstand og risiko på sektornivå med hensyn til sikkerhet og beredskap.

[1] Se vedlegg 1 for en oppsummering av kravene i styringsdokumentet og policyen.

Det innebærer at opplegget for kartleggingen er endret sammenliknet med tidligere år. Endringene betyr at kartleggingen både tar sikte på å

a) gi en oversikt over forsknings- og høyere utdanningssektoren arbeid med sikkerhet og beredskap, og
b) fremskaffe dybdeinformasjon for å vurdere den reelle sikkerhetstilstanden.

Det siste dreier seg blant annet om å undersøke hvilke sikkerhetstiltak som utvalgte virksomheter har iverksatt, og å vurdere disse opp mot anbefalt praksis.

For å gi en oversikt over sektorens arbeid med sikkerhet og beredskap, har virksomhetene besvart et spørreskjema med 28 spørsmål. Spørsmålene handlet om hvordan virksomhetene mener de etterlever de krav som gjelder. I tillegg ble det stilt spørsmål om blant annet uønskede hendelser, sårbarheter og iverksatte sikkerhets- og personverntiltak. Det er dessuten innhentet data fra Sikt – kunnskapssektorens tjenesteleverandør om digitale sikkerhetshendelser og personvernavvik i forskning.

Videre er det gjennomført intervjuer med 10 utvalgte virksomheter. Formålet med intervjuene var å fremskaffe supplerende informasjon om forhold som det spørres om i spørreskjemaet. Videre ble det gjennomført møter om digitale sikkerhetshendelser med fire universiteter. Møtene fokuserte på det digitale trusselbildet i sektoren.

Til sist har vi gjennomført dybdeundersøkelser hos tre virksomheter. Undersøkelsene foregikk ved stedlige besøk, og formålet var kontroll av sikkerheten i skytjenester.

Nytt sikkerhetsoppdrag til HK-dir

Kunnskapsdepartementet har gitt HK-dir i oppdrag å gjennomføre kontroller av forsknings- og høyere utdanningssektoren arbeid med samfunnssikkerhet og beredskap, og nasjonal sikkerhet. Kontrollene på samfunnssikkerhetsområdet ble tidligere utført av Nasjonalt organ for kvalitet i utdanningen (NOKUT).

Det nye oppdraget ble overført til HK-dir med virkning fra 1. januar 2025. Resultater fra disse kontrollene vil inngå i HK-dir sine tilstands- og risikorapporter fra neste år.

Veien videre

I kapittel 2-6 gir vi en oversikt over trusselbildet og den generelle sikkerhetstilstanden i sektoren. I tillegg til svarene på spørreskjemaet, intervjuer og data fra Sikt, baserer

kapitlet seg på EOS-tjenestenes[2] vurderinger av trusler og risiko. Det baserer seg også på rapporter fra norsk politi og internasjonale sikkerhets- og IT-selskaper.

I kapittel 7 oppsummerer vi funn fra dybdeundersøkelsen, det vil si tiltak som er iverksatt for å styrke tilgangsstyringen i virksomhetenes skytjenester.

I kapittel 8 vurderer vi risikoen for uønskede sikkerhets- og personvernhendelser i sektoren. Vurderingene baserer seg på funn og konklusjoner i de tidligere kapitlene.

I kapittel 9 gir vi anbefalinger om tiltak som sektoren bør iverksette for å styrke etterlevelsen av kravene i departementets styringsdokument for sikkerhet og beredskap og i policyen for informasjonssikkerhet og beredskap. Anbefalingene har også til hensikt å redusere risikoen for uønskede sikkerhets- og personvernhendelser drøftet i det foregående kapitlet.

[2] EOS-tjenestene er Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E-tjenesten).

Kapittel 2: Trusselbildet i sektoren

Virksomhetenes arbeid med sikkerhet må ta utgangspunkt i et oppdatert og relevant trusselbilde. Dette er viktig for å kunne vurdere risiko for brudd på sikkerheten og personvernet, og for å kunne iverksette effektive forbedringstiltak.

I dette kapitlet gir vi derfor en kort oppsummering av hvordan etterretnings- og sikkerhetstjenestene (EOS-tjenestene) vurderer dagens trusselbilde. Deretter ser vi nærmere på hvordan disse truslene påvirker forsknings- og høyere utdanningssektoren. For å supplere vurderingene fra EOS-tjenestene, benytter vi hendelses- og sårbarhetsdata fra Sikt, samt rapporter fra norsk politi og internasjonale sikkerhets- og IT-selskaper.

Til sist gir vi en oversikt over digitale sikkerhetshendelser i sektoren i 2024. Vi ser på hvilke typer hendelser virksomhetene har registrert og hvilke avvik i behandlingen av personopplysninger som ble varslet til Datatilsynet.

Det generelle trusselbildet

Trusselbildet for norske virksomheter preges av økt geopolitisk spenning og et forverret internasjonalt samarbeidsklima. Etterretningstjenesten peker på at Norge må forvente økt aktivitet fra statlige og ikke-statlige aktører som søker å påvirke nasjonale interesser (E-tjenesten, 2025).

Trusler og trusselaktører

Med trussel mener vi en mulig årsak til en hendelse som kan føre til skade på et system eller en organisasjon (ISO/IEC 27000:2018).

Med trusselaktør mener vi enkeltindivider og grupper som utgjør en konkret trussel mot en enkeltperson, en virksomhet eller et datasystem (Kripos, 2025, s. 104).

Politiets sikkerhetstjeneste (PST) mener at etterretningstrusselen mot Norge er skjerpet i 2025, med Russland og Kina som de mest aktive aktørene (PST, 2025).[3] Disse statene benytter et bredt spekter av virkemidler for å innhente sensitiv informasjon og påvirke norske beslutningsprosesser.

Også Nasjonal sikkerhetsmyndighet (NSM) beskriver det digitale risikobildet som stadig mer komplekst og krevende, og peker på at digitaliseringen har skapt nye sikkerhetsutfordringer, blant annet knyttet til kunstig intelligens (NSM, 2025a, s. 26-30).

[3] PST forventer også etterretningsaktivitet fra Iran og Nord-Korea i 2025 (PST, 2025, s. 11-27).

NSM understreker at virksomheter må forvente forsøk på kompromittering gjennom hele verdikjeden – inkludert leverandører og samarbeidspartnere.

I 2024 har NSM observert en økning i antallet nettfiskekampanjer. I tillegg peker NSM på at det er særlig tre metoder som trusselaktører benytter seg av: «angriper-i-midten», [4] utnyttelse av nulldagssårbarheter[5] og løsepengevirus[6] (NSM, 2025a, s. 26). Dette ser ut til å samsvare med internasjonale trender. Verizon (2025) rapporterte for eksempel om økt utnyttelse av kjente sårbarheter, nulldagssårbarheter og løsepengevirus.

Videre oppgir Kripos at trusselen fra nettkriminelle grupper mot norske virksomheter økte i 2024 (Kripos, 2025). De fleste angrepene som Kripos har registrert ble utført av profittmotiverte aktører, og rammer ofte små og mellomstore virksomheter.

Spesielt om forsknings- og høyere utdanningssektoren

For virksomhetene i høyere utdanning og forskning er det spesielt to typer aktører som utfordrer sikkerheten gjennom digitale angrepsmetoder: statlige etterretningstjenester og nettkriminelle grupper.[7] I tillegg kan egne ansatte utgjøre en trussel gjennom ubevisste eller bevisste avvik fra interne sikkerhetsrutiner.

Etterretningstjenester og statlig støttede nettkriminelle grupper (Advanced Persistent Threats - APT) utgjør en trussel mot virksomhetene i høyere utdanning og forskning (PST, 2025, s. 18-23). Disse aktørene antas å være ute etter sensitiv teknologi og

---

[4] Angriper-i-midten (eng: adversary-in-the-middle) er en type phishingangrep hvor en trusselaktør opererer mellom offeret og en påloggingsnettside, slik at angriperen kan lure til seg passord og komme seg forbi flerfaktorautentisering (NSM, 2025a, s. 29-30).

[5] Nulldagssårbarheter er tidligere ukjente sikkerhetshull i programvare, IT-utstyr eller -systemer, og som man på oppdagelsestidspunktet har hatt null dager på å utbedre (Ibid.).

[6] Løsepengeangrep er dataangrep hvor en trusselaktør tar seg inn i virksomheters datanettverk for å sperre tilgangen til systemer og data. Aktøren kan også stjele data. Deretter presses virksomhetene for penger i bytte mot løfter om at tilgangen til systemer og data vil bli gjenopprettet, eventuelt at data som er stjålet ikke vil bli publisert eller solgt (Ibid.).

[7] «Hacktivister» er trusselaktører som bruker ulike digitale angrepsmetoder for å fremme et politisk budskap. Nettkriminelle grupper er typisk motivert av økonomisk vinning. For mer om ulike trusselaktører, se Cyberkriminalitet 2025 s. 104-106.

kunnskap som sektoren besitter, spesielt innen forsknings- og teknologiområder som PST (2025 s. 19) fremhever i sin nasjonale trusselvurdering.[8]

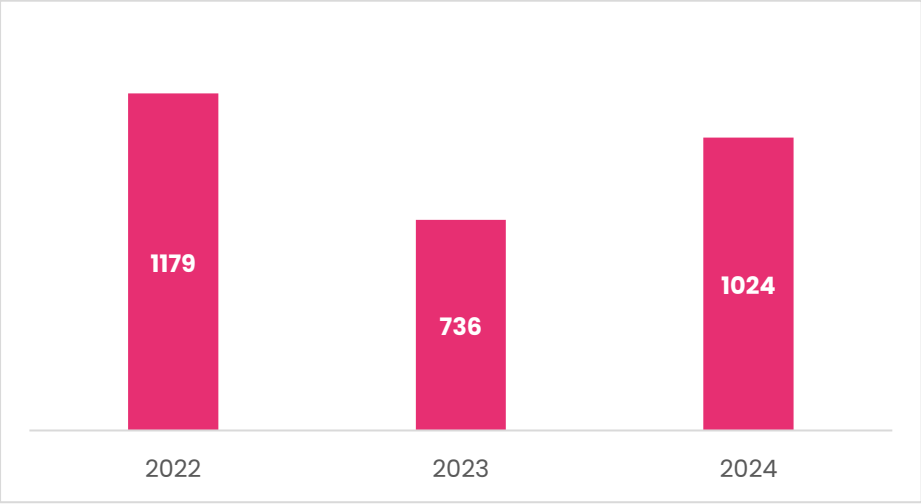
Kunstig intelligens (KI) i cyberangrep

NSM mener at trusselaktørene kan styrke sin kompetanse og kapasitet ved bruk av KI, blant annet for å kompensere for manglende teknisk kompetanse (NSM 2025a, s. 36). Også Kripos (2025, s. 97) påpeker at bruk av KI skjerper trusselbildet i samfunnet.

Google sier at trusselaktører bruker KI til blant annet koding av skadevare og generering av nettfiskeeposter (Google Threat Intelligence Group, 2025). Verizon (2025, s. 13) rapporterer om at omfanget av KI-generert tekst i nettfiskeeposter kan ha doblet seg de to siste årene.

Rapporterte hendelser

Digitale sikkerhetshendelser som virksomhetene i sektoren registrerer, gir viktig informasjon om trusselbildet. Digitaliseringen i sektoren – hvor kjerneoppgaver blir stadig mer avhengig av IT-systemer, -tjenester og datanettverk – betyr at slike hendelser berører både samfunnssikkerhet, nasjonal sikkerhet, informasjonssikkerhet og personvern.



Figur 1: Informasjonssikkerhetshendelser og -brudd 2022-2024

Figur 1 viser utviklingen i antall digitale sikkerhetshendelser hos universitetene i Oslo, Bergen, Trondheim og Tromsø de tre siste årene. Som vi ser, har antallet registrerte

[8] Bioteknologi, materialteknologi og metallurgi, kjernefysikk, kryptografi, kvanteteknologi, nanoteknologi, romfart og fremdriftsteknologi, sensor- navigasjonsteknologi, robotikk og autonomi, og mikroelektroniske systemer.

hendelser økt fra 2023 til 2024, men er likevel noe lavere enn i 2022. Av de øvrige 24 virksomhetene som kartlegges hvert år, oppga tre av dem at de ikke hadde registrert digitale sikkerhetshendelser i 2024.

Også cybersikkerhetssenteret hos Sikt rapporterte om en økning i antall registrerte sikkerhetshendelser og sårbarheter hos sine kunder i 2024.

Cybersikkerhetssenteret for forskning og utdanning (eduCSC) [9]

Cybersikkerhetssenteret hos Sikt opplyste om en økning på 25 prosent i antall registrerte sikkerhetshendelser og sårbarheter fra 2023 og 2024.

Av aktuelle trusler fremhever eduCSC datainnbrudd hvor «angriper-i-midten»-teknikker benyttes. Målrettede nettfiskeangrep er en annen trussel i sektoren. EduCSC påpeker at innføring av nettfiskeresistent autentisering vil bidra til å redusere risikoen som disse truslene innebærer.

I likhet med i fjor, mener eduCSC at tjenestenektangrep (DDoS-angrep) er en viktig trussel i forsknings- og høyere utdanningssektoren, og at utpressingsangrep, særlig løsepengevirus, er en tilbakevendende trussel.

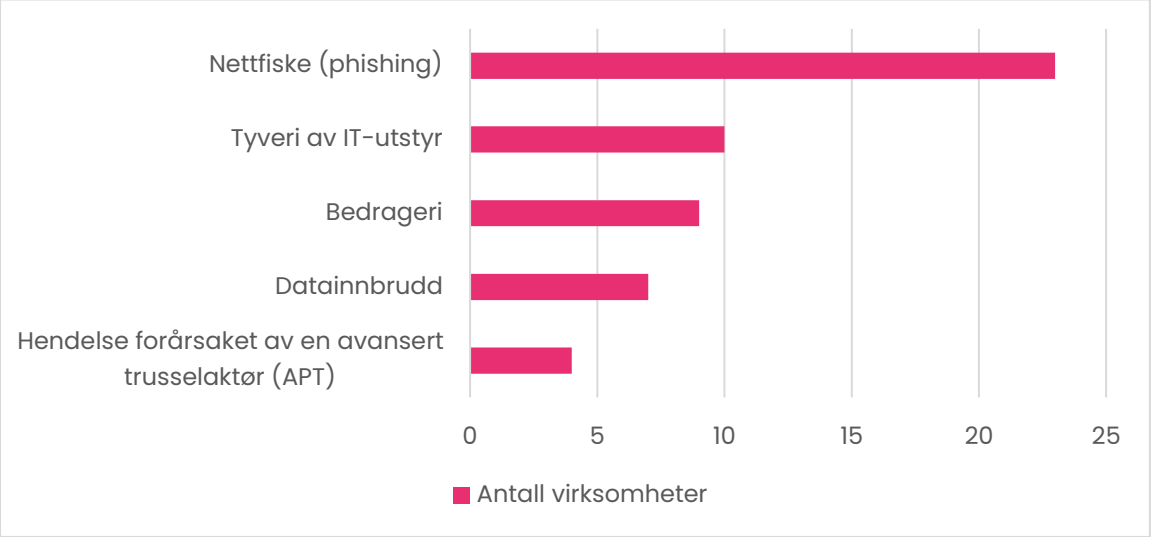
Endringene i 2024, både hos de fire utvalgte universitetene og hos Sikt, indikerer at trusselbildet i sektoren er noe skjerpet sammenliknet med 2023. Det sammenfaller i så fall med EOS-tjenestenes vurdering av utviklingen i det generelle trusselbildet i samfunnet.

Typer sikkerhetshendelser

I spørreskjemaet ble virksomhetene spurt om hvilke typer digitale sikkerhetshendelser de hadde registrert i 2024. Figuren nedenfor viser de fem vanligste hendelsestypene som virksomhetene rapporterte om. Stolpene i figuren viser antallet virksomheter som oppga at de hadde registrert de ulike hendelsestypene.[10]

[9] Statistikken gjelder i utgangspunktet alle 140 kunder av forskningsnettet, men mesteparten av rapporteringen kommer fra cybersikkerhetssenterets 62 kunder. 27 av de 28 virksomhetene som HK-dir kartlegger inngår i statistikken.

[10] En hendelse kan være sammensatt av flere angrepsmetoder og få ulike konsekvenser, og kan derfor passe inn i flere kategorier.



Figur 2: De fem vanligste digitale sikkerhetshendelsene i 2024

Av figuren ser vi at nettfiske er den vanligste hendelsestypen i 2024. I intervjuene med 10 utvalgte virksomheter ble det rapportert at selv om nettfiske er en vanlig hendelse, er det et fåtall av forsøkene som fører til reelle sikkerhetsbrudd. Fem av virksomhetene oppga at de hadde opplevd både nettfiske og datainnbrudd.[11]

Når det gjelder tyveri av IT-utstyr, handler det om innbrudd i virksomhetenes lokaler eller tyveri på arbeidsplassen/studiestedet, for eksempel fra lesesaler. Ingen av de 10 virksomhetene som ble intervjuet opplyste at tyveri av IT-utstyr hadde ført til kompromittering av sensitiv informasjon. Begrunnelsen var at virksomhetene hadde innført kryptering av lokal lagring.

Hendelsene som er kategorisert som bedrageri handler om svindelforsøk av typen direktør- eller fakturasvindel. Det ble rapportert at én av disse hendelsene førte til at en ansatt ble lurt til å gjøre innkjøp av et gavekort. Det ble i tillegg rapportert at en trusselaktør hadde tatt kontakt med økonomiavdelingen og utgitt seg for å være leder i virksomheten.[12] Forsøket ble oppdaget og stoppet.

Sikkerhetshendelser som kategoriseres som datainnbrudd i figur 2, handler om kapring av brukerkontoer. Kontokapring fører til at trusselaktøren får tilgang til lokale

[11] Datainnbrudd (sammen med bedrageri) var også blant de vanligste hendelsestypene som ble rapportert fra næringslivet i 2024 (Næringslivets Sikkerhetsråd, 2025, s. 17-18).

[12] Økonomiavdelingen ble bedt om å endre kontonummer for lønnsutbetaling, slik at utbetalingen havnet på trusselaktørens konto.

ressurser og informasjon, for eksempel e-posttjenesten og dokumenter. I enkelte av disse tilfellene har trusselaktøren benyttet seg av «angriper-i-midten»-metoder for å omgå flerfaktorautentisering. Dette er derfor en angrepsmetode som det er viktig at sektoren kjenner til og har evne til å forebygge, oppdage og håndtere.

Avanserte aktører

EOS-tjenestene er særlig opptatt av trusselen fra avanserte aktører (APT)[13], spesielt fra Russland og Kina. Dette er aktører som ofte ønsker å tilegne seg informasjon om forskning og teknologiutvikling innen områder som sektoren jobber med, og som kan ha betydning for nasjonal sikkerhet (se ovenfor).

I 2024 oppga fire virksomheter at de hadde vært utsatt for hendelser forårsaket av avanserte trusselaktører. Hos én av virksomhetene dreide det seg om et tjenestenektangrep (DDoS[14]) mot deres webtjenester. To av de andre virksomhetene oppga at de hadde registrert varsler fra Microsoft Defender som ble kategorisert som APT-alarmer. Den siste virksomheten hadde registrert rekognoseringsaktivitet fra IP-adresser de mistenker kan tilhøre en APT-aktør.

Ut over dette, oppga én virksomhet at den hadde blitt utsatt for flere forsøk på løsepengevirusangrep i 2024.

Avvik på personvernområdet

Trusselbildet i sektoren preges også av hendelser og avvik som kan innebære brudd på personvernet til studenter, ansatte, deltakere i forskning og andre tilknyttede personer. Som tidligere år, har vi spurt de 28 virksomhetene om antall og typer personvernavvik og -hendelser som er varslet til Datatilsynet.

I 2024 oppga 20 virksomheter å ha registrert personvernavvik og -hendelser. Av disse hadde 14 virksomheter vurdert at ett eller flere av avvikene var såpass alvorlige at de var varslingspliktige til Datatilsynet.

---

[13] For mer om avanserte trusselaktører, se for eksempel What is an Advanced Persistent Threat (APT)? | CrowdStrike, sist besøkt 26.05.2025.

[14] Et tjenestenektangrep har til hensikt å hindre tilgang til eller utførelse av digitale tjenester. Angrepet kan gjennomføres ved å overbelaste kommunikasjonsprotokoll, applikasjon, nettverkskapasitet, maskinvare eller andre ressurser (NSM, 2023). Se for eksempel Håndtering av personvernet ved digitale angrep | Datatilsynet, sist besøkt 26.05.2025.

Hos de 14 virksomhetene som rapporterte om varslingspliktige avvik, ble det totalt sendt inn 57 varsler til Datatilsynet i 2024. Dette er en økning på ni saker sammenlignet med 2023, og en økning på 31 saker sammenliknet med 2022.[15]

Økningen kan bety at personvernet i forsknings- og høyere utdanningssektoren er under noe større press i 2024 enn for et par år siden. På den annen side kan økningen skyldes at virksomhetene har blitt flinkere til å oppdage og varsle om avvik. Det kan i så fall bety at personvernet er styrket fordi problemer avdekkes i større grad enn tidligere og korrigerende tiltak iverksettes. Men det kan også tenkes at noe av økningen de to siste årene skyldes tilfeldige variasjoner.

Personvern i forskning

Sikt sin personverntjeneste bistår institusjonene med å sørge for at behandling av personopplysninger i forskningsprosjekter skjer i tråd med personvernregelverket.[16]

I 2024 registrerte personverntjenesten hos Sikt en økning i alle typer avvik i forskningsprosjekter hvor personopplysninger behandles. Avvikene handlet typisk om at studenter eller forskere hadde startet datainnsamlingen uten først å ha registrert forskningsprosjektet hos Sikt, eller andre former for formelle feil.

[15] Blant de 57 sakene som ble varslet til Datatilsynet, var 11 av dem relatert til en feil i Feide. Feilen førte til at en del tjenesteleverandører fikk tilgang til flere personopplysninger enn avtalt, inkludert fødselsnummer til brukere hos andre virksomheter. For mer informasjon om hendelsen, se Enkelte tjenester har fått utdelt fødselsnumre uten avtale| Feide, sist besøkt 06.03.2025.

[16] Tjenestene omfatter blant annet digitale verktøy som meldeskjema og institusjonsportalen, se Personverntjenester, sist besøkt 26.03.2025.

Kapittel 3: Sikkerhetsledelse og -styring

Virksomhetene skal iverksette planlagte og systematiske tiltak for å forebygge, oppdage og håndtere trusler mot sikkerheten og personvernet drøftet i forrige kapittel. Det innebærer at virksomhetene etablerer styringssystem for sikkerhet etter sikkerhetsloven og ledelsessystem for informasjonssikkerhet,[17] som blant annet ivaretar sikkerheten til personopplysninger.[18] Styrings- og ledelsessystemene beskriver mål og prioriteringer for sikkerhetsarbeidet, hvordan arbeidet er organisert og hvilke rutiner og planer som gjelder.

Styrings- eller ledelsessystemet skal være forankret hos toppledelsen og der hvor det er aktuelt på styrenivå.

Det skal i tillegg etableres planlagte og systematiske tiltak innen samfunnssikkerhet og beredskap. Disse tiltakene drøftes særskilt i kapittel 5 og 6.

I dette kapitlet drøftes i hvilken grad virksomhetene har etablert og iverksatt styringssystem for sikkerhet og ledelsessystem for informasjonssikkerhet. Vi ser også på om styringssystemet for sikkerhet er samordnet med ledelsessystemet for informasjonssikkerhet, og om sikkerhetsledelse inngår i den øvrige virksomhetsstyringen.[19]

Styringssystem for sikkerhet

Styringssystemet for sikkerhet omfatter alle aktiviteter som inngår i det forebyggende sikkerhetsarbeidet (jf. fotnote 17 nedenfor). Et systematisk og helhetlig arbeid med sikkerhet er derfor avhengig av at et slikt styringssystem er etablert og fungerer etter hensikten.

---

[17] 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. For mer om styringssystem for sikkerhet, se Etabler styringssystem for sikkerhet - Nasjonal sikkerhetsmyndighet, sist besøkt 03.06.2025. For mer om ledelsessystem for informasjonssikkerhet, se Internkontroll/ styringssystem/ ledelsessystem for informasjonssikkerhet | Digdir, sist besøkt 03.06.2025.

[18] Jf. også reglene i e-forvaltningsforskriften om styring og kontroll på informasjonssikkerhetsområdet.

[19] I styringsdokumentet for sikkerhet og beredskap stiller departementet krav om samordning av styrings- og ledelsessystemer.

Som vi ser av figur 3, svarte litt over halvparten av virksomhetene (16) bekreftende på spørsmål i spørreskjemaet om de har etablert et styringssystem for sikkerhet. De øvrige virksomhetene (12) oppga at de ikke hadde et fullverdig styringssystem på tidspunktet for årets kartlegging.

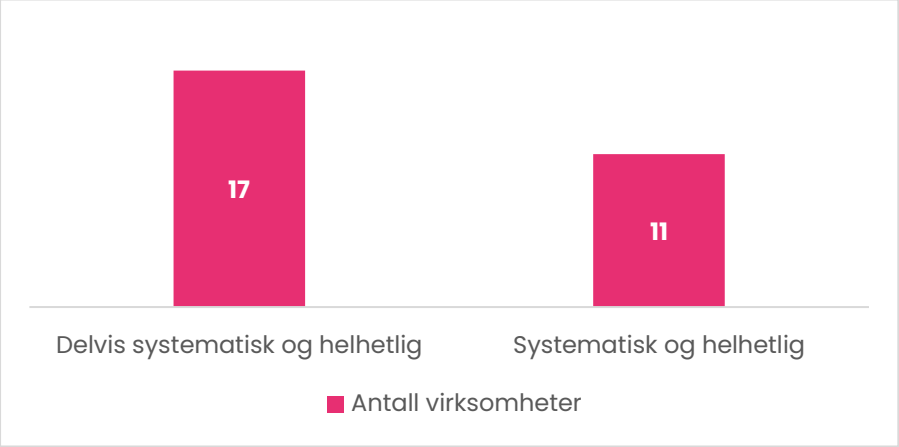
Figur 3: Etablering av styringssystem for sikkerhet

Hos de virksomhetene som i stor eller svært stor grad mente at styringssystemet var etablert, ble det likevel rapportert om enkelte mangler. Åtte av disse 16 virksomhetene oppga for eksempel at de ikke hadde utarbeidet overordnet risikovurdering eller at de ikke hadde beredskaps- og kontinuitetsplaner som omfattet nasjonal sikkerhet.

I intervjudelen av kartleggingen opplyste åtte av de 10 virksomhetene som deltok at de har planer om å starte arbeidet med etablering av et styringssystem for sikkerhet i løpet av 2025.

Ledelsessystem for informasjonssikkerhet

Figur 4 viser hvor mange virksomheter som etter vår vurdering har etablert et fullverdig ledelsessystem for informasjonssikkerhet. Vurderingen er basert på informasjon fra intervjuene og informasjon fra tidligere års kartlegginger av informasjonssikkerhet og personvern.



Figur 4: Etablering av ledelsessystem for informasjonssikkerhet

I 2024 hadde 11 av 28 virksomheter etablert et ledelsessystem for informasjonssikkerhet som fungerer på en god måte innenfor alle deler av kjernevirksomheten. Dette er en økning på to virksomheter sammenlignet med forrige kartlegging. 17 virksomheter hadde i noen grad lyktes med dette. Ingen av virksomhetene er vurdert å ha et lite systematisk og helhetlig ledelsessystem.

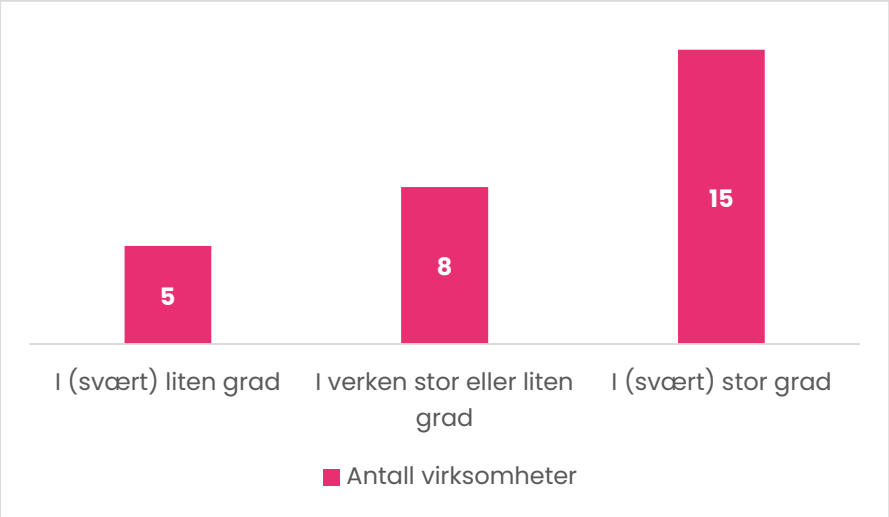
De 17 virksomhetene som delvis har etablert et systematisk og helhetlig ledelsessystem, har enkelte mangler når det gjelder gjennomføring av viktige oppgaver som inngår i ledelsessystemet. Det handler primært om risikostyring av informasjonssikkerheten i IT-løsninger og utarbeidelse av beredskaps- og kontinuitetsplaner for digitale sikkerhetshendelser.

Mangler i implementering og praktisering både av styringssystemer for sikkerhet og ledelsessystemer for informasjonssikkerhet, indikerer at sektoren har behov for fortsatt å styrke systematikken og helheten i sikkerhetsarbeidet. Dette er viktig for at sektoren skal kunne forbedre sin evne til å forebygge, oppdage og håndtere trusler drøftet i forrige kapittel.

Samordning av styrings- og ledelsessystem

I spørreskjemaet ble virksomhetene spurt om de hadde samordnet eller integrert styringssystemet for sikkerhet med ledelsessystemet for informasjonssikkerhet.[20]

[20] Samordning kan innebære flere gevinster. Det kan for eksempel styrke systematikken i det samlede sikkerhetsarbeidet, gi bedre oversikt over hvilke krav og forventninger ledelsen stiller til dette arbeidet og bidra til mer effektiv utnyttelse av ressurser på tvers av sikkerhetsområder.



Figur 5: Samordning av styringssystemet for sikkerhet og ledelsessystemet for informasjonssikkerhet

I figuren ser vi at et knapt flertall av virksomheter (15) svarer at styrings- og ledelsessystemet i høy eller relativt høy grad er samordnet med hverandre. Samtidig er det 13 virksomheter som i begrenset eller liten grad har gjort dette. Et relativt lite mindretall (5) oppgir at de i svært liten grad har gjennomført samordningsaktiviteter.

På bakgrunn av intervjudata fra årets og tidligere års kartlegginger, kan det virke som at samordningen skjer ved at virksomhetene legger ledelsessystemet for informasjonssikkerhet til grunn for samordningsarbeidet. Det innebærer at ledelsessystemet for informasjonssikkerhet utvides til også å omfatte de øvrige sikkerhetsområdene (samfunnssikkerhet og beredskap, og nasjonal sikkerhet).

Sikkerhetsledelse og virksomhetsstyring

Toppledelsen i virksomhetene skal lede sikkerhetsarbeidet. Det innebærer blant annet at ledelsen stiller krav til, følger opp og sørger for tilstrekkelig med ressurser til arbeidet. Det innebærer i tillegg at sikkerhetsledelse inngår som en del av virksomhetsstyringen.

Resultatene fra spørreskjemaundersøkelsen indikerer at forsknings- og høyere utdanningssektoren i begrenset grad har lyktes med å integrere sikkerhetsledelse i den øvrige virksomhetsstyringen. Det kommer til uttrykk ved at et flertall av virksomhetene – 16 av 28 – rapporterte om at sikkerhetsledelse enten ikke inngår i virksomhetsstyringen på en god nok måte eller at den ikke inngår i det hele tatt. De siste 12 virksomhetene mente at sikkerhetsledelse er inkludert i virksomhetsstyringen.

Blant de 10 virksomhetene som ble intervjuet, mente et par av dem at sikkerhetsledelse er en integrert del av virksomhetsstyringen. De begrunnet dette med at sikkerhetsområdet nå inngår i plan- og budsjettarbeidet og at status på sikkerhetsområdet rapporteres til toppledelsen. Det ble også begrunnet med at det gis opplæring i relevante oppgaver og rutiner.[21]

Resultatene ovenfor kan tyde på at viktige deler av sektoren har utfordringer med å få sikkerhetsledelse til å bli en del av virksomhetsstyringen. Resultatene indikerer også at sektoren har behov for ytterligere samordning av aktiviteter på tvers av sikkerhetsområder. Dette kan bidra til at systematikken i arbeidet forbedres og at knappe ressurser utnyttes på en mer hensiktsmessig måte.

[21] Opplæring skjer for eksempel ved onboarding av nye medarbeidere og ledere, eller at sikkerhet og beredskap er tema som inngår i lederopplæringen.

Kapittel 4: Oversikt over verdier

Innledning

Vellykket implementering av styringssystemer for sikkerhet og ledelsessystemer for informasjonssikkerhet, avhenger av at de konkrete sikkerhetsoppgavene som inngår i styrings- og ledelsessystemene blir gjennomført som planlagt.

I dette og de to neste kapitlene gir vi en oversikt over i hvilken grad virksomhetene i forsknings- og høyere utdanningssektoren faktisk utfører sentrale sikkerhetsoppgaver. Det handler om å ha oversikt over egne informasjonsverdier, gjennomføring av risikovurderinger og iverksetting av risikoreduserende tiltak (kapittel 5), og håndtering av hendelser og styrking av beredskapsarbeidet (kapittel 6).

Disse oppgavene følger av kravene i departementets styringsdokument for sikkerhet og beredskap, og av tilsvarende krav i policy for informasjonssikkerhet og personvern.

Betydningen av verdioversikt

For å kunne beskytte virksomheten mot sikkerhetstrusler og brudd på personvernet, må den først ha oversikt over hvilke informasjonsverdier som virksomheten forvalter. Deretter må den vurdere hvor beskyttelsesverdige ulike typer informasjonsverdier er. Oversikt over beskyttelsesverdige informasjonsverdier er avgjørende for blant annet å kunne gjennomføre gode risikovurderinger og å prioritere riktige sikringstiltak.

Kort om verdier

Med informasjonsverdier menes blant annet personopplysninger, forskningsdata og kunnskap, IT-systemer, nettbaserte tjenester og personlig IT-utstyr. Begrepet inkluderer også informasjon om hvordan disse verdiene er beskyttet.

Virksomhetene må i tillegg etterleve en rekke andre regelverk som har til hensikt å beskytte liv, helse og materielle verdier.[22] De må derfor også ha oversikt over disse typene verdier.

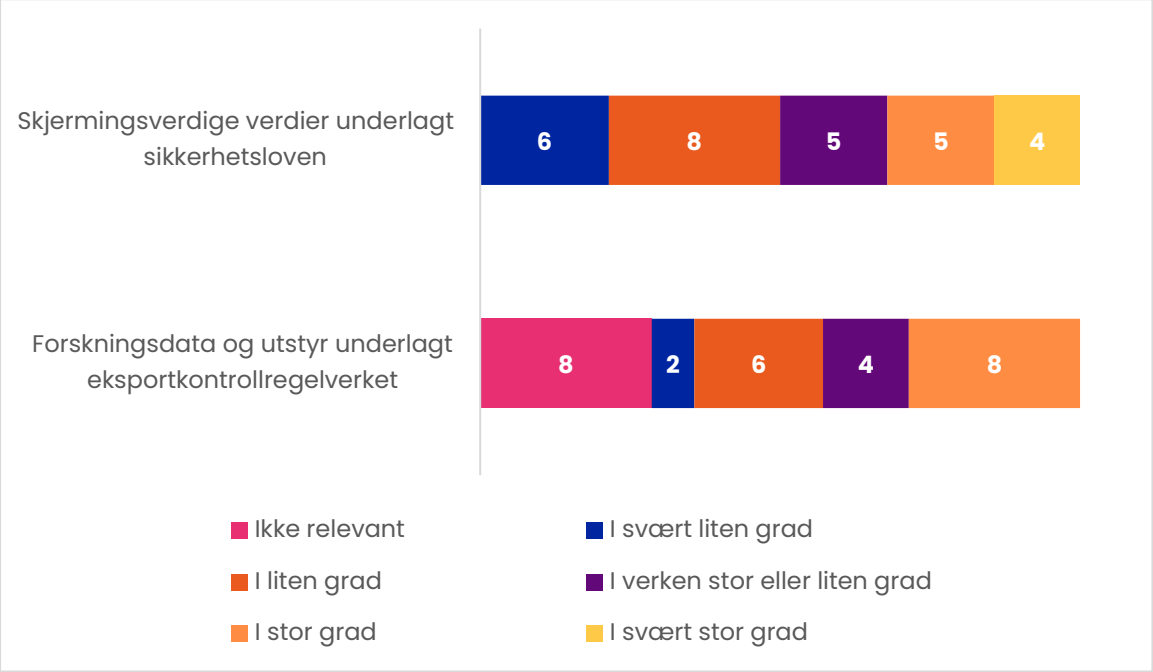
Nedenfor ser vi nærmere på i hvilken grad virksomhetene i forsknings- og høyere utdanningssektoren har oversikt over verdier som er underlagt sikkerhetsloven og eksportkontrollregelverket.

[22] For eksempel regelverk knyttet til brannvern (forskrift om brannforebygging), helse, miljø og sikkerhet (internkontrollforskriften), arbeid med kjemiske og biologiske risikofaktorer og andre arbeidsmiljøforhold (forskrift om utførelse av arbeid), smittevern (smittevernloven) og helseberedskap (helseberedskapsloven).

Vi ser også på om virksomhetene har oversikt over personopplysninger som de forvalter, og hvilke land utenfor EU/EØS som opplysningene overføres til.

Sikkerhetsloven og eksportkontrollregelverket

Sektoren forvalter verdier som krever særskilt beskyttelse i henhold til sikkerhetsloven, eksportkontrollregelverket og internasjonale sanksjoner,[23] blant annet innenfor teknologiområder som nanoteknologi, kryptografi og sensorteknologi. Figur 6 viser virksomhetenes svar på spørsmål i spørreskjemaet om de har oversikt over slike verdier.



Figur 6: Oversikt over verdier underlagt sikkerhetsloven og eksportkontrollregelverket

Her fremgår det at 9 av 28 virksomheter mener at de i stor elle svært stor grad har oversikt over verdier som skal skjermes i henhold til sikkerhetsloven. 19 virksomheter oppgir at oversikten over skjermingsverdige verdier enten er mangelfull eller svært mangelfull.

Figuren viser i tillegg at 12 virksomheter mener at de i stor elle svært stor grad har oversikt over verdier underlagt eksportkontrollregelverket. Av de 16 virksomhetene som oppgir at oversikten er mangelfull eller svært mangelfull, er det grunn til å tro at flere av dem forvalter verdier som kan være omfattet av eksportkontrollregelverket.

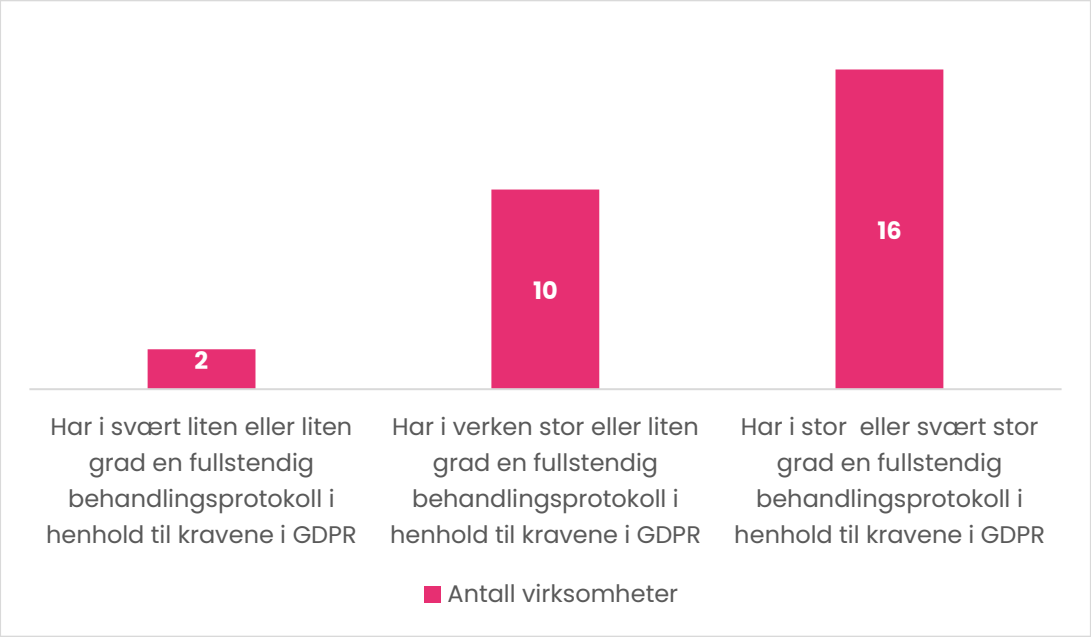
[23] Jf. lov om gjennomføring av internasjonale sanksjoner med forskrifter.

Svarene tyder på at flertallet av virksomhetene i sektoren har behov for å styrke arbeidet med verdioversikt for å få bedre kontroll med hvilke verdier de forvalter, både i henhold til sikkerhetsloven og eksportkontrollregelverket. Deretter vil de trolig også ha behov for å vurdere hvilke nye sikringstiltak som kan være nødvendige for å beskytte disse verdiene.

Personopplysninger (behandlingsprotokoll)

Personvernregelverket – personopplysningsloven og personvernforordningen (GDPR) – stiller krav om at virksomhetene fører en behandlingsprotokoll. Protokollen skal blant annet inneholde oversikt over kategorier av personopplysninger som virksomhetene behandler og hvem opplysningene gjelder, for eksempel studenter og ansatte (Datatilsynet, 2024).

Figur 7 viser hvor mange av de 28 virksomhetene som i spørreskjemaet svarte at de har en fullstendig behandlingsprotokoll i henhold til kravene i GDPR.[24]



Figur 7: Status for behandlingsprotokoll 2024

Her ser vi at et flertall av virksomhetene (16) oppgir at de har en tilfredsstillende protokoll som inneholder oversikter over hvilke kategorier personopplysninger de forvalter og hvem opplysningene gjelder. De siste 12 virksomhetene oppgir at

[24] Vi har lagt til grunn at de virksomhetene som svarte «i stor grad» eller «i svært stor grad» på dette spørsmålet har få mangler og avvik i sine behandlingsprotokoller.

oversikten er mangelfull, hvorav to av dem mener at den er svært mangelfull. Disse resultatene samsvarer med intervjudata fra tidligere kartlegginger (HK-dir, 2024a).

De 21 universitetene og høyskolene ble spurt om det er variasjoner i kvaliteten på oversikten over personopplysninger på tvers av virksomhetsområder.[25] I likhet med tidligere kartlegginger, oppgir universitetene og høyskolene å ha best oversikt over personopplysninger i forskning, etterfulgt av administrasjonen. Undervisning er det virksomhetsområdet hvor oversikten fremstår som mest mangelfull.

Selv om det er variasjoner mellom virksomhetsområder, indikerer resultatene at sektoren har bedre oversikt over personopplysninger enn informasjonsverdier underlagt sikkerhetsloven og eksportkontrollregelverket. Det kan skyldes at sektoren har jobbet lengre med etablering og oppdatering av oversikter over personopplysninger (behandlingsprotokoller) enn når det gjelder tilsvarende oversikter over skjermverdige informasjonsverdier underlagt sikkerhetsloven og eksportkontrollregelverket. Virksomhetene kan derfor ha ekstra behov for å styrke arbeidet med kartlegging av denne typen informasjonsverdier, spesielt innen sensitive forsknings- og kunnskapsområder.

Internasjonale overføringer

Virksomhetenes behandlingsprotokoll skal inneholde oversikt over overføringer av personopplysninger til tredjeland, det vil si land utenfor EU/EØS, spesielt USA. Dette temaet ble satt på agendaen etter at Datatilsynet rådet virksomheter som overfører personopplysninger til USA, for eksempel ved bruk av amerikanske skytjenester, om å forberede seg på at dagens regler for overføringer til USA før eller siden vil utfordres i EU-domstolen (Datatilsynet, 2025).

I spørreskjemaet ble virksomhetene spurt om de har oversikt over overføringer til tredjeland. 15 av 28 virksomheter oppga at de har tilfredsstillende oversikt over slike overføringer. De resterende 13 virksomhetene svarte at de ikke har god nok oversikt over hvilke land personopplysninger overføres til. Disse virksomhetene kan stå i fare for å bryte sentrale bestemmelser i personvernregelverket dersom USAs status som godkjent mottakerland skulle endre seg.

[25] Dette spørsmålet var i mindre grad relevant for direktorater uten undervisnings- eller forskningsoppgaver. Vi fokuserer derfor på universitetene og høyskolene.

Resultatene tyder på at en stor andel av virksomhetene har behov for å undersøke dataflyten i sine IT-løsninger, og å vurdere nærmere om eventuelle overføringer av personopplysninger til tredjeland skjer på riktig måte.

Kapittel 5: Risikostyring og sårbarheter

Innledning

Risikostyring er det mest sentrale enkeltelementet i styringssystemer for sikkerhet og i ledelsessystemer for informasjonssikkerhet. Dette er også krav som følger av lovverket, blant annet av sikkerhetsloven og GDPR, og av departementets styringsdokument for sikkerhet og beredskap (Kunnskapsdepartementet, 2025).

Risikostyring innebærer å identifisere og vurdere risikoen for hendelser som kan true skjermingsverdig informasjon, personopplysninger og andre verdier i sektoren, spesielt liv, helse og viktige materielle verdier. Videre skal det gjennomføres tiltak for å redusere risikoen for hendelser med uakseptabel høy risiko. Virksomhetene skal følge opp tiltakene og vurdere om de har gitt den forventede effekten.

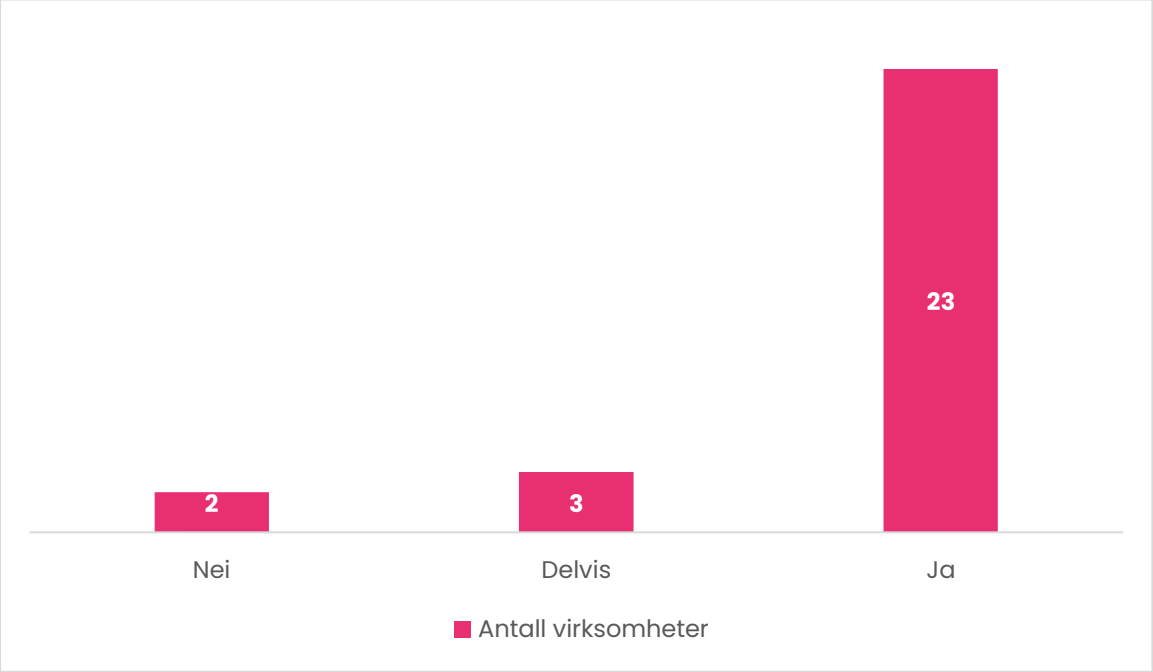
I dette kapitlet ser vi først på hvordan sektoren arbeider med risikovurderinger. Deretter gir vi en oversikt over hvilke typer sikringstiltak som de 28 virksomhetene rapporterte at de iverksatte i 2024 for å styrke sikkerheten og ivareta personvernet.

Til slutt ser vi på hvilke sårbarheter som virksomhetene mener det er viktig å utbedre i det videre sikkerhetsarbeidet.

Overordnet risikovurdering (ROS-analyse)

En viktig del av risikostyringen, er at virksomhetene hvert år gjennomgår og ved behov reviderer, en overordnet vurdering av risikoen for hendelser som kan true virksomhetens verdier. Hendelsene som analyseres kan true samfunnssikkerheten, den nasjonale sikkerheten og informasjonssikkerheten, inkludert sikkerheten til personopplysninger.

Figur 8 viser hvor mange av de 28 virksomhetene som i spørreskjemaet svarte at de har eller ikke har utarbeidet en slik risikovurdering.



Figur 8: Utarbeidet overordnet risikovurdering

Vi ser at et stort flertall av virksomhetene (23) rapporterte om at de har utarbeidet en overordnet risikovurdering. Dermed er det bare noen få virksomheter (5) som delvis eller ikke i det hele tatt har utarbeidet en overordnet risikovurdering. Resultatene i figur 8 kan tyde på at arbeidet med overordnede risikovurderinger er relativt godt institusjonalisert i sektoren.

Hos de 23 virksomhetene som svarte at de har utarbeidet en overordnet risikovurdering, fremkom det imidlertid at vurderingene hadde noen mangler. Manglene dreide seg om at enkelte av virksomhetene ikke hadde vurdert risiko for uønskede hendelser innenfor samtlige sikkerhetsområder (samfunnssikkerhet og beredskap, nasjonal sikkerhet, informasjonssikkerhet og personvern). Særlig hendelser som kan ha betydning for nasjonal sikkerhet var mangelfullt vurdert. Disse virksomhetene har derfor et forbedringspotensial når det gjelder helhetlig risikostyring, det vil si vurdering av risiko for hendelser innenfor alle de ulike områdene som de har ansvaret for.

Virksomhetene ble også spurt om hvor ofte de reviderer og oppdaterer sine overordnede risikovurderinger. Her svarte 20 av virksomhetene at dette skjer årlig. Åtte virksomheter svarte at de kun delvis gjør dette hvert år. Dette kan skyldes at virksomhetene har ulikt behov for å oppdatere sine risikovurderinger fra år til år.

Tiltaksplaner og tiltaksgjennomføring

Virksomhetene ble spurt om de har utarbeidet planer for håndtering av sikkerhetshendelser som, ifølge den overordnede risikovurderingen, har uakseptabel høy risiko.

Her svarte 22 virksomheter at de har utarbeidet tiltaksplaner på bakgrunn av den overordnede vurderingen. De seks siste virksomhetene rapporterer om at de kun delvis har utarbeidet slike planer.

Samtidig oppga 17 virksomheter at de jevnlig følger opp planene for å få oversikt over status på innføring av tiltak. De øvrige 11 virksomhetene mente at tiltaksplanene bare delvis eller ikke i det hele tatt blir fulgt opp.

I intervjuene fremkom det at manglene i risikostyringen skissert ovenfor, kunne skyldes flere forhold. Det ble blant annet pekt på at manglende ressurser kunne føre til at tiltaksplaner ikke blir utarbeidet eller at planlagte tiltak ikke blir gjennomført.

Resultatene antyder at deler av sektoren har behov for å styrke risikostyringen, spesielt at det utarbeides tiltaksplaner for sikkerhetshendelser med høy risiko og at risikoreduserende tiltak faktisk gjennomføres.

Tiltakstyper

Både i spørreskjemaet og i intervjuene med 10 utvalgte virksomheter, spurte vi om hvilke typer risikoreduserende tiltak de hadde iverksatt i 2024.

Nedenfor gjør vi rede for hvilke hovedtyper tiltak som virksomhetene rapporterte om. Vi har delt tiltakene i fire kategorier: kapasitetstiltak, organisatoriske tiltak, tekniske tiltak og pedagogiske tiltak.

Kapasitetstiltak

Som i tidligere kartlegginger, ba vi virksomhetene oppgi hvor mange årsverk de har avsatt til arbeidet med informasjonssikkerhet og personvern i 2024.

Om årsverksoversikten

Årsverksoversikten inkluderer altså kun årsverk som helt eller delvis er avsatt til arbeidet med informasjonssikkerhet og personvern. Vi mangler derfor en tilsvarende oversikt over årsverk innenfor de øvrige delene av sikkerhets- og beredskapsarbeidet.

Vi vil gi et mer helhetlig bilde av årsverksinnsatsen på sikkerhetsområdet i fremtidige kartlegginger.

Samlet sett økte årsverksinnsatsen med ca. 0,5 årsverk i 2024. Det ser derfor ut til at kapasitetsveksten har stabilisert seg sammenlignet med økningen på 14,1 årsverk i fra 2022 til 2023.

17 virksomheter rapporterte at de har kjøpt tjenester fra private aktører for å styrke kapasiteten på informasjonssikkerhets- og personvernområdet. Hvor mye den innleide kapasiteten utgjorde i årsverk, har vi ikke informasjon om.

Ut over egeninnsats og innleid kapasitet fra private aktører, benytter virksomhetene også personverntjenester fra Sikt[26] og informasjonssikkerhetstjenester fra sektorens cybersikkerhetssenter (eduCSC).

Organisatoriske tiltak

De organisatoriske tiltakene som virksomhetene rapporterte om i 2024, handlet i stor grad om revisjoner av styrings- og ledelsessystemet, kartlegging av IT-systemer og programvare, og revidering av rutiner for sikker behandling av personopplysninger. Ferdigstilling av behandlingsprotokoller og revidering av beredskaps- og kontinuitetsplaner var andre relativt vanlige tiltak i sektoren i 2024.[27]

Flere virksomheter oppga også at de har iverksatt tiltak for å forbedre styringen av tilganger til beskyttelsesverdige informasjonsverdier. Eksempler på slike tiltak inkluderte revisjon av retningslinjer for tilgangsstyring, innstramming av rettigheter for administratorer, og endrede rutiner for sletting av brukerkontoer.

Tekniske tiltak

Virksomhetene rapporterte om flere viktige tekniske sikringstiltak i 2024. Det gjaldt spesielt innføring av totrinnsinnlogging og styrking av sikkerhetsbarrierer i lokale

[26] For mer informasjon om Sikts personverntjenester, se Personverntjenester, sist besøkt 26.05.2025. Norsk senter for informasjonssikring og Sikresiden er andre offentlige aktører som tilbyr informasjonssikkerhets- og personverntjenester i høyere utdanning- og forskningssektoren. Se https://norsis.no/ og https://www.sikresiden.no/, sist besøkt 03.02.2025.

[27] I HK-dirs undersøkelse av status for arbeidet med orden i eget hus i kunnskapssektoren, ble det rapportert om at flere av universitetene og høyskolene har kartlagt behandling av personopplysninger og hvilke tilganger som er gitt i IT-systemer. Se Orden i eget hus i kunnskapssektoren | HK-dir s. 9, sist besøkt 28.03.2025.

datanettverk. To virksomheter opplyste at innføringen av felles identitets- og tilgangsstyring (IAM) fra Sikt, hadde bidratt til forbedret tilgangsstyring.[28]

Det ble også rapportert om en rekke tekniske tiltak for å styrke evnen til å oppdage og håndtere digitale sikkerhetshendelser. Eksempler på slike tiltak var penetrasjonstester av sikkerheten i IT-systemer, videreutvikling av interne sårbarhetsskann og oppsett av sikkerhetstjenester fra Microsoft (Defender).[29]

Pedagogiske tiltak

Til sist opplyste virksomhetene at de også i 2024 hadde iverksatt enkelte pedagogiske tiltak.

Disse tiltakene handlet, for det første, om opplæring og kompetanseheving rettet mot medarbeidere med særskilte roller og ansvar i sikkerhets- og personvernarbeidet. For det andre, handlet det om bevisstgjøringstiltak rettet mot øvrige ansatte og studenter. Dette var primært informasjon eller informasjonskampanjer som hadde til hensikt å øke sikkerhetsbevisstheten hos brukerne av IT-systemer og -tjenester, og å opplyse dem om digitale trusler.

Vanlige sårbarheter

Vi ba de 10 virksomhetene som vi intervjuet om å beskrive de viktigste sårbarhetene som gjensto etter at tiltakene skissert ovenfor var gjennomført.[30]

Samlet sett handlet de vanligste gjenstående sårbarhetene om mangler med hensyn til verdioversikter og gjennomføring av risikovurderinger. Andre eksempler på sårbarheter som ble nevnt, gjaldt beredskaps- og kontinuitetsplaner og evaluering av beredskapsøvelser. Vi kommer tilbake til flere av disse sårbarhetene i neste kapittel.

Ser vi spesifikt på samfunnssikkerhet og beredskap, og nasjonal sikkerhet, handlet sårbarhetene i stor grad om manglende kompetanse og kapasitet. I tillegg ble

---

[28] Felles identitets- og tilgangsstyring (IAM) skal sikre at brukere får riktig tilgang til digitale ressurser, til rett tid og med riktig sikkerhetsnivå. For mer informasjon om tjenesten, se Identitets- og tilgangsstyring – IAM, sist besøkt 06.03.2025.

[29] Enkelte virksomheter oppga at de hadde arbeidet med sikkerhetstiltak som følge av Riksrevisjonens gjennomgang av informasjonssikkerhet i forskningssystemer (Riksrevisjonen, 2024).

[30] Innenfor informasjonssikkerhet og personvern ba vi også alle virksomhetene om å oppgi årsakene til at digitale sikkerhetshendelser og -brudd hadde oppstått.

enkelte organisatoriske sårbarheter nevnt, særlig mangelen på helhetlig sikkerhetsstyring (jf. omtale av status for styrings- og ledelsessystem i kapittel 3).

Når det gjaldt informasjonssikkerhet og personvern, ble et par sårbarheter nevnt særskilt. Det gjaldt manglende oversikt over tilganger i IT-systemer, og liten kapasitet til eller kompetanse om gjennomføring av nødvendige sikringstiltak.

Manglende kjennskap til personvernregelverket blant studenter og forskere, og liten kjennskap til rutiner for melding av uønskede hendelser eller rutineavvik, var andre sårbarheter som det ble opplyst om.

Sårbarheter i arbeidet med personellsikkerhet

Personellsikkerhet handler om å sikre at personer som kan utgjøre en sikkerhetsrisiko, ikke får tilgang til stillinger eller informasjon som kan true nasjonale interesser eller bryte sikkerhetsloven (NSM, 2019).

De 10 virksomhetene vi intervjuet, ble spurt om status for arbeidet med personellsikkerhet. Disse virksomhetene rapporterte om flere sårbarheter i arbeidet. Det gjaldt særlig manglende kompetanse og mangelfulle rutiner og felles praksis i sektoren for sikkerhetsvurderinger ved ansettelser – spesielt når det gjelder personer fra land som Norge ikke har et sikkerhetspolitisk samarbeid med.[31]

Manglene kan føre til at ansettelsesprosessene gjennomføres med utilstrekkelige rutiner for bakgrunnssjekk og identitetskontroll, og mangelfull oppfølging av risikoutsatte medarbeidere, for eksempel ansatte som er av interesse for utenlandsk etterretning.[32] Det kan også medføre andre utfordringer, blant annet når det gjelder håndtering av gjesteforskere.

[31] HK-dir har utarbeidet retningslinjer for ansvarlig internasjonalt kunnskapssamarbeid (AIS). Retningslinjene ble utarbeidet som en oppfølgning av Panoramastrategien (2021-2027) for kunnskapssamarbeid med prioriterte land utenfor Europa (USA, Canada, Brasil, India, Sør-Afrika, Russland, Kina, Japan og Korea). For mer om AIS se Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid-Introduksjon | HK-dir, sist besøkt 30.06.2025.

[32] Sårbarhetssamtaler er et tiltak for oppfølging av slike medarbeidere. For mer informasjon, se Legg til rette for sårbarhetsoppfølging - Nasjonal sikkerhetsmyndighet, sist besøk 30.06.2025.

Kapittel 6: Beredskapsplaner og -øvelser

Innledning

I departementets styringsdokument for sikkerhet og beredskap, stilles det krav om beredskap, kontinuitet og beredskapsøvelser. Det forventes at virksomhetene utarbeider planer for håndtering av uønskede hendelser og krisescenarioer[33] som de har identifisert i den overordnede risikovurderingen (drøftet i forrige kapittel). Det kan for eksempel gjelde hendelser som datainnbrudd, stort personellfravær eller bortfall av strømforsyning.

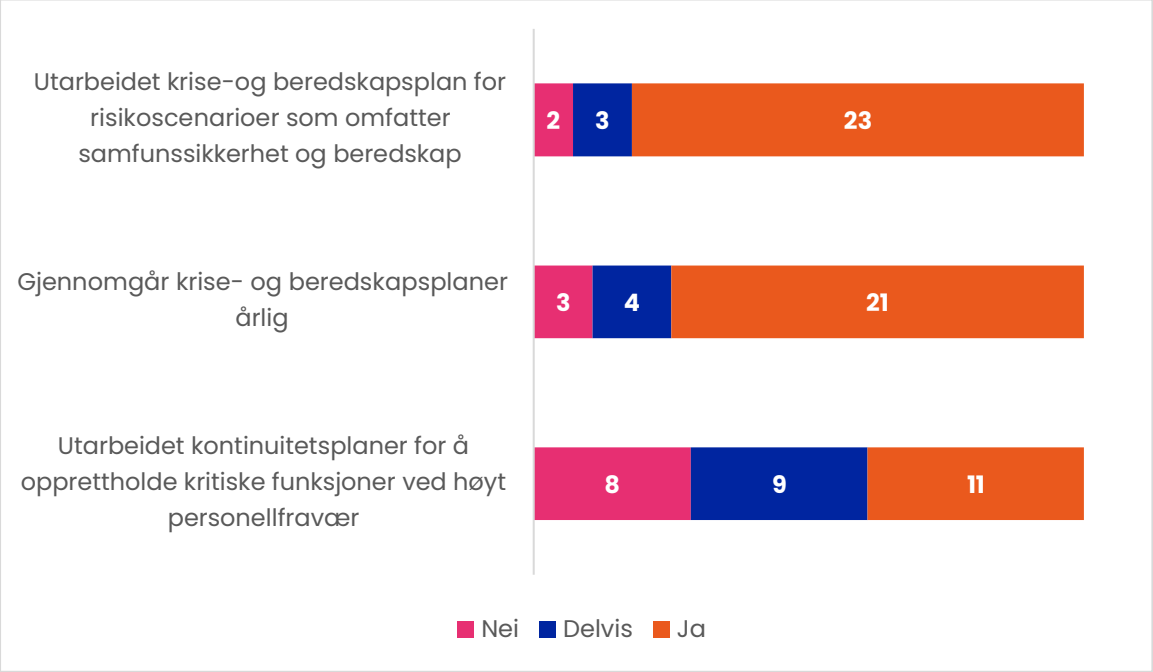
Virksomhetene skal også gjennomføre minst en øvelse i året på håndtering av hendelser som de har identifisert i den overordnede risikovurderingen. Hendelser som er vurdert til middels eller høy risiko skal prioriteres som valg av øvelsesscenario. I etterkant av øvelsene, skal virksomhetene lage en oppfølgingsplan. Planen skal inneholde læringspunkter fra øvelser, forslag til konkrete forbedringstiltak og tidsramme for gjennomføring av tiltakene.

I dette kapitlet drøfter vi hvordan kravene til beredskapsplaner og beredskapsøvelser praktiseres i forsknings- og høyere utdanningssektoren. Først ser vi på om virksomhetene har laget en beredskapsplan for håndtering av uønskede sikkerhetshendelser og kriser. Deretter ser vi på omfanget av øvelsesaktiviteten og hvordan erfaringer fra øvelsene følges opp.

Beredskapsplan

Figur 9 viser hvordan de 28 virksomhetene besvarte spørsmålene i spørreskjemaet som gjelder utarbeidelse og revisjon av beredskapsplaner.

[33] En krise kan oppstå som en plutselig hendelse, som en eskalerende hendelse som gradvis går fra normal håndtering til krisehåndtering, eller som en varslet krise. Krisesituasjoner krever ofte svært raske beslutninger og iverksettelse av tiltak på en raskere og mer effektiv måte enn i en normal situasjon (Kunnskapsdepartementet, 2025).



Figur 9: Utarbeidelse og revisjon av beredskapsplaner

Et stort flertall av virksomhetene (23) har utarbeidet beredskapsplaner for uønskede sikkerhetshendelser som de har identifisert i den overordnede risikovurderingen. Kun et fåtall virksomheter oppga at de ikke eller bare delvis har beredskapsplaner.

Det er også et stort flertall (21 virksomheter) som svarte at de reviderer beredskapsplanene årlig. Virksomhetene kan, i likhet med den overordnede risikovurderingen, ha ulikt behov for revidering av beredskapsplaner fra år til år.

Resultatene indikerer at selv om det er visse svakheter i beredskapsarbeidet hos noen virksomheter, overholder store deler av sektoren departementets krav til utarbeidelse av planer for håndtering av alvorlige sikkerhetshendelser.

Når det gjelder kontinuitetsplaner ved høyt personellfravær, som skal være en del av beredskapsplanen, fremgår det av tallene i figur 9 at manglene er større. Nesten hver tredje virksomhet oppgir at de enten ikke har eller bare delvis har utarbeidet slike planer.

Virksomhetene ble også spurt om de har utarbeidet pandemiplaner.[34] 24 virksomheter svarte at dette er gjort, mens fire virksomheter svarte at pandemiplanen enten er mangelfull eller at den ikke finnes.

Digital beredskap

Beredskaps- og kontinuitetsplaner innen digital sikkerhet skal sørge for at kritiske funksjoner opprettholdes ved større sikkerhetshendelser og sikre at normal IT-drift raskt kan gjenopprettes. Et oppdatert og testet beredskaps- og kontinuitetsplanverk er derfor avgjørende for å sikre robusthet og motstandskraft i digital infrastruktur og IT-systemer i sektoren.

I spørreskjemaet svarte 24 virksomheter at de har mangler i sine beredskaps- og kontinuitetsplaner for digitale sikkerhetshendelser. Fire virksomheter oppga at planverket var i henhold til kravene i departementets policy for informasjonssikkerhet og personvern.

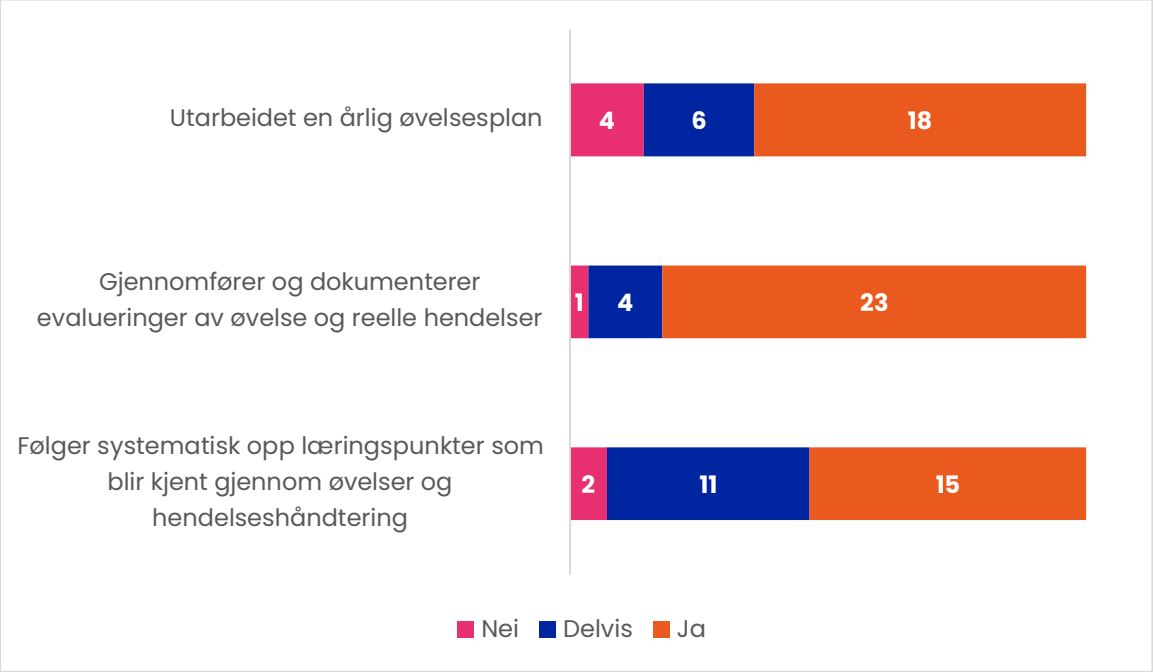
9 av de 10 virksomhetene vi intervjuet, opplyste om det samme. Det ble særlig trukket frem at planverket ofte er ufullstendig eller utdatert. Enkelte av virksomhetene som manglet beredskaps- og kontinuitetsplaner opplyste likevel om at de har lykkes med å gjenopprette data og driften av IT-systemer i etterkant av digitale sikkerhetshendelser.

Flere av de intervjuede virksomhetene planla å gjennomgå og videreutvikle beredskaps- og kontinuitetsplanene sine i løpet av 2025.

Beredskapsøvelser

Figur 10 viser virksomhetenes svar på spørsmålene i spørreskjemaet som omhandler planer for, gjennomføring og oppfølging av beredskapsøvelser.

[34] Pandemiplanen skal utfylle beredskapsplanen og skal revideres ved behov (Kunnskapsdepartementet, 2025).



Figur 10: Planlegging, gjennomføring og oppfølging av beredskapsøvelser

Vi ser at selv om det er relativt vanlig at virksomhetene utarbeider årlige planer for øvelser, svarte likevel omkring hver tredje virksomhet (10) at øvelsesplanen enten ikke foreligger eller er mangelfull. På den annen side svarte hele 23 virksomheter at de gjennomfører og dokumenterer erfaringer fra øvelser og reelle sikkerhetshendelser.

Disse resultatene kan tyde på at sektoren er bedre på å gjennomføre øvelser enn den er på å planlegge hva det skal øves på og hvilke typer øvelser som skal gjennomføres (for eksempel diskusjonsøvelser, spilløvelser eller fullskalaøvelser).

Videre ser vi av figur 10 at omkring halvparten av virksomhetene (15) svarte at læringspunkter fra øvelser og reelle sikkerhetshendelser systematisk følges opp med forbedringstiltak. Den andre knappe halvparten svarte at de bare delvis eller ikke i det hele tatt gjør dette.

Dette indikerer at oppfølging av erfaringer fra øvelser (og reelle hendelser) – og å bruke disse i eget forbedringsarbeid – er et område hvor sektoren har et tydelig forbedringsbehov. Resultatene antyder også at sektoren er bedre på å dokumentere øvelsesaktiviteten enn den er på å evaluere de øvelsene som gjennomføres.

Øvelsesscenarioer

Til slutt ble virksomhetene spurt om hvilke typer hendelser de øvde på i 2024. Her fremkom det at øvelsene i stor grad dreide seg om følgende scenarioer:

- fravær av nøkkelpersonell ved alvorlige hendelser,
- gjenoppretting av data fra sikkerhetskopi,
- dataangrep og løsepengevirus,
- innsidehendelser (uønskede hendelser forårsaket av bevisste eller ubevisste feil fra egne ledere eller medarbeidere), og
- personopplysninger på avveie.

Øvelser på digitale sikkerhetshendelser

Oversikten over øvelsesscenarioer viser at sektoren i stor grad forbereder seg på sikkerhetstruende hendelser i det digitale rom, for eksempel dataangrep og løsepengevirus. Virksomhetene ble derfor spurt særskilt om øvelser som omhandler denne typen uønskede hendelser.

18 av 28 virksomheter svarte at de i 2024 hadde gjennomført egne øvelser på håndtering av digitale sikkerhetshendelser, inkludert hendelser som gjaldt personopplysningssikkerheten.[35] 10 virksomheter oppga at de ikke hadde øvd på håndtering av slike hendelser i 2024. Av disse svarte halvparten at de planla å gjennomføre minst én øvelse i 2025, og enkelte av dem ønsket å gjennomføre øvelser i samarbeid med andre virksomheter i sektoren.

Også disse resultatene indikerer at omfanget av øvelsesaktiviteten i sektoren ikke er på samme nivå som forventet av departementet (jf. kravene i styringsdokumentet for sikkerhet og beredskap og i policy for informasjonssikkerhet og personvern). Sektoren har derfor behov for å styrke denne delen av sikkerhetsarbeidet.

[35] Av disse hadde ni virksomheter gjennomført diskusjonsøvelser, mens fem virksomheter hadde gjennomført kombinerte diskusjons- og spilløvelser. Én virksomhet oppga å ha gjennomført fullskalaøvelse.

Kapittel 7: Tilgangsstyring i skytjenester

Innledning

Drøftelsene i tidligere kapitler indikerer at trusselbildet i sektoren er skjerpet (se særlig kapittel 2). Den vanligste fremgangsmåten som trusselaktører benytter for å få tilgang til skjermverdig informasjon, personopplysninger og andre dataressurser, er å ta kontroll over virksomhetens administrator- eller brukerkontoer.[36] Tilfredsstillende sikring, spesielt av administratorkontoer, er derfor avgjørende for å forebygge digitale sikkerhetshendelser, for eksempel løsepengevirusangrep og datatyveri.

Riksrevisjonens undersøkelse av informasjonssikkerheten i forskningssystemer i forsknings- og høyere utdanningssektoren, avdekket likevel mangler i rutiner og oppsett for sikring av tilganger i IT-systemer og -tjenester i sektoren (Riksrevisjonen 2024).[37] I årets kartlegging har vi derfor valgt å følge opp Riksrevisjonens funn ved å se nærmere på tilgangsstyringen i skytjenester. Skytjenester er valgt fordi de utgjør en stor del av sektorens IT-portefølje og fordi tjenestene er basert på å være tilgjengelige overalt. Dette øker potensialet for uautorisert tilgang til tjenestene.

Tilgangsstyringen hos tre virksomheter ble undersøkt. Virksomhetene representerer ulike deler av sektoren med hensyn til størrelse og faglig profil.

I dette kapitlet oppsummerer vi funn fra undersøkelsene og anbefalinger som vi har formidlet til resten av sektoren på bakgrunn av hva vi fant.

Praktisk gjennomføring

Undersøkelsene av tilgangsstyring i skytjenester ble gjennomført i form av fysiske møter hos de tre utvalgte virksomhetene. Møtene ble avholdt i perioden desember 2024 til januar 2025. Hvert møte hadde en lengde på omkring fire timer.

I forkant av møtene fikk virksomhetene oversendt informasjon om formål, ønsket deltakelse og gjennomføring av møtene.

Virksomhetene mottok også informasjon om fokusområder/tema for undersøkelsen, og om ulike forhold knyttet til tilgangsstyring som vi var særlig interessert i å se nærmere på.

[36] Bruken av metoder som omgår tradisjonelle tiltak for sikring av administrator- og brukerkontoer, blant annet tofaktorautentisering, gjør det ekstra viktig å sikre kontoer mot kompromittering og misbruk.

[37] Én av virksomhetene som vi undersøkte i årets kartlegging var også med i Riksrevisjonens undersøkelse.

Metodikk og kontrollkriterier

Vår undersøkelse tok utgangspunkt i metoder og funn fra Riksrevisjonens undersøkelse nevnt ovenfor, samt god praksis for tilgangsstyring. Hovedfokuset var virksomhetenes kontroll av kontoer med utvidede rettigheter i Microsoft Entra ID.

Om Microsoft Entra ID

Entra ID er Microsofts tjeneste for håndtering av identiteter og tilgangsstyring i selskapets skytjenester. Oppsettet i denne tjenesten håndterer tilgangene til blant annet Microsoft 365-applikasjonene, som for eksempel Teams og OneDrive.

Kriteriene som vi vurderte virksomhetenes tilgangsstyring opp mot, var hentet fra NSMs (2021b) grunnprinsipper for IKT-sikkerhet, nærmere bestemt grunnprinsipp 2.6 «Ha kontroll på identiteter og tilganger». Vi hadde spesielt fokus på disse anbefalte sikkerhetstiltakene:

- Ikke tildel administratorrettigheter til sluttbrukere (tiltak 2.6.4a i NSMs grunnprinsipper).
- Håndter spesialbrukere som unntaksvis kan ha behov for utvidede systemrettigheter, inkludert administrative rettigheter (tiltak 2.6.4b i NSMs grunnprinsipper).
- Unngå bruk av upersonlige kontoer (tiltak 2.6.5c i NSMs grunnprinsipper).
- Etabler forskjellige kontoer til de ulike driftsoperasjonene (tiltak 2.6.5a i NSMs grunnprinsipper).
- Begrens bruken av kontoer med domene-admin-rettigheter til kun et minimum av virksomhetens driftsoperasjoner (tiltak 2.6.5b i NSMs grunnprinsipper).
- Implementer som et minimum multifaktorautentisering på brukerkontoer som har tilgang til kritiske data eller systemer, samt brukere med driftsoppgaver (tiltak 2.6.7a i NSMs grunnprinsipper).

I møtene med virksomhetene gikk vi i tillegg gjennom overordnede forhold som omhandlet koblingen mellom lokal brukerdatabase og Entra ID. Vi undersøkte også hvordan aktiviteter tilknyttet administratorkontoer ble logget, rutiner for periodisk

gjennomgang av administratorkontoer[38] og andre sikkerhetstiltak knyttet til brukere og tilganger.

Formålet med denne delen av undersøkelsen var å få kontekstinformasjon om virksomhetens kobling mellom ulike brukerdatabaser, og eventuell bruk av spesifikk sikkerhetsfunksjonalitet i Microsoft Entra ID.

Sentrale funn

Undersøkelsen viste at det var stor variasjon i virksomhetenes prosedyrer for tilgangsstyring og hvilke sikkerhetstiltak som var etablert. Utgangspunktet var imidlertid likt hos alle virksomhetene, med en oversiktlig domenestruktur, klare definisjoner på hva som er autoritative kilder for brukere og kontroll på synkronisering mellom ulike brukerdatabaser. Dette gir virksomhetene et godt utgangspunkt for å ha kontroll på identiteter/kontoer og tilganger i skytjenestene.

To av virksomhetene hadde etablert et tydelig skille mellom sluttbrukerkontoer og administratorkontoer, både lokalt og i Microsoft Entra ID. Hos den tredje virksomheten var dette ikke gjort, og rettigheter for å utføre driftsoppgaver (administratorrettigheter) var tildelt sluttbrukerkontoer.

De to virksomhetene som hadde etablert separate administratorkontoer hadde også rutiner for tilpassing av rettighetsnivået ut fra tjenstlige behov (ansvarsområde eller driftsoppgaver som medarbeiderne skal utføres). Den tredje virksomheten hadde kun gjort dette i begrenset grad.

Antallet kontoer med rettighetsnivået «Global Administrator»,[39] varierte fra fem til ti blant virksomhetene som ble undersøkt, inkludert såkalte «Break Glass»-kontoer.[40] Ifølge Microsofts beste praksis, anbefales mindre enn fem kontoer med dette tilgangsnivået (Microsoft, 2025).

Blant de tre undersøkte virksomhetene var det også variasjoner i hvilke tiltak de hadde iverksatt for å sikre administratorkontoene. Microsofts standardoppsett har

---

[38] Dette omfatter blant annet periodisk gjennomgang for å tilpasse tilgangsnivået til tjenstlige behov, og rutiner for å sikre at inaktive kontoer blir deaktivert/slettet.

[39] Dette rettighetsnivået tilsvarer domene-admin, og gir fullstendig kontroll over ressursene virksomheten har i Microsofts skyløsning.

[40] Dette er kontoer opprettet for å sikre tilgang til domenet i nødstilfeller, det vil si dersom pålogging med andre administrative kontoer ikke fungerer. Se nærmere forklaring på Manage emergency access admin accounts - Microsoft Entra ID | Microsoft Learn, sist besøkt 08.07.2025.

krav om multifaktorautentisering for slike kontoer, men hos én av virksomhetene fungerte ikke dette kravet på undersøkelsestidspunktet.

Hos de to virksomhetene som hadde aktivert krav om multifaktorautentisering, var det i tillegg egne regler med krav om såkalt nettfiskeresistent autentisering.[41] Én av disse virksomhetene hadde dessuten krav til sikkerhet på datamaskiner som benyttes av administratorer («compliant device»[42]). Hos denne virksomheten var det også etablert begrensninger på hvilke land det var mulig å logge på fra.

Virksomheter i forsknings- og høyere utdanningssektoren har ofte internasjonalt samarbeid og brukere som trenger å arbeide fra andre land, og i Entra ID er det mulig å etablere geografiske begrensninger på bruken av administratorkontoer. I vår undersøkelse var det altså kun én virksomhet som hadde innført slike begrensninger. Dette var gjort for alle brukere, og det var etablert rutiner for håndtering av unntak.

I Microsoft Entra ID finnes det i tillegg ulike mekanismer for å styrke sikkerhetsnivået i tilgangsstyringen. En av disse mekanismene er «Privileged Identity Management» (PIM). PIM gjør det mulig å tildele rettigheter i skytjenester for et begrenset tidsrom, og det kan kreves at tildelingen må godkjennes av særlig autoriserte brukere. Denne mekanismen ble brukt av to virksomheter i vår kartlegging, og da med egengodkjenning av rettighetstildelingen av praktiske hensyn.

Vurdering og oppfølging

De tre virksomhetene som ble undersøkt representerer ulike deler av sektoren, og det var som nevnt relativt store forskjeller i sikkerhetsnivået mellom dem. Særlig én av virksomhetene hadde et betydelig forbedringspotensial. Her var det derfor behov for å iverksette ytterligere sikringstiltak. Disse bør kunne iverksettes relativt enkelt og uten at det medfører store kostnader.

Vi antar at de svakhetene i tilgangsstyringen som ble oppdaget hos denne virksomheten også kan finnes hos andre virksomheter i sektoren.

I etterkant av besøkene fikk de tre virksomhetene oversendt et referat fra møtet. Det ble også oversendt notater om tilstanden på tekniske sikkerhetstiltak. De undersøkte virksomhetene mottok i tillegg anbefalingsbrev, hvor de fikk konkrete anbefalinger om

---

[41] NSM anbefaler overgang til phishingresistent autentisering - Nasjonal sikkerhetsmyndighet, sist besøkt 08.07.2025.

[42] Dette medfører at autentiseringen bare kan gjøres fra dataenheter som er innrullert i virksomhetens flåtestyring. Videre kan det settes krav til den tekniske tilstanden til dataenheten, for eksempel at operativsystemet er oppdatert.

hvilke tekniske sikkerhetstiltak som bør prioriteres i det videre arbeidet med forbedring av tilgangsstyringen i skytjenester.

Samtlige av de øvrige virksomhetene som inngår i HK-dir sine årlige kartlegginger av sikkerhet og beredskap, mottok også anbefalingsbrev hvor de ble oppfordret til å gjennomgå rutiner og praksis for håndtering av administrative kontoer i sine skytjenester.

Nærmere om anbefalte tiltak

De generelle anbefalingene som ble formidlet i brev til de øvrige virksomhetene i sektoren, var koblet til sikkerhetstiltak som NSM har plassert i prioriteringsgruppe 1.[43] Disse tiltakene omtales som de mest tidskritiske, det vil si at fraværet av slike tiltak ofte er «rotårsaken» til vellykkede dataangrep. Gjennomføring av tiltakene i prioriteringsgruppe 1 vil likevel ikke være veldig ressurskrevende eller medføre store investeringskostnader for sektoren, men kan kreve endringer i driftsrutiner og holdninger.[44]

I anbefalingsbrevene, og på bakgrunn av funn fra undersøkelsene hos de tre utvalgte virksomhetene, ble de øvrige delene av sektoren bedt om å iverksette følgende sikkerhetstiltak:

- Etabler administratorkontoer som er adskilt fra sluttbrukerkontoer. Dette tiltaket gjør det mulig å innføre særskilte sikkerhetskrav for å gi administratorkontoene ekstra beskyttelse. Det vil også redusere bruken av slike kontoer, og dermed redusere sannsynligheten for at kontoer med utvidede tilganger kommer på avveie.
- Tilpass rettighetsnivået på kontoene til de oppgavene som skal utføres, og begrens bruken av «Global Administrator» til et minimum. Dette vil redusere sannsynligheten for at en trusselaktør tar seg inn i og får full kontroll over systemmiljøet.

---

[43] Se ark «02 Om prioritering av tiltak» på https://nsm.no/getfile.php/1313978-1717742007/NSM/Filer/Dokumenter/Veiledere/Regneark%20med%20tiltak%20fra%20NSMs%20grunnprinsipper%20for%20IKT-sikkerhet.xlsx, sist besøkt 08.07.2025.

[44] Eksempelvis vil etablering av separate administrasjonskontoer være mer arbeidskrevende for de som utfører driftsoperasjoner i virksomheten, særlig når det opprettes spesifikke kontoer for ulike typer driftsoppgaver. Denne kostnaden må veies opp mot behovet for å redusere sannsynligheten for at kontoer kommer på avveie og de konsekvenser som dette kan innebære.

- Innfør multifaktorautentisering på administratorkontoer i skyløsninger. Dette kravet bør utvides til også å inkludere bruk av såkalt nettfiskeresistent autentisering. Nettfiskeresistent autentisering sikrer kontoer mot nye angrepsmetoder som mange trusselaktører nå benytter, for eksempel angriper-i-midten.

Iverksetting av de anbefalte tiltakene vil bidra til å redusere risikoen for flere av risikoscenariene (uønskede sikkerhetshendelser) som drøftes i neste kapittel.

Kapittel 8: Risikovurdering på sektornivå

Innledning

I dette kapitlet vurderer vi risiko for utvalgte risikoscenarioer, det vil si hendelser som representerer trusler mot samfunnssikkerheten, den nasjonale sikkerheten, informasjonssikkerheten og personvernet i sektoren. Scenarioene som vi vurderer, har betydning for minst to av disse sikkerhetsområdene. Dette er derfor hendelser som det er særlig viktig at sektoren er forberedt på og iverksetter tiltak for å forebygge, oppdage og håndtere.

Scenarioer som ikke berører minst to av sikkerhetsområdene, for eksempel risiko for direktør- eller fakturasvindel, vil ikke bli drøftet i dette kapitlet. Disse og flere andre former for nettsvindel, er likevel scenarioer som sektoren må kunne forebygge, oppdage og håndtere på en god måte.

Vurderinger av risiko for hver av de scenarioene som vi har valgt å fremheve i dette kapitlet, baserer seg på funn og konklusjoner i kapittel 2-7.

Vårt rammeverk for vurdering av risiko, finnes i vedlegg 2.

Sikkerhet og internasjonalt samarbeid

Det finnes også andre scenarier enn de vi fremhever i dette kapitlet som sektoren bør være oppmerksom på fremover.

HK-dir har for eksempel kartlagt mulige konsekvenser for internasjonalt kunnskapssamarbeid som følge av den ustabile geopolitiske situasjonen (HK-dir 2024b). Her fremkom det at aktører i sektoren er bekymret for en mulig nedkjøling av dette samarbeidet, og for hvordan en eventuell nedkjøling kan påvirke det fremtidige kunnskapsarbeidet.

Sett i lys av denne bekymringen, er det viktig at sektoren balanserer hensynet til tilfredsstillende sikkerhet og behovet for internasjonalt samarbeid om forskning og utdanning på en god måte, særlig når det gjelder risikoland.

Risikoscenario 1: Hendelser som skyldes manglende beskyttelse av viktige verdier – middels risiko

Vår vurdering er at det er middels risiko for at sektoren ikke klarer å beskytte viktige verdier (verdier underlagt sikkerhetslov, eksportkontroll, fysisk infrastruktur, objekter eller forskningsresultater). Dette begrunner vi med at oversikten over viktige verdier er

mangelfull, og at dette kan øke sannsynligheten for uautorisert tilgang til skjermingsverdige verdier.

Verdiene kan for eksempel utsettes for sabotasje eller innsidevirksomhet. Dette er også noe som det pekes på i NSM sin siste risikorapport. Tap av viktige verdier i UH-sektoren kan ha stor negativ innvirkning på sektorens leveranseevne, økonomi og omdømme. I ytterste konsekvens kan dette påvirke norske sikkerhetsinteresser, gjennom tap av sensitive forskningsdata til fremmede stater, og utgjøre en trussel mot den nasjonale sikkerheten.

Når det gjelder hendelser, er det generelt få eksempler som kan trekkes frem. Samtidig har norsk UH-sektor alltid vært preget av åpenhet. Det er derfor enkelt å bevege seg på norske campus og det er lite overvåking eller tilsyn. Virksomhetene etablerer tiltak som reduserer både sannsynligheten for og konsekvensene av tap av viktige verdier. Sektoren har for eksempel startet arbeid med å etablere verdioversikter, med mer systematisk lederforankring, og stadig flere etablerer rutiner for personellsikkerhet (ansettelser).

Risikoscenario 2: Mangelfull håndtering av alvorlige hendelser – middels til høy risiko

Vår vurdering er at det er middels til høy risiko for at virksomhetene ikke klarer å håndtere en alvorlig hendelse, grunnet manglende helhetlig styring. Eksempler på slike hendelser inkluderer sammensatte trusler,[45] alvorlige tilsiktede handlinger (PLIVO), eller alvorlige utilsiktede handlinger (naturhendelser).

Årets kartlegging tilsier at flere virksomheter har mangler i eget sikkerhetsarbeid, som kan bidra til at sektoren får utfordringer i hendelseshåndtering dersom en større, kompleks hendelse inntreffer. Blant annet er det mangler knyttet til årlig gjennomgang av planverk, sammenhenger mellom scenariene i lokale ROS-analyser og hva virksomhetene øver på, samt arbeid med tiltaksplaner.

[45] Sammensatte trusler er strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt. Kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske og finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsetninger. Virkemiddelbruken er gjerne bredt distribuert, langsiktig i sin tilnærming og kan kombinere åpne, fordekte og skjulte metoder. Se NOU 2023: 17, s. 115.

Manglende helhetlig styring kan også medføre at virksomhetene ikke er i stand til å fange opp potensialer for eskalering eller utvikling av en hendelse på tvers av sikkerhetsdomener, eller konsekvenser for verdier utover de som er direkte rammet. Dette kan medføre negative virkninger for virksomhetens leveranseevne, ved at tjenester, forskning og utdanning får opphold eller stans. Omdømme kan også rammes.

Vi anser at noen virksomheter kan være mer utsatt for enkelte typer alvorlige hendelser, spesielt basert på geografisk beliggenhet eller faglig profil. Eksempler kan være virksomheter som ligger i eller utfører forskning knyttet til nordområdene eller som forvalter verdier underlagt eksportkontollregelverket. Derfor anses risikoen for dette risikoscenarioet som middels til høy.

Risikoscenario 3: Løsepengevirus – høy risiko

Vår vurdering er at risikoen for løsepengevirusangrep fortsatt er høy i sektoren. I årets kartlegging oppga én virksomhet å ha blitt utsatt for flere forsøk på løsepengevirusangrep. NSM mener at løsepengevirus er den største digitale sikkerhetsutfordringen for norske virksomheter (Risiko 2025a, s. 29).

Under undersøkelsene av tilgangsstyring i skytjenester, fant vi flere sårbarheter som kan utnyttes i denne typen angrep (se forrige kapittel). Vi legger til grunn at disse sårbarhetene kan være til stede hos andre virksomheter i sektoren enn enkelte av de som ble undersøkt. Vår vurdering er derfor at løsepengevirus er et sannsynlig risikoscenario i forsknings- og høyere utdanningssektoren også i 2025.

Løsepengevirus kan i verste fall få store negative konsekvenser, avhengig av hvilke rettigheter angriperen tilegner seg i virksomhetens datanettverk.[46] Det kan for eksempel medføre driftsstans, tap av data, betydelige oppryddingskostnader, kompromittering av skjermingsverdig informasjon, personvernavvik og svekket omdømme.

Risikoscenario 4: Kunnskapsspionasje – høy til lav risiko

Vår vurdering er at risikoen for kunnskapsspionasje er ujevnt fordelt mellom virksomhetene i sektoren. Risikoen fremstår som lav hos virksomheter med en faglig profil som i liten grad samsvarer med kunnskapsområder som PST mener er

[46] Virksomheter med svak tilgangsstyring er derfor særlig utsatt for løsepengevirus.

interessante for utenlandsk etterretning (PST, 2025, s.19).[47] For en del andre virksomheter, som driver forskning og undervisning innen disse kunnskapsområdene, er vår vurdering at risikoen er høy.

I årets kartlegging rapporterte fire virksomheter om sikkerhetstruende aktivitet fra statlige eller statsstøttede aktører. Samtidig kan sårbarheter i tilgangsstyringen, drøftet i forrige kapittel, utnyttes til kunnskapsspionasje (uautorisert tilgang til skjermingsverdig informasjon, infrastruktur, personopplysninger og andre dataressurser). Vi vurderer det derfor som sannsynlig at slike hendelser kan forekomme i 2025.

Selv om slike hendelser ikke har medført store negative konsekvenser i 2024, er skadepotensialet likevel stort. Hendelsene kan for eksempel true nasjonale sikkerhetsinteresser gjennom kompromittering av kunnskap og teknologi underlagt eksportkontroll eller sikkerhetsloven. De kan også føre til omfattende opprydningskostnader og svekke virksomhetens omdømme.

Risikoscenario 5: Utilsiktede feil og uhell – middels risiko

Vår vurdering er at det er en middels risiko i sektoren for hendelser og brudd som skyldes utilsiktede menneskelige eller tekniske feil og uhell. Denne typen hendelser er relativt vanlige i sektoren, og ligger i stor grad bak økningen i antall saker som ble varslet til Datatilsynet. Samtidig rapporterte virksomhetene om sårbarheter som kan føre til slike hendelser, blant annet mangelfulle rutiner for håndtering av skjermingsverdig informasjon og personopplysninger. Vi vurderer det derfor som svært sannsynlig at slike hendelser også vil inntreffe i 2025.

Konsekvensene av utilsiktede feil og uhell fremstår som begrensede. Hendelsene fører vanligvis til at ansatte får tilgang til en begrenset mengde personopplysninger de ikke har tjenstlige behov for. Samtidig kan slike hendelser medføre utilsiktet tilgang til andre beskyttelsesverdige informasjonsverdier, for eksempel informasjon av betydning for nasjonal sikkerhet. Vi har likevel ikke registrert at det har skjedd i løpet av de årene vi har kartlagt sikkerhetstilstanden i sektoren. I 2024 ble det rapportert et par hendelser som hadde konsekvenser for personvernet til flere ansatte og studenter.

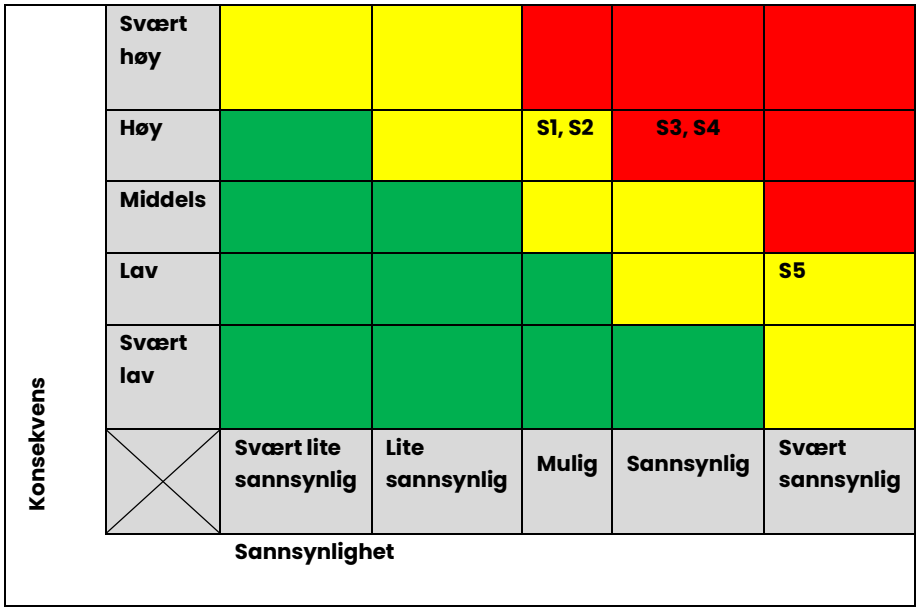
[47] PST peker spesielt på teknologi og forskning innen områder som bioteknologi, materialteknologi og metallurgi, kjernefysikk, kryptografi, kvanteteknologi, nanoteknologi, romfart og fremdriftsteknologi, sensorteknologi, navigasjonsteknologi, robotikk og autonomi, og mikroelektroniske systemer.

Vår vurdering er derfor at konsekvensene av slike hendelser trolig vil være relativt begrensede også i 2025.

Risikomatrisen

Risikovurderingen av de fem scenarioene oppsummeres i risikomaterien nedenfor. Scenarioene benevnes S1–S5:

- S1 = manglende beskyttelse av viktige verdier
- S2 = mangelfull håndtering av alvorlige hendelser
- S3 = løsepengevirus
- S4 = kunnskapsspionasje
- S5 = utilsiktede feil og uhell



Figur 11: Risikomatrise

Kapittel 9: Anbefalinger til virksomhetene

I dette kapittelet gir vi anbefalinger for virksomhetenes videre arbeid med samfunnssikkerhet, nasjonal sikkerhet, informasjonssikkerhet og personvern. Anbefalingene har til hensikt å lukke avvik fra kravene som departementet stiller til sikkerhetsarbeidet i sektoren og som vi har drøftet i kapittel 3-7. De har også til hensikt å redusere risikoen for uønskede hendelser drøftet i forrige kapittel.

Anbefalingene er formidlet i brev til hver av de 28 virksomhetene som omfattes av våre årlige kartlegginger.

Styrings- og ledelsessystem

Virksomheter som ikke har et dokumentert og fungerende styringssystem for sikkerhet eller ledelsessystem for informasjonssikkerhet, må prioritere dette. Et helhetlig styrings- og ledelsessystem er avgjørende for at virksomhetene skal kunne ivareta kravene i sikkerhetsloven og annen relevant lovgivning, for eksempel GDPR.

Ferdigstillelse av styrings- og ledelsessystemer innebærer blant annet å dokumentere roller og ansvar, etablere rutiner for risikostyring og hendelseshåndtering, utarbeide beredskaps- og kontinuitetsplaner, og sørge for at sikkerhetsarbeidet er forankret hos toppledelsen.

Vi anbefaler at virksomhetene gjennomgår status for styrings- og ledelsessystemer, og lager en plan for ferdigstillelse og innføring. Virksomhetene bør også vurdere hvordan styrings- og ledelsessystemer kan samordnes og hvordan sikkerhetsledelse kan inngå i den øvrige virksomhetsstyringen.

Verdioversikt

Virksomheter som har skjermingsverdige informasjonsverdier som omfattes av eksportkontroll, internasjonale sanksjoner eller er underlagt sikkerhetsloven, bør prioritere å få oversikt over disse. Det samme gjelder for virksomheter som fortsatt har mangler i sin behandlingsprotokoll for personopplysninger.

Vi anbefaler derfor at alle virksomheter gjennomgår sin verdioversikt for å sikre at den er oppdatert og relevant. Oppdaterte verdioversikter er grunnlaget for et risikostyrt sikkerhetsarbeid og bidrar til å redusere risiko for uautorisert tilgang, tap/skade eller manipulering av viktige verdier.

Risikostyring

Alle virksomheter må sørge for at overordnede risikovurderinger (ROS-analyser) følges opp med konkrete sikkerhetstiltak der hvor risikoen er uakseptabel høy. Funn fra årets kartlegging tyder på at planlagte sikkerhetstiltak ikke alltid gjennomføres eller at de ikke følges opp.

Oppfølging av sikkerhetstiltak skal inngå i virksomhetens styringssystem og rapporteringsrutiner. Dette bidrar til at risikoer faktisk reduseres over tid.
Vi anbefaler derfor at virksomheter etablerer rutiner for oppfølging og rapportering av status på sikkerhetstiltak til egen toppledelse.

Øvelser

Vi anbefaler at alle virksomheter prioriterer å gjennomføre flere øvelser på håndtering av alvorlige sikkerhetshendelser, og utarbeider en øvingsplan som dekker de ulike sikkerhetsområdene (samfunnssikkerhet, nasjonal sikkerhet, informasjonssikkerhet og personvern). Regelmessige øvelser vil forbedre evnen til å håndtere uønskede hendelser, blant annet ved å styrke sikkerhetsbevisstheten, kompetansen og samhandlingsevnen i organisasjonen.

Vi anbefaler at virksomheten involverer ansatte og ledelse i både planlegging og evaluering av øvelser.

Kontinuitetsplaner

Vi anbefaler at virksomheter som helt eller delvis mangler en kontinuitetsplan om å prioritere og lukke dette avviket. Kontinuitetsplaner skal bygge på virksomhetens overordnede risikovurdering. Den skal inneholde tiltak for å opprettholde viktige funksjoner og gjenopprette normal driftstilstand så raskt som mulig.

Planene skal omfatte digital infrastruktur og IT-systemer og -tjenester som er kritiske for kjernevirksomheten. Den bør også ta høyde for fravær av personell som er kritiske for gjennomføring av viktige sikkerhetsoppgaver.

Personellsikkerhet

Vi anbefaler at alle virksomheter etablerer, eventuelt gjennomgår, rutiner for personellsikkerhet. Dette for å redusere risikoen for uautorisert tilgang til skjermingsverdig informasjon, personopplysninger og andre verdier som sektoren forvalter.

Personellsikkerhet omfatter blant annet rutiner for bakgrunnssjekk og gjennomføring av sårbarhetssamtaler. Det bør også iverksettes tiltak i forbindelse med ansettelser

og håndtering av gjesteforskere fra land som Norge ikke har sikkerhetspolitisk samarbeid med.

Tilgangsstyring

Vi anbefaler at alle virksomheter gjennomgår rutiner og praksis for håndtering av administrative tilganger i sine skytjenester. Der hvor det identifiseres svakheter i tilgangsstyringen, anbefaler vi at det iverksettes tiltak for å utbedre disse.

Vi anbefaler videre at tiltakene tar utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet (Nasjonal sikkerhetsmyndighet 2021b). Det innebærer at virksomhetene iverksetter følgende tiltak:

- gjennomgår oppsett av administrasjonskontoer for å påse at rettighetsnivået er begrenset til de driftsoppgavene som den enkelte skal utføre,
- gjennomgår rutiner for oppfølgning av sårbarhetsskann for internetteksponerte tjenester, og sørger for at nødvendige oppdateringer gjennomføres,
- etablerer logging på viktige IT-systemer og -tjenester, og utarbeider rutiner for sikkerhetsovervåkning,
- etablerer rutiner for håndtering av digitale sikkerhetshendelser.

I tillegg anbefaler vi at virksomhetene innfører nettfiskeresistent autentisering på administrasjonskontoer (og andre viktige brukerkontoer) i skytjenester og andre internetteksponerte tjenester.

Referanseliste

Datatilsynet. (2024, 13. mars). *Protokoll over behandlingsaktiviteter.* https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/, sist besøkt 27.05.2025.

Datatilsynet. (2025, 15. januar). Informasjon om overføringer til USA. https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/informasjon-om-overforinger-til-usa/, sist besøkt 23.05.2025.

Digitaliseringsdirektoratet. (2022, 27. september). *Informasjonssikkerhet – Skjermingsverdige verdier etter sikkerhetsloven*. https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-skjermingsverdige-verdier-etter-sikkerhetsloven/2283

Direktoratet for eksportkontroll og sanksjoner. (u.å.). DEKSA. https://deksa.no/

Direktoratet for høyere utdanning og kompetanse. (2024a, 10. juni). *Informasjonssikkerhet og personvern i høyere utdanning og forskning: Risiko- og tilstandsvurdering 2024* (Rapport nr. 4/2024). https://hkdir.no/rapporter-undersokelser-og-statistikk/informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning-risiko-og-tilstandsvurdering-2024

Direktoratet for høyere utdanning og kompetanse. (2024, 17. november). Geopolitisk spenning og internasjonalt kunnskapssamarbeid. En kvalitativ studie av erfaringer i norske fagmiljø (Rapport nr. 12/2024). https://hkdir.no/rapporter-undersokelser-og-statistikk/geopolitisk-spenning-og-internasjonalt-kunnskapssamarbeid-en-kvalitativ-studie-av-erfaringer-i-norske-fagmiljo

Direktoratet for høyere utdanning og kompetanse. (2025, 21. januar). *Styring av informasjonssikkerhet og personvern*. https://hkdir.no/hoyere-utdanning-og-forskning/sikkerhet/styring-av-informasjonssikkerhet-og-personvern, sist besøkt 23.05.2025.

Etterretningstjenesten. (2025). *Fokus 2025*. https://www.forsvaret.no/aktuelt-og-presse/aktuelt/fokus-2025

Google Threat Intelligence Group. (2025, January 29). *Adversarial misuse of generative AI*. Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai

International Organization for Standardization. (2018). Information technology—Security techniques—Information security management systems—Overview and vocabulary (ISO/IEC Standard No. 27000:2018). https://www.iso.org/standard/73906.html

Kripos. (2025, 12. februar). *Cyberkriminalitet 2025*. Politiet. *Cyberkriminalitet 2025*

Kunnskapsdepartementet. (2025). *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor.* Regjeringen.no.

https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeid-med-sikkerhet-og-beredskap-i-kunnskapsdepartementets-sektor/id3096694/

Microsoft. (2025). *Microsoft Entra role-based access control (RBAC) documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/

Nasjonal sikkerhetsmyndighet. (2019). *Hva er personellsikkerhet?* https://nsm.no/fagomrader/personellsikkerhet/hva-er-personellsikkerhet-1/

Nasjonal sikkerhetsmyndighet. (2021a). *Veileder i verdivurdering av informasjon*. Veileder i verdivurdering av informasjon 2021_07_01.pdf

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

Nasjonal sikkerhetsmyndighet. (2023, 16. mars). *Forebyggelse av tjenestenektangrep.* Forebyggelse av tjenestenektangrep - Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet. (2025a). *Risiko 2025: Et sikkert Norge i en usikker verden*. *NSM Risikorapport 2025*

Nasjonal sikkerhetsmyndighet. (2025b). *Veileder i sikkerhetsstyring*. *Veileder i sikkerhetsstyring - Nasjonal sikkerhetsmyndighet*

Næringslivets Sikkerhetsråd. (2025). *Mørketallsundersøkelsen 2024*. Mørketallsundersøkelsen 2024 – Næringslivets Sikkerhetsråd

Politiets sikkerhetstjeneste. (2025). *Nasjonal trusselvurdering 2025*. Nasjonal trusselvurdering 2025

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

Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon

Vedlegg 1: Definisjoner og krav

Flere av begrepene som vi bruker i rapporten er hentet fra Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor (Kunnskapsdepartementet, 2025). Nedenfor har vi gjengitt definisjonene av sikkerhetsdomene i styringsdokumentet for å tydeliggjøre hva de omfatter.

Samfunnssikkerhet er samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være utslag av tekniske eller menneskelige feil eller bevisste handlinger. Samfunnssikkerhetsarbeid omfatter forebygging, beredskap og krisehåndtering. Arbeidsmiljørelatert HMS-arbeid er i utgangspunktet ikke en del av samfunnssikkerhetsarbeidet, men det er viktig å se områdene i sammenheng.

Statssikkerhet er ivaretagelse av statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet. Statssikkerhet har tradisjonelt vært knyttet til forsvaret av territoriet mot væpnede angrep, men den kan også utfordres ved påvirkning med ulike former for pressmidler mot norske myndigheter og samfunnsaktører.

Nasjonal sikkerhet er definert som statssikkerhet pluss den delen av samfunnssikkerhetsområdet, som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser, for eksempel handlefriheten til de øverste statsorganer og forholdet til andre stater og internasjonale organisasjoner.

Informasjonssikkerhet handler om å beskytte informasjonsverdiers konfidensialitet, integritet og tilgjengelighet, uavhengig av informasjonens karakter og lagringsmedium, gjennom en risikostyringsprosess. Sikkerheten til personopplysninger (personopplysningssikkerhet) inngår i begrepet informasjonssikkerhet i denne rapporten.

Personvern kan forstås som vern av den personlige integriteten. Et vesentlig element i personvernet er at den enkelte skal ha kontroll over, og i størst mulig grad kunne bestemme over, egne personopplysninger. Dette innebærer blant annet retten til å få vite hvilke opplysninger andre kjenner til om en selv og hva opplysningene brukes til. Det er primært vernet av personopplysninger denne dimensjonen som er underlagt lovregulering, for eksempel i personopplysningsloven og personvernforordningen (GDPR) og reglene om taushetsplikt i forvaltningen.

I tillegg benyttes følgende definisjoner:

Eksportkontroll innebærer at forsvarsmateriell og flerbruksvarer, og relatert teknologi og tjenester, ikke kan eksporteres fra Norge uten lisens utstedt av DEKSA (u.å.).[48]

Formålet med eksportkontroll er å sikre at eksporten av forsvarsmateriell fra Norge skjer i tråd med norsk sikkerhets- og forsvarspolitikk, at eksporten av flerbruksvarer ikke bidrar til spredning av masseødeleggelsesvåpen (kjernefysiske, kjemiske og biologiske våpen), og leveringsmidler for slike våpen.

Skjermingsverdige verdier er et samlebegrep for skjermingsverdig informasjon, skjermingsverdige informasjonssystemer, skjermingsverdig infrastruktur og skjermingsverdige objekter i henhold til sikkerhetsloven (Kunnskapsdepartementet, 2025, NSM 2025b).

Krav til sikkerhets- og personvernarbeidet

Nedenfor har vi oppsummert kravene som departementet stiller til virksomhetenes sikkerhetsarbeid i styringsdokument for sikkerhet og beredskap i Kunnskapsdepartementets sektor (Kunnskapsdepartementet, 2025).[49]

Samfunnssikkerhet og beredskap

Departementets krav til arbeidet med samfunnssikkerhet og beredskap retter seg mot grunnelementene i beredskapsarbeidet: ROS-analyser, beredskapsplanverk og øvelser.

ROS-analyser

Virksomheten skal

- Utarbeide en helhetlig overordnet ROS-analyse. Analysen skal bygge på risikovurderinger fra nasjonal sikkerhet, informasjonssikkerhet og også se til HMS-feltet.
- Gjennomgå analysen minimum hvert år og revidere den ved behov.
- Presentere analysen i en helhetlig rapport.

[48] Direktoratet for eksportkontroll og sanksjoner (DEKSA) er den nasjonale fagmyndigheten for eksportkontroll og sanksjoner i Norge. Direktoratet skal følge opp Norges internasjonale forpliktelser og iverksette regjeringens politikk innenfor eksport av forsvarsmateriell og strategisk teknologi, og på sanksjonsområdet (DEKSA, u.å.).

[49] Disse kravene er bør-krav for virksomheter som ikke er underlagt departementets eierstyring. Alle virksomhetene som omfattes av vår kartlegging skal etterleve disse kravene.

- Utarbeide en tiltaksplan til analysen for samtlige uønskede hendelser med middels eller høy risiko (denne kan inkluderes i den helhetlige ROS-rapporten).
- I tiltaksplanen beskrive hvordan de enkelte tiltakene reduserer risikoen knyttet til den enkelte analyserte uønskede hendelsen.

Beredskapsplanverk

Virksomheten skal utarbeide en beredskapsplan som skal gjennomgås årlig, og revideres ved behov. Planen skal som et minimum inneholde:

- Definerte roller, oppgaver og fullmakter i en beredskapssituasjon eller krise
- Rutiner for krisekommunikasjon internt og eksternt
- Varslingsrutiner (herunder varsling av departementet)
- Utarbeide en kontinuitetsplan som del av beredskapsplanen. Holdes oppdatert og revideres ved behov
- Utarbeide en pandemiplan som utfyller beredskapsplanen. Revideres ved behov.

Beredskapsøvelser

Virksomheten skal utarbeide en årlig øvelsesplan som minimum skal inneholde:

- Formålet med den enkelte øvelse
- Tid og sted for gjennomføring
- Øvelsesscenario
- Type øvelse
- Målgruppe
- Gjennomføre minimum en beredskapsøvelse per år. Øvelsene skal ta utgangspunkt i uønskede hendelser identifisert i virksomhetens ROS-analyse.

Evaluering av øvelser og hendelser

Virksomheten skal

- Gjennomføre evalueringer i etterkant av hver beredskapsøvelse og etter reelle hendelser
- Gjennomføre ledelsesforankrede oppfølgingsplaner med utgangspunkt i evalueringene. Disse skal som et minimum inneholde:
- Læringspunkter
- Beskrivelse av tiltakene

- Tidsramme/frist for gjennomføring av tiltakene
- Ansvarlig for hvert enkelt tiltak

Krav til arbeidet med nasjonal sikkerhet

Styringsdokumentet stiller også krav til virksomhetenes arbeid med nasjonal sikkerhet med utgangspunkt i sikkerhetsloven.

Virksomheten skal

- Etablere og vedlikeholde et styringssystem for sikkerhet som sørger for at virksomheten oppfyller kravene gitt i eller med hjemmel i loven
- Samordne styringssystemet med ledelsessystem for informasjonssikkerhet og med virksomhetsstyringen for øvrig
- Dokumentere styringssystemet skriftlig og revidere ved behov.
- Føre oversikt over virksomhetens ansatte som er sikkerhetsklarert og/eller autorisert iht. sikkerhetsloven. Oversikten skal til enhver tid være oppdatert.
- Vurdere, kartlegge og holde oversikt over virksomhetens skjermingsverdige verdier (definert som skjermingsverdig informasjon, informasjonssystemer, infrastruktur eller objekter).
- Kunne motta og håndtere sikkerhetsgradert informasjon til minimum BEGRENSET.

Krav til arbeidet med informasjonssikkerhet og personvern

Kunnskapsdepartementets stiller særskilte krav til virksomhetenes arbeid med informasjonssikkerhet og personvern. Disse kravene er oppsummert i policy for informasjonssikkerhet og personvern (HK-dir, 2025).[50]

Virksomheten skal

- ha et ledelsessystem for informasjonssikkerhet,
- ha oversikt over informasjon og personopplysninger,
- gjennomføre risikovurderinger og etablerer sikringstiltak,
- etablere løsninger for hendelseshåndtering, lukking av avvik og kontinuitet,
- sørge for kontroll med tjenesteleverandører,
- ha internkontroll for behandling av personopplysninger,

[50] Kravene i policyen baserer seg på lovkrav, blant annet i forvaltningsloven og e-forvaltningsforskriften, sikkerhetsloven med forskrifter, personopplysningsloven og personvernforordningen, og reglement for økonomistyring i staten.

- ivareta de registrertes rettigheter,
- utnevne personvernombud,
- gjennomføre vurderinger av personvernkonsekvenser (DPIA),
- sørge for innebygd personvern og informasjonssikkerhet,
- sørge for opplæring og kompetanseheving,
- dokumentere arbeidet med informasjonssikkerhet og personvern.

Vedlegg 2: Rammeverk for vurdering av risiko

Sannsynlighetsverdier (hendelsesfrekvens)

Svært lite sannsynlig: Det forventes at hendelsen kan skje sjeldnere enn hvert femte år.

Lite sannsynlig: Det forventes at hendelsen kan skje sjeldnere enn hvert år, men oftere enn hvert femte år.

Mulig: Det forventes at hendelsen kan skje hvert år.

Sannsynlig: Det forventes at hendelsen kan skje 2 til 4 ganger hvert år.

Svært sannsynlig: Det forventes at hendelsen kan skje flere ganger hver måned.

Konsekvensverdier

Svært lav: Dette er hendelser hvor konsekvensene kan være at personopplysninger kan være midlertidig utilgjengelige for den registrerte, eller enkelte mindre viktige opplysninger kan være misvisende. En intern bruker kan ha tilgang til noen få alminnelige opplysninger etter at behovet er bortfalt. En hendelse kan føre til noe ekstraarbeid og mindre misnøye blant enkelte ansatte eller studenter.

Lav: Dette er hendelser hvor konsekvensene kan være at små mengder alminnelige personopplysninger kan være eksponert for uvedkommende, eller være utilgjengelige i inntil fem dager. Enkeltpersoner kan ha blitt lurt til å betale små beløp i forbindelse med nettfiske eller svindel. Det kan oppstå misnøye blant viktige interne brukergrupper, og enkelte forskningsdata kan være eksponert for uvedkommende.

Middels: Dette er hendelser hvor konsekvensene kan være at moderate mengder alminnelige personopplysninger kan være eksponert eller feilaktige, og være utilgjengelige i inntil fem dager. Tjenester som ikke er kritiske kan være utilgjengelige i én til tre dager. Det kan føre til omtale i lokale/regionale medier, og forskningsdata med betydning for nasjonale interesser kan være kompromittert.

Høy: Dette er hendelser hvor konsekvensene kan være at større mengder personopplysninger kan være eksponert eller feilaktige, og være utilgjengelige i opptil én måned. Kritiske tjenester kan være utilgjengelige i én til sju dager, eller ustabile i viktige perioder som eksamen. Hendelsen kan føre til større økonomiske tap, negativ nasjonal medieomtale og brudd på internasjonale sanksjoner.

Svært høy: Dette er hendelser hvor konsekvensene kan være at sensitive personopplysninger kan være eksponert i stort omfang, og være utilgjengelige i mer enn én måned. Kritiske tjenester og tidskritiske data kan være utilgjengelige i over én uke. Hendelsen kan føre til tap av uerstattelige data, store økonomiske kostnader, riksmedieomtale over en lengre periode og alvorlig svekkelse av nasjonale interesser.

Når en uønsket hendelse har flere konsekvenser med ulik alvorlighet, legges den mest alvorlige konsekvensen til grunn for vurderingen av risiko.

Risikomatrise:

Konsekvens						
	Svært høy	**5**	**10**	**15**	**20**	**25**
	Høy	**4**	**8**	**12**	**16**	**20**
	Middels	**3**	**6**	**9**	**12**	**15**
	Lav	**2**	**4**	**6**	**8**	**10**
	Svært lav	**1**	**2**	**3**	**4**	**5**
		Svært lite sannsynlig	**Lite sannsynlig**	**Mulig**	**Sannsynlig**	**Svært sannsynlig**
		Sannsynlighet				

Vedlegg 3: Ressurser og veiledninger

Det finnes ulike nettressurser som kan brukes i arbeidet med sikkerhet og beredskap. Flere av dem fremgår av referanselisten i denne rapporten, men vi ønsker likevel å peke særskilt på følgende ressurser:

Nasjonal sikkerhetsmyndighets veileder for sikkerhetsstyring for råd og veiledning om styringssystem for sikkerhet: veileder-i-sikkerhetsstyring.pdf, sist besøkt 04.07.2025.

Digitariseringsdirektoratets nettsider for råd og veiledning om ledelsessystem for informasjonssikkerhet: Internkontroll/ styringssystem/ ledelsessystem for informasjonssikkerhet | Digdir, sist besøkt 04.07.2025.

Datatilsynets nettsider for råd og veiledning om internkontroll for personvern: Etablere internkontroll | Datatilsynet, sist besøkt 04.07.2025.

Sikts oversikt over veiledere for råd og veiledning om blant annet verdioversikt, klassifisering av verdier og kontinuitetsplaner: Anbefalinger for arbeid med sikkerhet og beredskap, sist besøkt 04.07.2025.

Direktoratet for samfunnssikkerhet og beredskap sin veileder for øvelser: *Øvingsveiledning*, sist besøkt 04.07.2025.

Figurliste

Direktoratet for
høyere utdanning
og kompetanse

post@hkdir.no hkdir.no