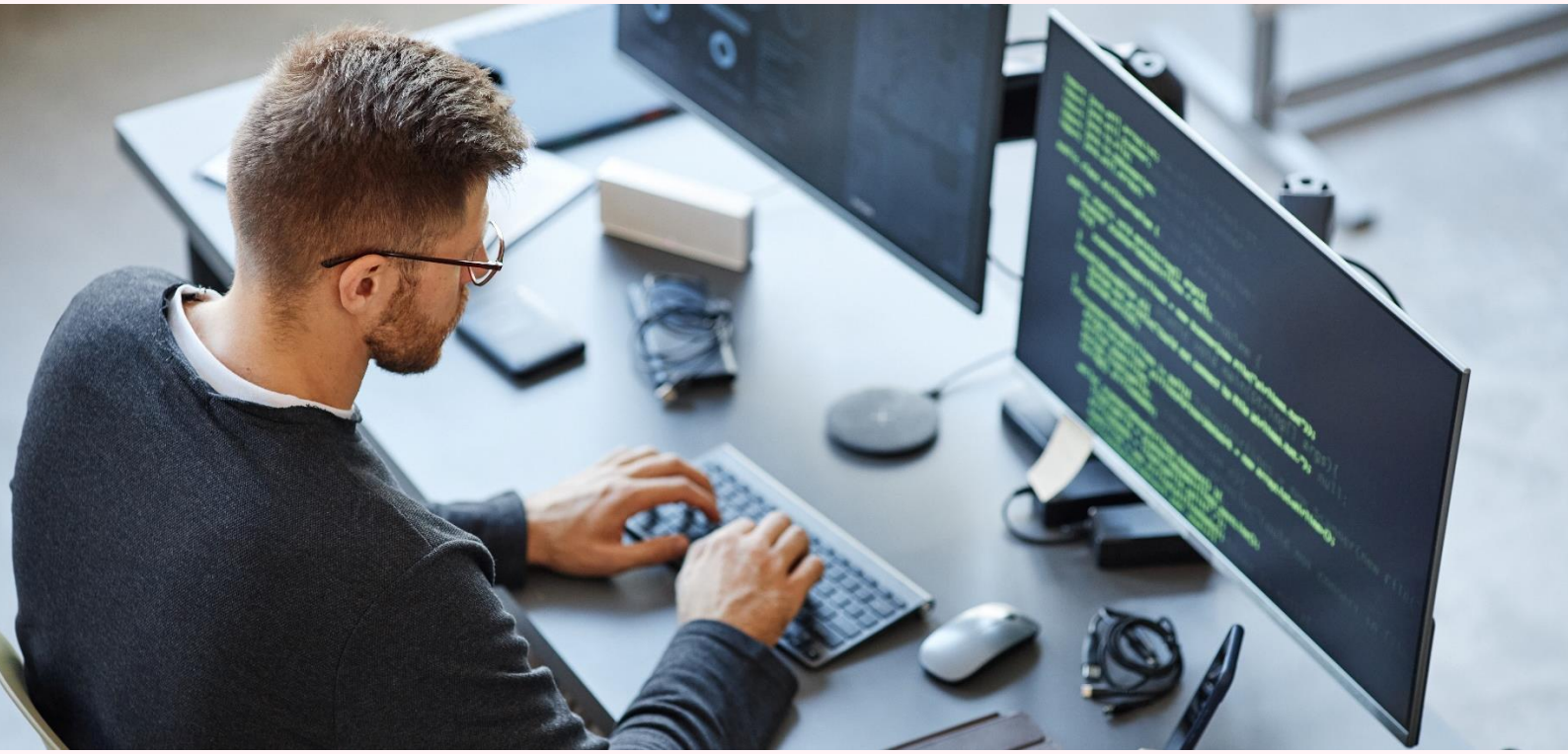
Riksrevisjonen

Informasjonssikkerhet i forskning innenfor kunnskapssektoren

Offentlig versjon av Dokument 3:11 (2023–2024)

Deler av rapporten er unntatt offentlighet. Noe informasjon er også gradert BEGRENSET etter sikkerhetsloven.



Forsidefoto: SeventyFour / Shutterstock / NTB
ISBN 978-82-8229-585-7

Riksrevisjonen

Til Stortinget

Riksrevisjonen legger med dette fram Dokument 3:11 (2023−2024) *Informasjonssikkerhet i forskning innenfor kunnskapssektoren*

Dokumentet har følgende inndeling:

- Riksrevisjonens konklusjoner, utdyping av konklusjoner, anbefalinger, statsrådens svar og Riksrevisjonens uttalelse til statsrådens svar
- Vedlegg 1: Riksrevisjonens brev til statsråden
- Vedlegg 2: Statsrådens svar
- Vedlegg 3: Forvaltningsrevisjonsrapport med vurderinger – offentlig versjon

I vedlegg 3 er noe informasjon skjermet ved bruk av «sladding». Dette gjelder informasjon som er unntatt offentlighet jf. offentleglova § 24 tredje ledd, og noe informasjon som også er gradert BEGRENSET jf. sikkerhetsloven § 5-3 første ledd bokstav d. Stortinget mottar også en usladdet versjon av dette vedlegget.

Riksrevisjonen, 16. januar 2024

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen

riksrevisor

Innhold

Riksrevisjonen kan gi kritikk etter disse tre alvorlighetsgradene:

1. **Sterkt kritikkverdig** er Riksrevisjonens sterkeste kritikk. Vi bruker dette kritikknivået når vi finner alvorlige svakheter, feil og mangler. Ofte vil disse kunne få svært store konsekvenser for enkeltmennesker eller samfunnet.
2. **Kritikkverdig** bruker vi når vi finner betydelige svakheter, feil og mangler som ofte vil kunne få moderate til store konsekvenser for enkeltmennesker eller samfunnet.
3. **Ikke tilfredsstillende** bruker vi når vi finner svakheter, feil og mangler, men som i mindre grad får direkte konsekvenser for enkeltmennesker eller samfunnet.

1 Innledning

Sikkerhetssituasjonen innenfor høyere utdannings- og forskningssektoren har blitt mer utfordrende de siste årene. Antallet registrerte dataangrep mot sektoren økte kraftig på verdensbasis både i 2020 og 2021.[1] Sikkerhetssituasjonen ble ytterligere skjerpet da Russland invaderte Ukraina i 2022.[2] I sine risikovurderinger for 2020, 2021, 2022 og 2023 har PST[3], Etterretningstjenesten[4] og NSM[5] pekt på at norske forskningsmiljøer er utsatte etterretningsmål. Direktoratet for høyere utdanning og kompetanse (HK-dir) rapporterer også om en sikkerhetssituasjon preget av større trusler og flere hendelser i Norge.[6]

I tillegg til trusselen fra utenlandsk etterretning vil også kriminelle aktører ha interesse for forskningsdata og -systemer. Politiets trusselvurdering 2023 anser løsepengevirus[7] rettet mot bedrifter og virksomheter som den største kriminalitetstrusselen mot IT-sikkerhet og digital infrastruktur.[8] I sin risiko- og tilstandsvurdering for 2023 vurderer HK-dir at risikoen for løsepengevirus, som fører til brudd på informasjons- og personopplysningssikkerheten, er høy innenfor forsknings- og utdanningssektoren.

En sentral årsak til at sektoren er interessant for angripere, er at den inneholder store informasjonsverdier i form av forskningsdata. Svak sikring av forskningsdata kan potensielt få store økonomiske konsekvenser, føre til spredning av sensitive opplysninger som personopplysninger og forretningshemmeligheter og gjøre at virksomhetene taper omdømme. Noen universiteter og høyskoler forsker på områder som er viktige for å sikre nasjonale interesser, for eksempel forskning på olje og energi, elektronisk kommunikasjon (ekom), forsvarsmateriell og annen flerbruksteknologi.[9]

Det er et viktig prinsipp for offentlig finansierte forskningsdata at disse skal være «så åpne som mulig, så lukkede som nødvendig».[10] Prinsippet innebærer en forventning om at forskningsdata skal tilrettelegges for åpen tilgang så framt ikke hensynet til sikkerhet, personvern, immaterielle rettigheter, forretningshemmeligheter og lignende tilsier at dataene må skjermes. Virksomhetene må finne en balanse mellom disse hensynene. Samtidig begrenser ikke trusselen mot forskning seg kun til sensitive kunnskapsområder. En angriper kan også gjøre utilgjengelig eller slette andre viktige forskningsdata eller manipulere dataene. Mer generelt vil tilliten

[1] Hystad, J. (2020, 26. september). Kraftig økning i dataangrep mot utdanningssektoren. *Khrono*. https://khrono.no/kraftig-okning-i-dataangrep-mot-utdanningssektoren/517861; Strand, H. K. og Hystad, J. (2022, 7. februar). Opplever 1600 dataangrep i veka: — Ein indikator på stor verdi. *Khrono*. https://khrono.no/opplever-1600-dataangrep-i-veka-ein-indikator-pa-stor-verdi/657438

[2] NSM Risiko (2023).

[3] Nasjonal trusselvurdering (2020), Nasjonal trusselvurdering (2021), Nasjonal trusselvurdering (2022), Nasjonal trusselvurdering (2023).

[4] Fokus (2020), Fokus (2021), Fokus (2022), Fokus (2023).

[5] NSM Risiko (2020), NSM Risiko (2021), NSM Risiko (2022), NSM Risiko (2023).

[6] Unit. (2021). *Risiko- og tilstandsvurdering 2021: Informasjonssikkerhet og personvern i høyere utdanning og forskning*; HK-dir. (2022). *Risiko- og tilstandsvurdering 2022: Informasjonssikkerhet og personvern i høyere utdanning og forskning*; HK-dir. (2023). *Risiko- og tilstandsvurdering 2023: Informasjonssikkerhet og personvern i høyere utdanning og forskning*.

[7] I denne typen angrep brukes skadevare til å kryptere data i offerets datasystem, før aktøren krever løsepenger mot å heve kryptering.

[8] Politiets sikkerhetsvurdering 2023, side 16.

[9] Flerbruksteknologi omfatter teknologier og produkter som kan anvendes både til sivile og militære formål. Kilde: NSM Risiko (2023), side 36-37.

[10] Nasjonal strategi for tilgjengeliggjøring og deling av forskningsdata, side 3.

til forskning svekkes hvis det mistenkes at eksterne aktører har hatt tilgang til forskningen og resultatene av den.

Målet med undersøkelsen har vært å vurdere

- hvordan forskningsinstitusjoner under Kunnskapsdepartementet sikrer forskningsdata mot dataangrep, og
- hvordan departementet ivaretar sitt overordnede ansvar for informasjonssikkerhet i høyere utdanning og forskning.

Med forskningsinstitusjoner under Kunnskapsdepartementet mener vi universiteter, høyskoler og andre virksomheter under departementet som driver med forskning.

Undersøkelsen har blant annet tatt utgangspunkt i følgende vedtak og forutsetninger fra Stortinget:

- *Lov om behandling av personopplysninger*
- *Lov om helseregistre og behandling av helseopplysninger*
- *Lov om medisinsk og helsefaglig forskning*
- *Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.*
- *Lov om nasjonal sikkerhet*
- *Bevilgningsreglementet*
- *Reglement for økonomistyring i staten*
- Innst. 275 S (2020−2021) *Innstilling fra justiskomiteen om Samfunnssikkerhet i en usikker verden, jf.* Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*
- Innst. 187 S (2017−2018) *Innstilling fra justiskomiteen om IKT-sikkerhet. Et felles ansvar, jf.* Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*
- Prop. 1 S (2018–2019) Kunnskapsdepartementet, jf. Innst. 12 S (2018–2019)
- *Instruks for departementenes arbeid med samfunnssikkerhet*

Vi har gjennomført undersøkelser hos til sammen ti forskningsinstitusjoner under Kunnskapsdepartementet.[11] For alle virksomhetene har vi undersøkt tekniske og organisatoriske sikkerhetstiltak, og systematikken i arbeidet med informasjonssikkerhet. I tre av virksomhetene har vi gått mer i dybden, og blant annet gjennomført inntrengingstester.

Et sentralt metodisk grep i undersøkelsen er å sammenligne det vi har funnet i alle de ti virksomhetene med god praksis, som framgår av anerkjente standarder for informasjonssikkerhet. Vi har i hovedsak tatt utgangspunkt i følgende standarder:

- Center for Internet Security (2021) CIS Controls, version 8
- Nasjonal Sikkerhetsmyndighet (2020) Grunnprinsipper for IKT-sikkerhet, versjon 2.0
- Informasjonsteknologi – Sikringsteknikker – Tiltak for informasjonssikring, NS-ISO/IEC 27002:2017
- NS-ISO/IEC 27001:2017 – Ledelsessystemer for informasjonssikkerhet.

[11] Nord universitet, Norges idrettshøgskole, Norges teknisk-naturvitenskapelige universitet, Norsk utenrikspolitisk institutt, Universitetet i Bergen, Universitetet i Oslo, Universitetet i Stavanger, Universitetet i Sørøst-Norge, Universitetet i Tromsø – Norges arktiske universitet og Universitetssenteret på Svalbard AS

De tre virksomhetene i dybdeundersøkelsene ble informert om alle svakheter vi fant gjennom inntrengingstestene, like etter at disse var gjennomført. Alle de ti virksomhetene fikk en presentasjon av svakheter som vi avdekket gjennom kartlegging av tekniske sikkerhetstiltak.

Undersøkelsen omfatter i hovedsak perioden 2019–2022.

Rapporten ble forelagt Kunnskapsdepartementet ved brev 29. september 2023. Departementet har i brev 27. oktober 2023 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten og i dette dokumentet.

Riksrevisjonen har hatt en dialog med Kunnskapsdepartementet om hvilke opplysninger som bør utelates fra dette dokumentet, og om behov for skjerming av opplysninger i den mer detaljerte forvaltningsrevisjons-rapporten (vedlegg). I den forbindelse har vi også fått råd fra Nasjonal sikkerhetsmyndighet (NSM).

Rapporten, riksrevisorkollegiets oversendelsesbrev til departementet [Dato] og statsrådens svar [Dato] følger som vedlegg.

2 Konklusjoner

Konklusjoner

- Forskningsdata i forskningsinstitusjonene under Kunnskapsdepartementet er ikke i tilstrekkelig grad sikret mot dataangrep.
  - Inntrengingstester mot tre virksomheter ga full kontroll over IT-infrastruktur ved to av dem, og kontroll over forskeres IT-utstyr og skylagring ved det tredje.
  - Det er stor variasjon i gjennomføringen av tekniske sikkerhetstiltak, og mange av virksomhetene har vesentlige svakheter
  - Det er svakheter i organisatoriske sikkerhetstiltak som er etablert for å beskytte forskningsdata
- Virksomhetene har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen
- Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer.
  - Styringsmodellen for informasjonssikkerhet har gjort at den enkelte forskningsvirksomhet har fått tettere oppfølging
  - Kunnskapsdepartementet har i begrenset grad lyktes med å nå målet med informasjonssikkerhetssatsningen, og virkemidlene treffer i for liten grad virksomhetene som har størst behov for støtte
- Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp

3 Overordnet vurdering

- Det er kritikkverdig at forskningsdata i virksomheter under Kunnskapsdepartementet ikke er tilstrekkelig sikret mot dataangrep, gitt kravene i lovverket og de mulige konsekvensene av at sensitive data kommer på avveier.
- Virksomhetene har ikke god nok oversikt over forskningsdata som trenger beskyttelse. Dette er ikke tilfredsstillende.
- Tross forbedringer i undersøkelsesperioden, arbeider mange virksomheter i for liten grad systematisk med informasjonssikkerhet, og styrene i virksomhetene fyller ikke i stor nok grad rollen de skal ha. Dette er ikke tilfredsstillende.
- Kunnskapsdepartementet har gjennomført flere tiltak i perioden 2019–2022 som blant annet har ført til økt oppmerksomhet om informasjonssikkerhet i virksomhetene. Samtidig er det ikke tilfredsstillende at virkemidlene i for liten grad treffer virksomhetene som har størst behov for støtte.
- Det er ikke tilfredsstillende at departementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og at risikoreduserende tiltak ikke blir fulgt opp.

4 Utdyping av konklusjoner

4.1 Forskningsdata i forskningsvirksomhetene under Kunnskapsdepartementet er ikke i tilstrekkelig grad sikret mot dataangrep

Forskningsdata skal i hovedsak tilrettelegges for åpen tilgang, men hensyn til sikkerhet, personvern, immaterielle rettigheter, forretningshemmeligheter og lignende tilsier i en del tilfeller at forskningsdata ikke kan gjøres helt åpent tilgjengelige. En rekke lover og regler stiller krav til hvordan slike data skal sikres. Lovverket stiller også konkrete krav til virksomhetene om at de skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset risikoen. For å oppnå dette bør virksomhetene følge faglige standarder som angir god praksis.

Etter Riksrevisjonens vurdering er forskningsdata i virksomheter under Kunnskapsdepartementet ikke tilstrekkelig sikret mot dataangrep, gitt kravene i lovverket.

4.1.1 Inntrengingstester mot tre forskningsinstitusjoner ga full kontroll over IT-infrastruktur ved to av dem og kontroll over forskeres IT-utstyr og skylagring ved det tredje

Forskningsinformasjon og kunnskap generert av forskning kan være av stor interesse både for etterretningsorganisasjoner og kommersielle virksomheter. Det samles også inn store mengder, til dels sensitive, forskningsdata om personer som mange aktører kan ha interesse av og kan forsøke å utnytte blant annet i kriminell virksomhet. Riksrevisjonen gjennomførte inntrengingstester mot tre forskningsinstitusjoner for å teste hvor godt forskningsdata var beskyttet. Målet i testene var å få tilgang til sensitive forskningsdata, enten ved å få kontroll over IT-infrastruktur eller ved å utnytte tilgangsrettighetene den enkelte forsker har.

Inntrengingstestene ved to av virksomhetene ga full kontroll over IKT-infrastrukturen som benyttes av ansatte og studenter i deres daglige arbeid. Ved en av dem ble dette oppnådd den første dagen av inntrengingstesten, og det ble funnet flere veier som kunne gi slik kontroll.

Oppnådd kontroll innebar at vi kunne administrere alle brukerkontoer, PC-er og servere. Med slik tilgang kunne vi tildele oss selv alle ønskede rettigheter og skaffe oss tilgang til all informasjon lagret i dette nettverket, inkludert sensitiv forskningsinformasjon. Med rettighetene vi oppnådde, hadde det også vært mulig å endre, slette eller kryptere all informasjon dersom motivasjonen hadde vært økonomisk vinning eller sabotasje.

Ved den tredje forskningsinstitusjonen fikk vi kontroll med de fleste PC-er benyttet av ansatte, noe som ga muligheter til å hente ut eller manipulere informasjon lagret lokalt på PC-er og på eiernes skylagringsløsning. Denne skylagringsløsningen kan ut fra retningslinjer benyttes for sensitive forskningsdata (opp til nivået «fortrolig») ved flere av forskningsinstitusjonene. Tilgangen vi oppnådde kunne videre vært brukt til

et målrettet angrep mot utvalgte forskere med kunnskap og tilgang til informasjon som angriperen ønsker tilgang til. Vi fikk ikke kontroll med servere og datanettverk generelt ved den tredje forskningsinstitusjonen, fordi de sentrale delene av IT-infrastrukturen er bedre beskyttet.

Et av formålene med inntrengingstestene var å undersøke virksomhetenes evne til å oppdage aktiviteter i et dataangrep. Vi gjorde ingen forsøk på å skjule våre simulerte angrep, men produserte mye nettverkstrafikk og kjente tegn på angrep. Ved to av virksomhetene ble få eller ingen av aktivitetene i inntrengningstestene oppdaget. Ved den siste virksomheten ble inntrengingstesten oppdaget den fjerde testdagen, og de fleste aktivitetene ga spor i logger som kunne gi virksomheten et bilde av hvordan angrepet hadde blitt gjennomført og hvilke systemer som var berørte.

Noe sensitiv forskningsinformasjon er lagret i særskilte tjenester som er satt opp for å gi informasjonen bedre beskyttelse. Disse tjenestene har ikke vært omfattet av inntrengingstesten. Kontrollen vi oppnådde over forskeres brukerkontoer og IT-utstyr kunne imidlertid vært brukt som utgangspunkt for et angrep for å få tilgang også til informasjon som forskere har lagret her.

De tre virksomhetene som ble testet har alle planlagt og til dels gjennomført en rekke tiltak som øker deres sikkerhet i etterkant av våre undersøkelser. De konkrete svakhetene som ble utnyttet i inntrengingstestene er utbedret.

Inntrengingstestene ga full kontroll i to virksomheter blant annet fordi det benyttes svake passord, mange brukerkontoer tildeles store rettigheter, og det er svakheter i beskyttelsen av nettverk. I tillegg ble lite oppdaget fordi overvåkningen var mangelfull. Kontroll av sikkerhetstiltak omtalt nedenfor viser at disse svakhetene er vanlige i virksomhetene i sektoren. Det gir grunn til å tro at inntrengingstester ved andre virksomheter i sektoren kunne gitt lignende resultater. Etter Riksrevisjonens vurdering viser dette at mange av forskningsinstitusjonene ikke er godt nok beskyttet mot dataangrep.

4.1.2 Det er stor variasjon i gjennomføringen av tekniske sikkerhetstiltak, og mange av virksomhetene har vesentlige svakheter

Forskningsinstitusjonene skal gjennomføre tekniske sikkerhetstiltak for å oppnå en egnet sikring av sine IKT-systemer og informasjonen som er lagret. Tekniske sikkerhetstiltak skal bidra til å forebygge at dataangrep lykkes. Det er også viktig å ha tiltak for å oppdage de angrep man ikke klarer å forebygge.

For å få et bredere bilde enn det som inntrengingstestene kunne gi, har vi undersøkt tekniske sikkerhetstiltak ved ti forskningsinstitusjoner. Undersøkelsen viser at sentrale anbefalinger i NSMs Grunnprinsipper for IKT-sikkerhet, som anses som god praksis, ikke følges av mange av de undersøkte virksomhetene. Undersøkelsen viser:

1. **Mangelfull kontroll med brukerkontoer og tilgangsrettigheter**: Flere av virksomhetene har mange brukerkontoer med høye rettigheter og tilgangsrettigheter som ikke reflekterer arbeidsdeling ved drift av

systemer. Dette gjør det lettere for en angriper å eskalere rettigheter og få kontroll med all IKT-infrastrukturen når et fotfeste er etablert.

2. **Svake krav til brukerautentisering**: Krav til passord varierer, og det er ofte ikke satt sterkere krav til passord for kontoer som har høye rettigheter. Lave krav gjør det mulig å gjette eller knekke passord. Tofaktor-autentisering er innført mange steder, men det gjelder ikke alle tjenester og påloggingsmuligheter
3. **Mangelfull sårbarhetsstyring av IT-utstyr og programvare**: De fleste virksomhetene har på plass rutiner for sikkerhetsoppdatering av programvare for å fjerne kjente sårbarheter, men flere virksomheter har ikke god helhetlig sårbarhetsstyring som kan hindre og oppdage sårbarheter. Dette øker risikoen for at en angriper kan finne og utnytte sårbarheter i et dataangrep.
4. **Det er svakheter i nettverkssikkerheten**: Universitetene og høyskolene i undersøkelsen er åpne virksomheter, samtidig som det er svakheter i sikkerhetstiltak for å beskytte egne nettverk.
5. **Mangelfull logging og overvåkning**: Det er mangler i datagrunnlaget for å oppdage og håndtere dataangrep ved at det ofte logges mindre enn anbefalt. Enkelte av virksomhetene har etablert et godt grunnlag for å oppdage dataangrep, men flere har enklere overvåkningsløsninger og mindre kapasitet til å gjennomgå overvåkningsdata.

Nivået på sikkerhetstiltakene i forskningsvirksomhetene varierer imidlertid betydelig, og de har også ulike sikkerhetsmessige utfordringer. Enkelte gjennomfører i stor grad systematiske sikkerhetstiltak og er mer robuste mot dataangrep, men har utfordringer med å sikre at tiltak gjennomføres konsekvent i hele virksomheten. Flere virksomheter har imidlertid kommet kortere, har klare mangler i tekniske sikkerhetstiltak og begrenset evne til å oppdage dataangrep.

Undersøkelsen viser forbedringer i tekniske sikkerhetstiltak de seneste årene, som kan ha sammenheng med økt oppmerksomhet om risikoen i sektoren og i samfunnet generelt. For eksempel er tofaktorautentisering innført for mange tjenester, og ekstern sårbarhetsskanning er etablert av Sikt – Kunnskapssektorens tjenesteleverandør.

For flere av forskningsinstitusjonene er påviste svakheter i tekniske sikkerhetstiltak av en slik karakter at det vil ta tid å nå et tilfredsstillende sikkerhetsnivå. Etter Riksrevisjonens vurdering er det for store svakheter i grunnleggende tekniske sikkerhetstiltak i mange av forskningsvirksomhetene og dermed viktig med et systematisk arbeid for å oppnå en bedre beskyttelse mot dataangrep.

4.1.3 Det er svakheter i organisatoriske sikkerhetstiltak som er etablert for å beskytte forskningsdata

For at en virksomhet skal oppnå et egnet sikkerhetsnivå må de tekniske sikkerhetstiltakene omtalt over kombineres med sikkerhetstiltak i organisasjonen og rettet mot den enkelte bruker av IT-systemer. For alle de ti virksomhetene har vi derfor gjennomgått utvalgte organisatoriske sikkerhetstiltak som er ment å beskytte forskningsdata, og undersøkt om

disse er i tråd med god praksis. Undersøkelsen viser flere svakheter i gjennomføringen av disse tiltakene:

- **Virksomhetene har ikke god nok oversikt over forskningsdata.** Dette innebærer at de mangler grunnlag til å vurdere hva som bør beskyttes, og hvordan dette bør gjøres. Virksomhetene har i liten grad oversikt over andre sensitive forskningsdata enn de som omfatter personopplysninger. De fleste virksomhetene har en relativt god oversikt over personopplysninger i forskning, men oversiktene er ikke komplette.
- **Det gis lite veiledning om sikker behandling av forskningsdata utover personopplysninger.** Ni av ti virksomheter gir føringer om klassifisering av informasjon etter konfidensialitet, og tillatte lagringsløsninger. Disse virksomhetene har også utarbeidet rutiner for behandling av personopplysninger i forskning. Det er gjennomgående lite veiledning rundt klassifisering og lagring av andre sensitive forskningsdata.
- **Opplæring og bevisstgjøring om informasjonssikkerhet og håndtering av forskningsdata er lite systematisk ved de fleste av virksomhetene.** Alle virksomhetene har gjennomført enkeltstående opplæringstiltak og tilbyr noe støtte innenfor informasjonssikkerhet og personvern hvor forskere, veiledere og studenter kan få hjelp ved behov. Likevel tyder undersøkelsen på at forskerne i varierende grad kjenner til regler om informasjonssikkerhet, og at mange opplever klassifisering av data som skal beskyttes som vanskelig.
- **IT-systemer driftet lokalt i fakulteter, institutter og lignende omfattes ofte ikke av virksomhetenes sentrale retningslinjer og rutiner.** Det er i liten grad stilt krav eller gitt føringer om sikkerhetstiltak til lokale driftsansvarlige for drift av disse systemene. Lokale driftsansvarlige har også i liten grad laget skriftlige retningslinjer eller andre kravdokumenter for løsningene de drifter. Omfanget av lokal drift varierer mellom virksomhetene. Undersøkelsen viser imidlertid at trenden går i retning av sentralisering av IT-drift og/eller skjerping av kravene til lokale IT-miljøer.
- **Sikkerheten hos leverandører av IT-løsninger blir i liten grad fulgt opp av virksomhetene.** Virksomhetene har tjenesteutsatt store deler av databehandlingen i forskning, undervisning, administrasjon og formidling. Mange av virksomhetene oppgir at de gjør vurderinger av informasjonssikkerhet hos leverandørene ved innkjøp av nye IT-løsninger, men det er svært begrenset oppfølging i etterkant av dette.

Undersøkelsen viser at det er gjort forbedringer i gjennomføringen av disse organisatoriske sikkerhetstiltakene de siste årene. Spesielt har virksomhetene, som en oppfølging av den nye personopplysningsloven i 2018, arbeidet med å kartlegge og forbedre rutiner for behandling av personopplysninger. Arbeidet med andre organisatoriske sikkerhetstiltak har imidlertid virksomhetene kommet kortere med. Etter Riksrevisjonens vurdering er det særlig et behov for bedre sikkerhetstiltak for å identifisere og beskytte forretningssensitiv informasjon og informasjon som kan være av interesse for fremmede stater.

4.2 Virksomhetene har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen

Virksomhetene skal ha et ledelsessystem for informasjonssikkerhet. Ledelsessystemet skal sette planlegging, gjennomføring, kontroll/evaluering og oppfølging av informasjonssikkerhetsarbeidet i system. Systemet skal sikre at passende sikkerhetstiltak gjennomføres og tilfredsstillende sikkerhet oppnås.

Undersøkelsen viser at de fleste virksomhetene har lagt rammene for arbeidet med informasjonssikkerhet ved å etablere de overordnede dokumentene i et ledelsessystem. Alle virksomhetene i undersøkelsen unntatt én hadde dokumentert et ledelsessystem på undersøkelsestidspunktet. Arbeidet med informasjonssikkerhet har fått mer oppmerksomhet de siste årene, og ansvaret for dette arbeidet i virksomhetene er i hovedsak klarlagt.

Selv om arbeidet med informasjonssikkerhet har kommet lenger, er det fortsatt mangler i implementeringen av ledelsessystemene i virksomhetene. De viktigste utfordringene er

- **ledelsessystem.** Implementeringen av ledelsessystemet på et konkret nivå er ofte mangelfull, selv om overordnede policyer er vedtatt. Bare tre av de ti virksomhetene stiller for eksempel tydelige krav i temaspesifikke policyer til tekniske sikkerhetstiltak som vi har kontrollert i denne undersøkelsen. Der det ikke stilles konkrete krav, blir det i stor grad opp til den enkelte IT-ansatte å vurdere hva som er tilstrekkelig sikkerhet.
- **gjennomføring av besluttede tiltak.** Planer for å iverksette strategier ut fra policyer som ledelsen har vedtatt, er ofte mangelfulle fordi de ikke dekker hele virksomheten, plangrunnlaget er mangelfullt og tidsfrist og ansvar for oppgaver ikke er definert. Samtidig viser undersøkelsen at virksomhetene har utfordringer med å gjennomføre tiltak som er besluttet.
- **risikostyring.** Undersøkelsen viser at det gjøres langt færre risikovurderinger enn hva virksomhetene selv setter krav om, og at det i liten grad gjennomføres systematiske risikovurderinger av IT-infrastruktur. Videre bygger ikke overordnede risikovurderinger klart på informasjon fra mer detaljerte risikovurderinger av de enkelte IT-systemer mv. Svakhetene i risikostyringen gjør at mange av virksomhetene har et dårlig grunnlag for å vurdere hvilke sikkerhetstiltak som skal implementeres, og for å gjennomføre vedtatte tiltak.
- **evalueringer og etterkontroller av sikkerhetstilstanden.** I de fleste virksomhetene er det begrenset med kontroll og evalueringer av arbeidet med informasjonssikkerhet og personvern samt av hvordan forskningsdata behandles. Noen virksomheter har ikke satt krav om kontroller og evalueringer i ledelsessystemet. Andre har satt krav, men sliter med å gjennomføre vedtatte kontroller og evalueringer. Dermed har mange av virksomhetene lite kunnskap om ledelsessystemet og

sikkerhetstiltakene fungerer som forutsatt, og om hva som faktisk er sikkerhetstilstanden i virksomheten.

- **avklaringer om roller og ansvar.** Selv om ansvar på et overordnet nivå er avklart i de fleste virksomheter, er det eksempler på at arbeidet med informasjonssikkerhet har blitt hemmet av at det mangler en overordnet/samlende rolle. I flere virksomheter er det noe uklarhet både om hvilke tekniske sikkerhetstiltak som skal implementeres, og hvem som har ansvaret for å følge opp at tiltakene blir iverksatt i IT-driften. I flere virksomheter er det ikke klart hvem som har ansvaret for organisatoriske sikkerhetstiltak som opplæring og bevisstgjøring.
- **kompetanse og ressurser.** Det er store forskjeller mellom virksomhetene med hensyn til tilgang til ressurser og kompetanse om informasjonssikkerhet. Det varierer mellom virksomhetene hvor mye ressurser de kan sette av til informasjonssikkerhet, og i hvilken grad de har mulighet til å tiltrekke seg spesialistkompetanse. Kompetanse og ressurser er nødvendig for å identifisere og iverksette nødvendige sikkerhetstiltak.
- **ledelsens informasjonsgrunnlag.** I syv av ti virksomheter har toppledelsen gjennomgått status for ledelsessystemet og sikkerhetstilstanden ett eller flere av årene i undersøkelsesperioden. Innholdet i gjennomgangene varierer imidlertid betydelig, og få av virksomhetene bruker resultatet fra risikoarbeidet eller statusen for gjennomføring av tiltaksplaner i særlig grad. Dermed har ledelsen ofte ikke et fullstendig bilde av hvordan sikkerhetstilstanden er, og et svakt grunnlag for å kunne vurdere tiltak.
- **styrets rolle.** I flere virksomheter mottar styret lite av informasjonen de trenger for å ivareta sin rolle som det organet med det øverste ansvaret for informasjonssikkerheten. I noen virksomheter er det heller ikke definert hva som er styrets rolle og ansvar i ledelsessystemet, eller det er uklart hvilken informasjon styret skal motta.

Det er stor variasjon i virksomhetenes arbeid med informasjonssikkerhet. Dette er til dels naturlig da de har svært ulik størrelse, ulikt omfang av forskningsdata og ulik kompleksitet i IT-infrastruktur. Hvordan utfordringene i punktlisten ovenfor skal tas tak i, må være tilpasset virksomhetene.

Selv om informasjonssikkerhet har fått mer oppmerksomhet de senere årene og ledelsessystem er utarbeidet i virksomhetene, gjenstår det betydelig arbeid for å implementere systemene fullt ut slik at de oppnår ønsket sikkerhetsnivå. Styret har det øverste ansvaret for å håndtere risikoen for informasjonssikkerheten og for at virksomheten har systemer som hindrer at sensitive forskningsdata i virksomheten kommer på avveier. Etter Riksrevisjonens vurdering mottar de fleste styrene for lite informasjon om informasjonssikkerhetsrisikoen til å kunne ta stilling til sikkerhetsnivået. Trusselsituasjonen i sektoren er betydelig skjerpet de siste årene, og etter Riksrevisjonens vurdering er det viktig at styrene tar sitt ansvar for å påse at virksomhetene har god nok informasjonssikkerhet.

4.3 Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer

Departementet har ansvar for å avklare sentrale roller og ansvarsområder på informasjonssikkerhetsområdet og sørge for at den overordnede organiseringen og virkemiddelbruken på området er ressurseffektiv. Departementet har videre ansvar for å følge opp at underliggende virksomheter jobber for å nå mål og oppfylle krav på informasjonssikkerhetsområdet. Det innebærer blant annet å gi føringer på området og sørge for at virksomhetene gir dem et tilstrekkelig informasjonsgrunnlag for styringen. Departementet bør også vurdere hensiktsmessige virkemidler overfor de aktørene i sektoren der departementet mangler direkte styringslinjer.

I 2019 satte Kunnskapsdepartementet i gang et fireårig informasjonssikkerhetsprogram i universitets- og høyskolesektoren. Målet med programmet var å styrke informasjonssikkerheten i sektoren. Programmet skulle forbedre sektorens evne til å forebygge, oppdage og håndtere trusler mot forskningsnettet, og det skulle inkludere tiltak som analyseverktøy og kompetanseheving.

Sentrale resultater av satsingen er at det ble etablert

- en styringsmodell for informasjonssikkerhet, hvor ansvaret ble gitt til HK-dir – Direktoratet for høyere utdanning og kompetanse
- et Cybersikkerhetssenter for høyere utdanning og forskning, eduCSC, hvor ansvaret er gitt til Sikt – Kunnskapssektorens tjenesteleverandør

4.3.1 Styringsmodellen for informasjonssikkerhet har gjort at den enkelte forskningsvirksomhet har fått tettere oppfølging

Gjennom **styringsmodellen** er HK-dir – Direktoratet for høyere utdanning og kompetanse gitt ansvaret for den løpende sektorstyringen av informasjonssikkerhet og personvern i til sammen 29 virksomheter direkte underlagt departementet. Kunnskapsdepartementet har fastsatt en overordnet *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*, som sammenfatter krav og føringer på området. HK-dir gjennomfører årlige kartleggingsmøter med virksomhetene hvor de tar utgangspunkt i krav og føringer i policyen, og leverer forslag til konkrete tilbakemeldinger som departementet kan bruke i sin oppfølging av virksomhetene.

HK-dir gir også konkrete anbefalinger til virksomhetene om det videre arbeidet med informasjonssikkerhet og personvern. En del av virksomhetene som er undersøkt, oppgir at de har hatt nytte av HK-dirs kartlegging, og at det har bidratt til å rette virksomhetenes oppmerksomhet mot informasjonssikkerhet og sette retning for arbeidet. Dette er særlig tilfellet for de minste virksomhetene.

Undersøkelsen viser at departementet har fulgt opp virksomhetene som er omfattet av styringsmodellen gjennom etats- og eierstyringen. Departementet har også brukt pedagogiske virkemidler overfor enkelte virksomheter i sektoren der styringsmulighetene er mer begrensede. De har gitt *anbefalinger* til private høyskoler som ikke er omfattet av styringsmodellen, gjennom tilskuddsbrev.

Etter Riksrevisjonens vurdering er det positivt at Kunnskapsdepartementet er tydelig om hvilke krav og føringer som gjelder for underliggende virksomheter, og følger opp dette gjennom styringsmodellen. Dette har bidratt til større oppmerksomhet om informasjonssikkerhetsarbeidet i virksomhetene som er omfattet av styringsmodellen. Samtidig har personvernforordningen blitt innført og trusselbildet skjerpet etter konkrete hendelser i sektoren. Det er også positivt at departementet bruker pedagogiske virkemidler overfor enkelte virksomheter i sektoren der departementet ikke har en direkte styringslinje.

Departementet har ikke uttrykt forventninger om hvordan universiteter og høyskoler skal følge opp informasjonssikkerheten i selskapene de eier. Departementet framholder at de på generelt grunnlag forventer at universiteter og høyskoler utøver sitt eierskap på en god måte og etterlever gjeldende lover og krav. Undersøkelsen viser at de tre største universitetene ikke har gitt føringer eller forventninger til informasjonssikkerheten gjennom eierdialogen til selskaper som driver med forskning eller teknologioverføring. Riksrevisjonen vil understreke at de samme forventningene til informasjonssikkerhet må legges til grunn, uavhengig av hvordan universitetene og høyskolene har valgt å organisere forskningsvirksomheten.

4.3.2 Kunnskapsdepartementet har i begrenset grad lyktes med å nå målet med informasjonssikkerhetssatsingen, og virkemidlene treffer i for liten grad virksomhetene som har størst behov for støtte

Som ledd i fireårssatsingen fikk Sikt (den gang Uninett) ansvar for å etablere et analysesenter og ta rollen som sektorvist responsmiljø for å forbedre sektorens evne til å håndtere trusler. Videre fikk de ansvaret for å få på plass rådgivningstjenester som skulle bistå sektoren i å implementere ledelsessystemer for informasjonssikkerhet på en helhetlig måte, og for å etablere et program for kompetanseheving innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte i sektoren. Leveransene fra Sikt ble samlet i et eget **Cybersikkerhetssenter for høyere utdanning og forskning, eduCSC.** Senteret tilbyr også tjenester til virksomheter i sektoren som ikke er underlagt Kunnskapsdepartementet.

For å dekke ulike behov i virksomhetene har eduCSC fra 2023 etablert ulike abonnementer, eller «pakker» av tjenester, som kunder av senteret kan velge blant. Enkelte tjenester leveres som tilleggstjenester. Både prismodell og tjenesteinnholdet er forankret i Digitaliseringsstyret, som er øverste nivå i universitets- og høyskolesektorens samstyringsmodell for digitalisering. Digitaliseringsstyret har bestemt at abonnementet «basispakken» skal være obligatorisk for alle høyskoler og universiteter. Det har foreløpig vært

utfordrende for eduCSC å få senteret finansiert via brukerbetaling. Sikt anslår at senteret vil gå cirka ti millioner kroner i underskudd det første året med ny prismodell.

Undersøkelsen viser at leveransen eduCSC har kommet lengst med, er rollen som sektorvist responsmiljø. På dette området har departementet sørget for et rammeverk for håndtering av IT-sikkerhetshendelser i sektoren.

Når det gjelder evnen til å oppdage dataangrep, vurderer Sikt at denne har vært uendret i perioden. Dette skyldes at felles infrastruktur og logganalyse som eduCSC har kjøpt inn som del av satsingen, ikke tas i bruk, og at overvåking av nettverk ved hjelp av sensorer er lagt til abonnementet «plusspakken», mens flertallet av virksomhetene har valgt «basispakken».

Leveransene fra eduCSC med dårligst måloppnåelse er tiltakene innenfor rådgivningstjenester og kompetanseheving. Rådgivningstjenester er blant senterets tilleggstjenester, og så langt har få virksomheter valgt å benytte seg av dette tilbudet. De mest konkrete leveransene innenfor kompetanseheving er

- de to forumene for informasjonssikkerhet, CISO-forum og IRT Community
- utarbeidelse av en veileder
- revisjoner av enkelte andre veiledere
- gjennomføring av enkelte webinarer

Både HK-dir og Sikt vurderer at omfanget av rådgivning og kompetanseheving som tilbys er mindre enn tiden før fireårssatsingen.

Samtidig viser undersøkelsen at mange virksomheter ikke klarer å gjennomføre anbefalte sikkerhetstiltak. Flere virksomheter har blant annet svak evne til å oppdage dataangrep. Departementets virkemiddelbruk ved opprettelse av eduCSC ser foreløpig ikke ut til å ha avhjulpet dette problemet.

Spesielt evnen til å oppdage dataangrep avhenger av sterkt spesialisert kompetanse. eduCSC overvåker i dag kommunikasjonen inn og ut av virksomhetene, men senteret overvåker ikke virksomhetenes egne nettverk og systemer.

Flere virksomheter sliter også med andre tekniske sikkerhetstiltak, som tilgangsstyring og intern sårbarhetsskanning. Det varierer mellom virksomhetene om de bygger intern kompetanse på dette, og noen virksomheter er avhengig av støtte for å gjennomføre sikkerhetstiltak. Innhentede data viser at mange virksomheter leier inn konsulenter til å sette opp systemer og lignende, også med tanke på sikkerhet

De fire største universitetene har gått sammen om et eget sikkerhetssamarbeid, BOTT Digital Sikkerhet, og ønsker at færrest mulig av tjenestene til eduCSC burde være obligatoriske. De fire har en del felles utfordringer, og etter Riksrevisjonens vurdering en del å lære av hverandre. At de fire største universitetene samarbeider, løser imidlertid ikke

problemene som sektoren som helhet har på informasjonssikkerhetsområdet.

Riksrevisjonen vurderer det som positivt at departementet har etablert et cybersikkerhetssenter med tjenester til hele sektoren, også til virksomheter i sektoren der departementet mangler direkte styringslinjer. Per dags dato greier imidlertid ikke eduCSC å treffe behovene til virksomhetene. Departementet har i stor grad overlatt vurderingene av hva eduCSC skal tilby til de underliggende virksomhetene, gjennom universitets- og høyskolesektorens samstyringsmodell for digitalisering. Etter Riksrevisjonens vurdering styres imidlertid senterets tjenestetilbud i dag i for stor grad av den enkelte virksomhets etterspørsel og betalingsvilje, og i for liten grad av behovene til sektoren som helhet.

Kunnskapsdepartementet har definert rollene til de sentrale aktørene i sektoren innenfor informasjonssikkerhetsområdet. Undersøkelsen viser imidlertid at det i praksis er uklarheter i forholdet mellom Kunnskapsdepartementet, HK-dir og Sikt når det gjelder styring og gjennomføring av informasjonssikkerhetstiltak i sektoren.

Departementet har videre gitt NOKUT ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren. Undersøkelsen viser at NOKUT verken gjennomfører eller har kapasitet til å gjennomføre dette. Det er heller ikke avklart hvordan slike kontroller skal gjennomføres.

Samlet sett vurderer vi derfor at organiseringen og virkemiddelbruken på området for sektoren som helhet er mindre ressurseffektiv og målrettet enn den kunne ha vært.

4.4 Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp

Departementet skal utarbeide og vedlikeholde systematiske risiko- og sårbarhetsanalyser, ta stilling til sikkerhetsnivået i egen sektor samt iverksette nødvendige kompenserende tiltak. Departementet skal også sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater. Hvor ofte og i hvilken utstrekning et område som informasjonssikkerhet bør evalueres, må bestemmes ut fra blant annet risiko og vesentlighet, samt kvaliteten på og omfanget av øvrig rapportering. Mer generelt har departementet overordnet ansvar for blant annet at virksomhetene bruker ressurser effektivt, og at det gjennomføres kontroll med virksomhetene.

Som del av styringsmodellen for informasjonssikkerhet har HK-dir fra og med 2019 levert årlige risiko- og tilstandsvurderinger til departementet. Gjennom disse mottar departementet informasjon om trusler og sårbarheter. Her sammenfatter HK-dir informasjon fra kartleggingene i virksomhetene, vurderer virksomhetenes modenhetsnivå innenfor informasjonssikkerhet og personvern og sannsynligheten for at virksomhetene etterlever kravene som

er formulert i *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*. HK-dir trekker også inn informasjon fra andre kilder, slik som statistikk om IT-sikkerhetshendelser i forskningsnettet fra sektorvist responsmiljø (eduCSC) og risiko- og trusselvurderinger fra nasjonale myndigheter. På bakgrunn av dette utarbeider HK-dir også årlige risikohåndteringsplaner på sektornivå med forslag til tiltak for å håndtere risikoen. Kunnskapsdepartementet tar stilling til og slutter seg til planene.

Men HK-dir baserer risiko- og tilstandsvurderinger på virksomhetenes egenrapportering og gjør ingen form for sikkerhetstesting eller kontroller av den faktiske sikkerhetstilstanden. Verken HK-dir eller andre gjennomfører tester for å kartlegge den faktiske statusen eller om tiltakene institusjonene oppgir, er implementert og fungerer i praksis. Informasjonen departementet mottar fra HK-dir, dreier seg i hovedsak om virksomhetenes arbeid med organisatoriske sikkerhetstiltak, men sier lite om virksomhetenes tekniske sikkerhetstiltak og om tiltakene har effekt. Funnene fra de tekniske testene og inntrengingstestene i denne undersøkelsen viser at det er svakheter i de tekniske sikkerhetstiltakene hos alle virksomhetene.

Flere av virksomhetene i undersøkelsen har kjøpt inntrengingstester fra private konsulentselskaper/revisjonsfirmaer, men departementet får ikke informasjon om resultatene fra disse testene. Det er også en mulighet at eduCSC gjennomfører for eksempel inntrengingstester, men dette har senteret ikke kapasitet til per i dag.

Som nevnt har departementet gitt NOKUT ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren, men NOKUT gjennomfører ikke noen slike kontroller per i dag. NOKUT har heller ikke et kompetansemiljø innenfor informasjonssikkerhetstesting.

Samtidig viser undersøkelsen at risikoreduserende tiltak på sektornivå som er identifisert, og som departementet er orientert om, ikke blir gjennomført. Dette gjelder tiltak som inntrengingstesting og revisjoner av den enkelte virksomhets arbeid med informasjonssikkerhet og personvern og med kompetanseheving overfor virksomhetene. Ansvaret for å følge opp flertallet av tiltakene er gitt til Sikt ved Cybersikkerhetssenter for forskning og utdanning (eduCSC). En del av tiltakene har ikke blitt gjennomført, og har heller ikke vært realistiske å gjennomføre, da de i praksis har forutsatt både at Sikt/eduCSC etablerer nye tjenester og at virksomhetene i sektoren betaler for gjennomføringen.

Som vist i kapittel 4.1.3 mangler virksomhetene oversikt over egne informasjonsverdier i forskning som ikke er personopplysninger. Departementet har igangsatt et kartleggingsarbeid med utgangspunkt i sikkerhetsloven for å få bedre oversikt over informasjonsverdier i sektoren det er særlig viktig å beskytte. Dette arbeidet er ikke ferdigstilt.

Riksrevisjonen vurderer det som positivt at Kunnskapsdepartementet har etablert en prosess for risikostyring av sektoren som gir informasjon om arbeidet med informasjonssikkerhet i virksomhetene som er omfattet av styringsmodellen. Samtidig mottar departementet lite systematisk informasjon om de tekniske sikkerhetstiltakene som er iverksatt ute i virksomhetene, og om virkningen av tekniske og organisatoriske

sikkerhetstiltak. Kunnskap om den faktiske sikkerhetstilstanden og verdiene i sektoren er viktig for at departementet skal kunne målrette krav og tiltak slik at sektoren er bedre i stand til å forbedre sikkerheten.

5 Anbefalinger

Riksrevisjonen anbefaler at Kunnskapsdepartementet

- avklarer samarbeidet mellom departementet, HK-dir og Sikt om informasjonssikkerhet, og avklarer hva NOKUTs rolle skal være.
- gjennomgår virkemiddelbruken og vurderer tiltak som i større grad treffer forskningsvirksomhetene som har størst behov for støtte.
- sikrer et godt informasjonsgrunnlag om sikkerhetstilstanden og verdiene i sektoren, og følger opp at risikoreduserende tiltak på sektornivå blir gjennomført.
- påser at forskningsvirksomhetene
    - sørger for at ledelsessystem for informasjonssikkerhet blir implementert fullt ut slik at styret og toppledelse har oversikt over sikkerhetstilstanden, kan sikre at besluttede tiltak gjennomføres og at tiltakene faktisk forbedrer sikkerheten slik som forutsatt.
    - sørger for bedre oversikt over forskningsdata som skal beskyttes
    - iverksetter tekniske og organisatoriske sikkerhetstiltak som de anser nødvendige, for å redusere risikoen for at dataangrep lykkes.

6 Statsrådens svar

Dokument 3:11 (2023−2024) *Informasjonssikkerhet i forskning innenfor kunnskapssektoren* ble oversendt statsråden i Kunnskapsdepartementet.

Svaret fra statsråden følger i sin helhet i vedlegg 2.

7 Riksrevisjonens uttalelse til statsrådens svar

Riksrevisjonen har ingen ytterligere merknader.

Saken sendes Stortinget.

Vedtatt i Riksrevisjonens møte 12. desember 2023

Karl Eirik Schjøtt-Pedersen Tom-Christer Nilsen

Helga Pedersen Anne Tingelstad Wøien Torstein Dahle

Jens A. Gunvaldsen

Vedlegg

Vedlegg 1:

Riksrevisjonens brev til statsråden i Kunnskapsdepartementet

Riksrevisjonen

Vår saksbehandler
Thomas Solberg 22241465
Vår dato 23.11.2023
Vår referanse 2022/00216-132
Deres dato
Deres referanse

Utsatt offentlighet jf. rrevl § 18 (2)

KUNNSKAPSDEPARTEMENTET
Postboks 8119 DEP
0032 OSLO

Riksrevisjonens undersøkelse av informasjonssikkerhet i forskning innenfor kunnskapssektoren

Vedlagt oversendes utkast til Dokument 3:X (2023–2024) *Riksrevisjonens undersøkelse av informasjonssikkerhet i forskning innenfor kunnskapssektoren*.

Dokumentet er basert på rapport oversendt Kunnskapsdepartementet 29. september 2023, og på departementets svar 27. oktober 2023.

Statsråden bes redegjøre for hvordan departementet vil følge opp Riksrevisjonens merknader og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen.

Statsrådens svar vil i sin helhet bli vedlagt dokumentet. Det bes om at svaret oversendes som pdf lagret fra Word, ikke skannet som bilde, slik at innholdet kan gjøres tilgjengelig for alle i samsvar med krav til universell utforming.

Svarfrist: 5. desember 2023.

For riksrevisorkollegiet

Karl Eirik Schjøtt-Pedersen
riksrevisor

Brevet er godkjent og ekspedert digitalt.

Vedlegg:

Utkast til Dokument 3:X (2023–2024) *Riksrevisjonens undersøkelse av informasjonssikkerhet i forskning innenfor kunnskapssektoren*

Vedlegg 2:

Statsrådens svar

DET KONGELIGE
KUNNSKAPSDEPARTEMENT

Forsknings- og høyere utdanningsministeren

Riksrevisjonen
Postboks 6835 St. Olavs plass
0130 OSLO

Utsatt offentlighet, jf Lov om Riksrevisjonen § 18, 2. ledd

Deres ref	Vår ref	Dato
2022/00216-132	23/891-	8. desember 2023

Riksrevisjonens undersøkelse av informasjonssikkerhet i forskning innenfor kunnskapssektoren – redegjørelse fra forsknings- og høyere utdanningsministeren

Jeg viser til Riksrevisjonens brev av 23. november 2023 med oversendelse av utkast til Dokument 3:X (2023-2024) *Riksrevisjonens undersøkelse av informasjonssikkerhet i forskning innenfor kunnskapssektoren.* Riksrevisjonen ber om en redegjørelse for hvordan departementet vil følge opp Riksrevisjonens merknader og anbefalinger, og eventuelt om departementet er uenig med Riksrevisjonen.

Målet med Riksrevisjonens undersøkelse har vært å vurdere hvordan forskningsinstitusjoner under Kunnskapsdepartementet sikrer forskningsdata mot dataangrep, og hvordan departementet ivaretar sitt overordnede ansvar for informasjonssikkerhet i høyere utdanning og forskning. Undersøkelsen omfatter i hovedsak perioden 2019-2022.

Riksrevisjonen vurderer at arbeidet med informasjonssikkerhet har fått mer oppmerksomhet i sektoren de siste årene, og at innføringen av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning har bidratt til dette. Etter Riksrevisjonens vurdering gjenstår det imidlertid noen utfordringer som må tas tak i for at den enkelte virksomhet og sektoren som helhet kan oppnå ønsket sikkerhetsnivå.

Jeg vil takke Riksrevisjonen for en rapport som bygger på et stort datamateriale og grundige analyser, og som vil være nyttig for departementets og sektorens videre arbeid på dette feltet. I det følgende redegjør jeg for hvordan departementet vil følge opp Riksrevisjonens merknader og anbefalinger. Riksrevisjonens anbefalinger er inndelt i fire hovedpunkter. Den følgende teksten er strukturert slik at hver underoverskrift tar for seg ett av de fire anbefalingspunktene i rekkefølgen de er presentert i fra Riksrevisjonen.

Postadresse
Postboks 8119 Dep
0032 Oslo
postmottak@kd.dep.no

Kontoradresse
Kirkeg. 18

www.kd.dep.no

Telefon*
22 24 90 90
Org.nr.
872 417 842

For ordens skyld gjør jeg oppmerksom på at Riksrevisjonen ikke hadde avklart spørsmålet knyttet til behov for skjerming av opplysninger i forvaltningsrevisjonsrapporten, som Dokument 3:X (2023-2024) bygger på, da jeg ble bedt om å gi min uttalelse til Dokument 3. Jeg er derfor ikke kjent med eventuelle opplysninger som avviker fra det utkastet til forvaltningsrevisjonsrapport som ble forelagt departementet i september 2023.

Avklaring av roller

Riksrevisjonen anbefaler at Kunnskapsdepartementet avklarer samarbeidet om informasjonssikkerhet mellom departementet, Direktoratet for høyere utdanning og kompetanse (HK-dir) og Sikt – Kunnskapssektorens tjenesteleverandør, og avklarer hva Nasjonalt organ for kvalitet i utdanningen (NOKUT) sin rolle skal være. Riksrevisjonen skriver at selv om Kunnskapsdepartementet har definert rollene til de sentrale aktørene i sektoren innen informasjonssikkerhet, viser undersøkelsen at det i praksis er uklarheter i forholdet mellom departementet, HK-dir og Sikt når det gjelder styring og gjennomføring av informasjonssikkerhetstiltak i sektoren.

Jeg ønsker å gjøre oppmerksom på at samarbeidet mellom Kunnskapsdepartementet og HK-dir om informasjonssikkerhet og personvern er klart definert i beskrivelsen av styringsmodellen for informasjonssikkerhet og personvern i høyere utdanning og forskning. Dette samarbeidet fungerer i praksis slik det er beskrevet i styringsmodellen, og det er min oppfatning at verken departementet eller HK-dir opplever usikkerheter knyttet til egen rolle og ansvar i henhold til beskrivelsen i styringsmodellen.

Derimot er det behov for å tydeliggjøre rollen til Sikt i styringsmodellen. I den gjeldende versjonen av beskrivelsen av styringsmodellen er Sikt tildelt en rolle i å levere tjenester innen informasjonssikkerhet og personvern til sektoren og ha ansvaret for sektorvist responsmiljø (SRM), men det er som Riksrevisjonen påpeker noe uklarhet rundt hva denne rollen innebærer i praksis. Kunnskapsdepartementet har på denne bakgrunn allerede startet et arbeid for å involvere Sikt tettere i arbeidet innenfor styringsmodellen, enn det som tidligere har vært tilfelle. Departementet har blant annet bedt HK-dir og Sikt vurdere hvordan det kan være hensiktsmessig å utvikle samarbeidet på informasjonssikkerhetsområdet, og vil følge opp innspillene fra de to virksomhetene fremover. Som et ledd i vurderingen av hvordan Sikts rolle kan formaliseres i styringsmodellen, ble Sikt for første gang invitert til å delta som observatør med talerett på møtet *ledelsens gjennomgang* av styringsmodellen for informasjonssikkerhet og personvern i september 2023. Møtene avholdes halvårlig mellom Kunnskapsdepartementet og HK-dir for å sikre felles situasjonsforståelse, og diskutere status for området og mulige forbedringstiltak. Departementet vil fremover invitere Sikt fast inn i disse møtene for å sikre mest mulig lik situasjonsforståelse hos ledelsen i alle de sentrale aktørene i styringsmodellen.

Riksrevisjonen anbefaler også at Kunnskapsdepartementet avklarer NOKUTs rolle. NOKUT er i styringsmodellen tildelt ansvar for å føre selvstendig kontroll med informasjonssikkerhet og personvern hos virksomhetene i sektoren, men har av kapasitets- og ressurshensyn ikke

utført denne oppgaven. Jeg deler Riksrevisjonens vurdering av at det er behov for å avklare dette spørsmålet, og Kunnskapsdepartementet vil utrede nærmere om NOKUT skal fortsette å ha denne rollen eller ikke.

Bedre og mer treffsikker virkemiddelbruk

Riksrevisjonen anbefaler at Kunnskapsdepartementet gjennomgår virkemiddelbruken og vurderer tiltak som i større grad treffer de virksomhetene som har størst behov for støtte. I en så variert sektor som høyere utdannings- og forskningssektoren er, vil det være vanskelig å treffe alle behov like godt. Som Riksrevisjonen påpeker, er det store forskjeller mellom hvor mye kapasitet og kompetanse virksomhetene i sektoren har på informasjonssikkerhet. Det er også store forskjeller i organisasjonenes størrelse og kompleksitet. Dette påvirker hvordan virksomhetene jobber med informasjonssikkerhet, og hvilke behov de har for støtte i dette arbeidet.

HK-dir leverer årlig et forslag til Kunnskapsdepartementet om en risikohåndteringsplan med tiltak på sektornivået, som skal redusere risiko for informasjonssikkerhetshendelser og styrke etterlevelse av krav til informasjonssikkerhet og personvern i sektoren. Sikt – i hovedsak produktområdene Cybersikkerhetssenteret (eduCSC) og personverntjenester – har en viktig rolle i å levere de fleste sektortiltakene HK-dir foreslår. Som Riksrevisjonen påpeker har ikke Sikt prioritert kapasitet til å gjennomføre tiltakene i tråd med risikohåndteringsplanen. For å sikre at det i fremtidige forslag til risikohåndteringsplaner blir bedre samsvar mellom de tiltakene HK-dir foreslår og Sikts ressurser, har Kunnskapsdepartementet startet en dialog med HK-dir og Sikt om et tettere samarbeid mellom de to i utarbeidelsen av risikohåndteringsplanen. Departementet vil følge opp at det i fremtidige risikohåndteringsplaner legges vekt på forventede effekter av tiltakene på risiko og etterlevelse på sektornivået, og at forslagene må baseres på en nytte-kostnadsvurdering, slik at ressursene brukes på en mest mulig effektiv måte og kommer hele sektoren til gode, i tråd med Riksrevisjonens anbefaling.

HK-dir og Sikt har gitt Kunnskapsdepartementet tilbakemelding om at de ønsker å videreutvikle det eksisterende samarbeidet de har på informasjonssikkerhetsområdet. De har etablert faste tertialvise kontaktmøter mellom HK-dirs fagmiljø for informasjonssikkerhet og personvern og Cybersikkerhetssenteret (eduCSC) i Sikt, i tillegg til den løpende uformelle dialogen som allerede eksisterer mellom de to virksomhetene på dette fagområdet. HK-dir vil fremover involvere Sikt tidligere i prosessen med å lage forslag til risikohåndteringsplan. Tettere og tidligere involvering av Cybersikkerhetssenteret i prosessen vil gi bedre situasjonsforståelse i utarbeidelsen av forslag til tiltak, ettersom Cybersikkerhetssenteret har bedre innsikt i den tekniske og operative siden av informasjonssikkerheten i sektoren enn HK-dir. Det vil også sikre at tiltakene er mer i tråd med Sikt sine ressurser, og hva virksomhetene i kunnskapssektoren etterspør av støtte, slik Riksrevisjonen anbefaler.

Bedre informasjonsgrunnlag

Riksrevisjonen anbefaler at Kunnskapsdepartementet sikrer et godt informasjonsgrunnlag om sikkerhetstilstanden og verdiene i sektoren, og følger opp at risikoreduserende tiltak på sektornivå blir gjennomført. Riksrevisjonen påpeker at departementet ikke har tilstrekkelig informasjon om det tekniske sikkerhetsnivået hos virksomhetene i sektoren, ettersom HK-dirs kartlegging er basert på virksomhetenes egenrapportering og i hovedsak dreier seg om organisatoriske sikkerhetstiltak.

Som nevnt ovenfor vil departementet utrede om NOKUT skal fortsette å ha en kontrollerende rolle i styringsmodellen. Det er i den forbindelse naturlig å også utrede hvilken type kontroller det vil være hensiktsmessig å utføre på informasjonssikkerhetsområdet og hvordan slike kontroller eventuelt best kan gjennomføres, og av hvem. En mulighet, som Riksrevisjonen også nevner, er at Cybersikkerhetssenteret i Sikt får i oppdrag å gjennomføre tekniske sikkerhetstester, som kan bidra til å avdekke mangler og sårbarheter hos virksomhetene i sektoren, og gjøre det mulig for Kunnskapsdepartementet å ha oversikt over sikkerhetstilstanden, og om sektortiltak har blitt gjennomført og hatt ønsket effekt. Tekniske tester alene gir imidlertid ikke nødvendigvis tilstrekkelig informasjon om hvilke verdier sektoren forvalter som må beskyttes, eller hvorvidt de organisatoriske sikkerhetstiltakene er tilfredsstillende og gir ønsket effekt. Før Sikt eller en annen leverandør eventuelt kan bli tildelt en slik oppgave, må det derfor utredes nærmere hva både hva slags tester som kan være relevante og som vil gi departementet det nødvendige informasjonsgrunnlaget, og hvilke kostnader det er forbundet med.

Styring av Kunnskapsdepartementets underliggende virksomheter

Riksrevisjonen anbefaler til slutt at Kunnskapsdepartementet påser at virksomhetene sørger for at ledelsessystem for informasjonssikkerhet blir implementert fullt ut, sørger for bedre oversikt over forskningsdata som skal beskyttes, og iverksetter tekniske og organisatoriske sikkerhetstiltak for å redusere risikoen for at dataangrep lykkes.

Jeg mener dette er viktige tiltak for å bedre informasjonssikkerheten, noe som illustreres av at de er nedfelt i krav til virksomhetene gjennom Rundskriv F-04-20 *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning,* henholdsvis i policyens punkt 1-4. Kunnskapsdepartementet har siden 2020 stilt krav til virksomhetene i de årlige tildelingsbrevene og i forbindelse med etatsstyringsmøtene om at implementering av krav i policyen skal prioriteres. Som Riksrevisjonen også påpeker, har virksomhetene jobbet mye med å forbedre etterlevelsen av policyen siden den ble fastsatt i 2020, og mange virksomheter har kommet et godt stykke på vei, noe både HK-dirs årlige kartlegginger og Riksrevisjonens undersøkelse viser. Det gjenstår allikevel en del arbeid før samtlige virksomheter oppfyller kravene i policyen. Derfor er dette et fagområde departementet vil fortsette å rette oppmerksomhet mot og følge opp i etatsstyringen, i samarbeid med HK-dir og Sikt og virksomhetene i sektoren.

Kunnskapsdepartementet har satt i gang flere initiativer som skal støtte virksomhetene i sektoren i deres arbeid med å kartlegge hvilke verdier som trenger beskyttelse. Det er krevende både på overordnet nivå og for den enkelte virksomhet å få oversikt over alle verdier i kunnskapssektoren, og identifisere hvilke verdier som har behov for særskilte sikringstiltak. Derfor leder Kunnskapsdepartementet en interdepartemental arbeidsgruppe bestående av seks departementer, i tillegg til Kunnskapsdepartementet, som blant annet skal kartlegge såkalte sensitive fagområder innen forskning og høyere utdanning som kan være forbundet med risiko for skade mot nasjonal sikkerhet. En egen arbeidsgruppe bestående av representanter fra sektoren og ledet av Universitets- og høyskolerådet (UHR) bidrar også i dette arbeidet. Dette fordi det er sektoren selv som sitter med mest detaljert kunnskap om hvilke fagområder som kan være forbundet med risiko for skade mot nasjonal sikkerhet og dermed kan være sensitive fagområder. Hensikten er å få bedre oversikt over hvilke verdier som finnes i sektoren og identifisere relevante sikringstiltak ved behov. Utredningen vil se hen til og koordineres med relevante pågående prosesser, blant annet nasjonal verdikartlegging og vurderinger knyttet til eventuell utpeking av grunnleggende nasjonale funksjoner etter sikkerhetsloven i Kunnskapsdepartementets sektor.

Et annet eksempel på tiltak som er utviklet for å bistå virksomhetene i sektoren i deres arbeid med forebyggende sikkerhet og verdikartlegging, er de nasjonale retningslinjene for ansvarlig internasjonalt samarbeid, utviklet av HK-dir og Norges forskningsråd, på oppdrag fra Kunnskapsdepartementet. Retningslinjene ble lansert 14. august 2023 og er tilgjengeliggjort som en rapport og en nettressurs på både norsk og engelsk som vil oppdateres jevnlig. Retningslinjene er primært utarbeidet for å støtte institusjonene i å håndtere risikoer og styrke sikkerheten ved internasjonalt samarbeid, men kan også benyttes som et verktøy i arbeidet med å kartlegge verdier ved institusjonen.

Kunnskapsdepartementets styring av høyere utdannings- og forskningssektoren er i hovedsak overordnet og strategisk, og innrettet etter risiko og vesentlighet. I henhold til Meld. St. 19 (2020-2021) *Styring av statlige universiteter og høyskoler* skal Kunnskapsdepartementet «styre i det store og ikke i det små». I utgangspunktet har ledelsen i den enkelte virksomhet ansvar for hvordan den styrer og drifter virksomheten, mens departementet styrer gjennom å formulere mer overordnede mål, krav og føringer. Riksrevisjonen bemerker at departementet ikke har uttrykt forventninger om hvordan universiteter og høyskoler skal følge opp informasjonssikkerhet i selskapene de eier. Departementet styrer ikke gjennom å uttrykke særskilte forventninger til de underliggende virksomhetene om hvordan de skal følge opp interne forhold i selskaper de har eierskap i, utover at departementet forventer at gjeldende lover og regler følges i disse selskapene, som de også skal i egen virksomhet. Dette er i tråd med *Reglement for økonomistyring i staten* § 10 «Oppfølging av statens eierinteresser m.m.», der det fremgår at utøvelsen av eierskapet skal understøtte en klar fordeling av myndighet og ansvar mellom eier og styret. Det er det øverste styrende organet i en virksomhet som har ansvaret for at informasjonssikkerheten er tilstrekkelig ivaretatt. Det er viktig at Kunnskapsdepartementet balanserer sitt overordnede ansvar for informasjonssikkerheten i sektoren opp mot virksomhetenes eget ansvar. Kunnskapsdepartementet vil følge opp Riksrevisjonens anbefalinger og sørge for at

departementet har god oversikt over status og risiko i sektoren på informasjonssikkerhetsområdet, og vurdere og iverksette relevante og hensiktsmessige sektortiltak for å redusere risikoen.

Med hilsen

Sandra Borch

Dokumentet er godkjent elektronisk og påført statsrådens signatur

Vedlegg 3:

Forvaltningsrevisjonsrapport med vurderinger – offentlig versjon

Dette er en offentlig versjon av forvaltningsrevisjonsrapporten. Den opprinnelige rapporten inneholder informasjon som er unntatt offentlighet jf. offentleglova § 24 tredje ledd, og noe informasjon som er gradert BEGRENSET jf. sikkerhetsloven § 5-3 første ledd bokstav d. I denne versjonen er slik informasjon skjermet ved bruk av «sladding».

Revisjonen er gjennomført som en forvaltningsrevisjon i henhold til

- **lov om Riksrevisjonen § 9 tredje ledd**
- **instruks om Riksrevisjonens virksomhet § 9**
- **INTOSAIs standard for forvaltningsrevisjon (ISSAI 3000)**
- **Riksrevisjonens faglige retningslinjer for forvaltningsrevisjon**

Innhold

Tabelloversikt

Figuroversikt

Faktaboksoversikt

1 Innledning

1.1 Bakgrunn

Sikkerhetssituasjonen innenfor høyere utdannings- og forskningssektoren har blitt mer utfordrende de siste årene. Antallet registrerte dataangrep mot sektoren økte kraftig på verdensbasis både i 2020 og 2021.[1] Sikkerhetssituasjonen ble ytterligere skjerpet da Russland invaderte Ukraina i 2022.[2] I sine risikovurderinger for 2020, 2021, 2022 og 2023 har PST[3], Etterretningstjenesten[4] og NSM[5] pekt på at norske forskningsmiljøer er utsatte etterretningsmål. Direktoratet for høyere utdanning og kompetanse (HK-dir) rapporterer også om en sikkerhetssituasjon preget av større trusler og flere hendelser i Norge.[6]

I tillegg til trusselen fra utenlandsk etterretning vil også kriminelle aktører ha interesse for forskningsdata og -systemer. Politiets trusselvurdering 2023 anser løsepengevirus[7] rettet mot bedrifter og virksomheter som den største kriminalitetstrusselen mot IT-sikkerhet og digital infrastruktur.[8] I sin risiko- og tilstandsvurdering for 2023 vurderer HK-dir at risikoen for løsepengevirus, som fører til brudd på informasjons- og personopplysningssikkerheten, er høy innenfor forsknings- og utdanningssektoren.

En sentral årsak til at sektoren er interessant for angripere er at det finnes store informasjonsverdier her i form av forskningsdata. Svak sikring av forskningsdata kan potensielt få store økonomiske konsekvenser, føre til spredning av sensitive opplysninger som personopplysninger og forretningshemmeligheter og gjøre at virksomhetene taper omdømme. Noen universiteter og høyskoler forsker på områder som er viktige for å sikre nasjonale interesser, for eksempel forskning på olje og energi, elektronisk kommunikasjon (ekom), forsvarsmateriell og annen flerbruksteknologi.[9]

Det er et viktig prinsipp for offentlig finansierte forskningsdata at disse skal være «så åpne som mulig, så lukkede som nødvendig».[10] Prinsippet innebærer en forventning om at forskningsdata skal tilrettelegges for åpen tilgang så framt ikke hensynet til sikkerhet, personvern, immaterielle rettigheter, forretningshemmeligheter og lignende tilsier at dataene må skjermes. Virksomhetene må finne en balanse mellom disse hensynene. Samtidig begrenser ikke trusselen mot forskning seg kun til sensitive kunnskapsområder. En angriper kan også gjøre utilgjengelig eller slette andre viktige forskningsdata eller manipulere dataene. Mer generelt vil tilliten til forskning svekkes hvis det mistenkes at eksterne aktører har hatt tilgang til forskningen og resultatene av den.

Kunnskapsdepartementet igangsatte i 2019 et fireårig informasjonssikkerhetsprogram for høyere utdanning og forskning (2019–2022). Programmet hadde til formål å styrke informasjonssikkerheten i sektoren og forbedre evnen til å forebygge og håndtere trusler mot Forskningsnettet, den nasjonale nettinfrastrukturen for forskning og utdanning. Departementet bevilget 17,5 millioner kroner årlig til dette, totalt 70 millioner kroner. Det er ikke gjennomført noen evaluering av denne satsingen.

[1] Hystad, J. (2020, 26. september). Kraftig økning i dataangrep mot utdanningssektoren. *Khrono*. https://khrono.no/kraftig-okning-i-dataangrep-mot-utdanningssektoren/517861; Strand, H. K. og Hystad, J. (2022, 7. februar). Opplever 1600 dataangrep i veka: — Ein indikator på stor verdi. *Khrono*. https://khrono.no/opplever-1600-dataangrep-i-veka-ein-indikator-pa-stor-verdi/657438
[2] NSM Risiko (2023).
[3] Nasjonal trusselvurdering (2020), Nasjonal trusselvurdering (2021), Nasjonal trusselvurdering (2022), Nasjonal trusselvurdering (2023).
[4] Fokus (2020), Fokus (2021), Fokus (2022), Fokus (2023).
[5] NSM Risiko (2020), NSM Risiko (2021), NSM Risiko (2022), NSM Risiko (2023).
[6] Unit. (2021). *Risiko- og tilstandsvurdering 2021: Informasjonssikkerhet og personvern i høyere utdanning og forskning*; HK-dir. (2022). *Risiko- og tilstandsvurdering 2022: Informasjonssikkerhet og personvern i høyere utdanning og forskning*; HK-dir. (2023). *Risiko- og tilstandsvurdering 2023: Informasjonssikkerhet og personvern i høyere utdanning og forskning*.
[7] I denne typen angrep brukes skadevare til å kryptere data i offerets datasystem, før aktøren krever løsepenger mot å heve kryptering.
[8] Politiets sikkerhetsvurdering 2023, side 16.
[9] Flerbruksteknologi omfatter teknologier og produkter som kan anvendes både til sivile og militære formål. Kilde: NSM Risiko (2023), side 36-37.
[10] Nasjonal strategi for tilgjengeliggjøring og deling av forskningsdata, side 3.

Virksomhetene innenfor høyere utdanning og forskning har selv ansvaret for informasjonssikkerhet og personvern i egen forskning. Forskningsvirksomheter *under Kunnskapsdepartementet* inkluderer både universiteter og høyskoler,[11] ett forskningsinstitutt[12] og to heleide selskaper som er direkte eid av departementet.[13] Videre eier flere av universitetene og høyskolene helt eller delvis forskningsselskaper[14] eller selskaper for teknologioverføring (TTO-er)[15] som blant annet har som formål å kommersialisere forskning ved institusjonene. Kunnskapsdepartementet tildeler også midler til forskningsinstitutter og til private høyskoler som driver med forskning.

Kunnskapsdepartementet har det overordnede ansvaret for informasjonssikkerheten i høyere utdanning og forskning. Departementets viktigste virkemidler på området er HK-dir og Sikt – Kunnskapssektorens tjenesteleverandør, som har ansvar for leveranser knyttet til IT og forskningsdata.[16] De legger til rette for lagring og deling av forskning gjennom teknisk infrastruktur,[17] og tilbyr sikkerhetstjenester til sektoren. I tillegg skal Nasjonalt organ for kvalitet i utdanningen (NOKUT) føre uavhengig kontroll med at kravene til informasjonssikkerhet og personvern etterleves. Departementet har også oppnevnt et råd for samfunnssikkerhet og beredskap i kunnskapssektoren (Beredskapsrådet).

Faktaboks 1 Begrepsavklaring

Informasjonssikkerhet handler om å sikre informasjonsbehandlingen ved å sikre at informasjon ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet), og er tilgjengelig ved behov (tilgjengelighet).[18] I denne undersøkelsen er vi opptatt av informasjon som behandles digitalt.

For virksomhetene er det viktig å identifisere hvilke **informasjonsverdier** som skal beskyttes, samt hvilke **trusler** de utsettes for, og hvordan verdiene er **sårbare** for disse truslene. Informasjonsverdi er et samlebegrep som rommer både informasjon og «støtteverdier» i form av IT-systemer, tjenestene som leveres av systemene, datautstyr, nettverk og så videre.[19] Med informasjonsverdier i forskning menes både forskningsdata og slike støtteverdier.

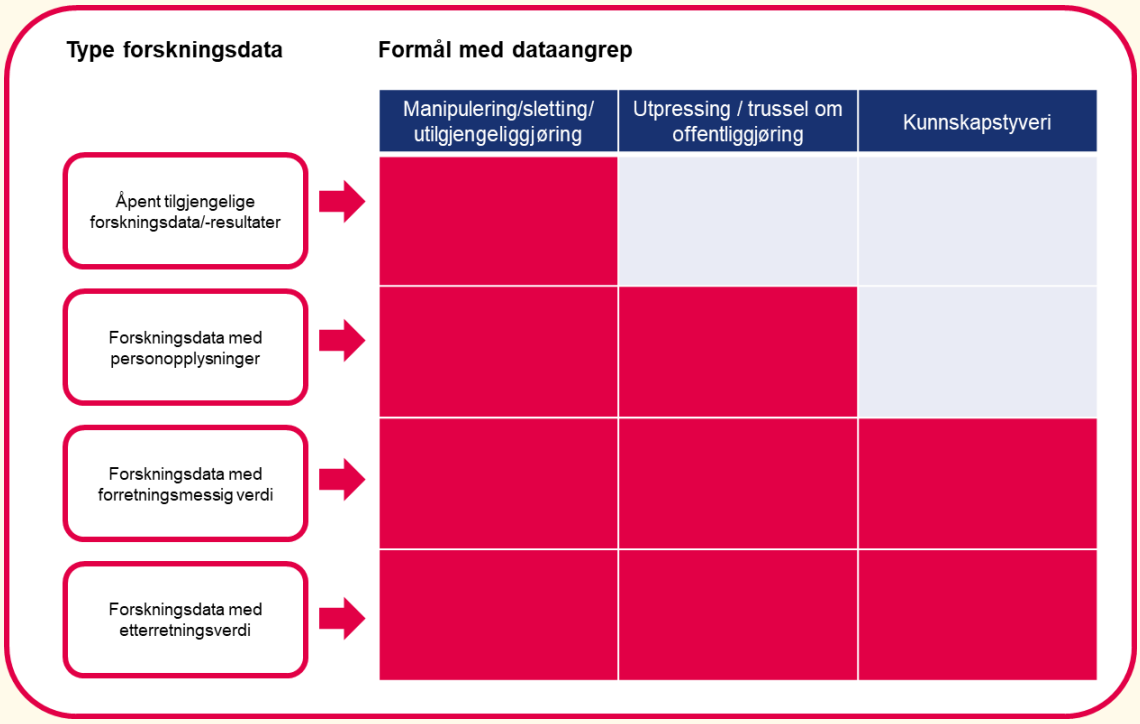
Sikkerhetsbrudd kan være utilsiktede, altså forårsaket av menneskelige feil/uhell, eller tilsiktede. Med **dataangrep** menes handlinger *som er ment* å skade eller påvirke et IT-system. Angrep kan gjennomføres på en rekke måter, og angrepsformene er i stadig utvikling.[20]

Med **høyere utdannings- og forskningssektoren** menes både områder som kan styres direkte av Kunnskapsdepartementet, og områder hvor styringsmulighetene er mer begrensede. Sistnevnte omfatter forskningsselskaper og teknologioverføringsselskaper eid av universiteter og høyskoler, samt forskningsinstitutter og private høyskoler som mottar tilskudd fra Kunnskapsdepartementet.

[11] Det er i dag ti universiteter, fem høyskoler og seks vitenskapelige høyskoler som er underlagt Kunnskapsdepartementet.
[12] Norsk utenrikspolitisk institutt (NUPI).
[13] De heleide selskapene som er direkte eid av Kunnskapsdepartementet, er Simula Research Laboratory AS og Universitetssenteret på Svalbard AS.
[14] Forskningsselskaper der staten eier mer enn 50 prosent: NTNU Samfunnsforskning AS (heleid), NORCE Norwegian Research Centre (deleid), Nordlandsforskning AS (deleid), Samfunns- og næringslivsforskning AS (deleid).
[15] TTO-er der staten eier mer enn 50 prosent: ARD Innovation AS (heleid), Inven2 AS (heleid), Nord Innovasjon AS (heleid), NTNU Technology Transfer AS (heleid), Vestlandets innovasjonsselskap AS (heleid).
[16] https://www.unit.no/en/node/3118
[17] Sikt har blant annet ansvar for å utvikle og drifte Forskningsnettet. De drifter også mange lokale nettverk, den nasjonale innloggings- og datadelingsløsningen Feide, videotjenesten Zoom, trådløs nettilgang via Eduroam m.m. Videre har de ansvar for et av verdens største arkiv for forskningsdata, som formidles til forskere og studenter i Norge og utlandet (tidligere NSD). Datterselskapet Uninett Sigma2 har ansvaret for å anskaffe, drifte og videreutvikle den generiske nasjonale e-infrastrukturen for tungregning og datalagring i Norge (NIRD).
[18] Begrepsliste: Informasjonssikkerhet | Digitaliseringsdirektoratet - Difi
[19] https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonsverdi
[20] https://www.netsecurity.no/fagblogg/hvilke-typer-dataangrep-finnes-det

Med **forskningsvirksomheter under departementet** menes virksomheter under Kunnskapsdepartementets som utfører forskning, det vil si alle universiteter og høyskoler, forskningsinstituttet Norsk utenrikspolitisk institutt (NUPI) og to heleide selskaper – Simula Research Laboratory AS og Universitetssenteret på Svalbard AS, som er direkte eid av Kunnskapsdepartementet.

Med **forskningsdata** menes alle data som er samlet inn eller frambrakt til bruk for eller som et resultat av forskning, og data som utgjør grunnlaget for publikasjoner, uavhengig av hvilken kilde dataene kommer fra.[21] I denne undersøkelsen gjør vi et grovt skille mellom fire kategorier forskningsdata. Figuren nedenfor viser disse, samt hva som kan være formålet med et dataangrep mot verdier i hver av kategoriene:



Kilde: Riksrevisjonens klassifisering i denne undersøkelsen

Den første kategorien omfatter forskningsdata/-resultater som er ment å være åpent tilgjengelige. Selv om disse dataene ikke er **sensitive**, kan de være **beskyttelsesverdige** for eksempel fordi kostnaden ved å gjenskaffe dem er svært høy dersom de går tapt eller blir ødelagt. De tre neste kategoriene omfatter forskningsdata som av ulike grunner er sensitive:

- forskningsdata med sensitive personopplysninger
- forskningsdata som har forretningsmessig verdi, for eksempel som følger av potensial for kommersialisering eller patentering, samt samarbeid med eller oppdrag fra industrien
- forskningsdata som av ulike grunner kan være av interesse for fremmede staters etterretning, som for eksempel forskning på olje og energi, elektronisk kommunikasjon (ekom), forsvarsmateriell og annen flerbruksteknologi, og enkelte data innenfor fagområder som berører norsk utenriks og sikkerhetspolitikk og nordområdene

I tillegg til dataene, kan utstyr og systemer som brukes i forskningen også være sensitive, for eksempel med tanke på ulovlig kunnskapsoverføring. De kan også ha en høy økonomisk verdi.

Med **tekniske sikkerhetstiltak** menes sikkerhetsmekanismer som er bygget inn eller definert i programvare eller maskiner, for eksempel tilgangskontroller, kontroll med kommunikasjon i nettverk (brannmurer og annet) og overvåkningssystemer.

Med **organisatoriske sikkerhetstiltak** menes for eksempel retningslinjer, prosedyrer og rutiner som er etablert på operativt nivå for å sikre forskningsdata, samt opplæring, kompetanseheving og annen støtte som gis for å sørge for at rutinene følges.

1.2 Mål og problemstillinger

Målet med undersøkelsen er å vurdere hvordan forskningsvirksomheter under Kunnskapsdepartementet sikrer forskningsdata mot dataangrep, og hvordan departementet ivaretar sitt overordnede ansvar for informasjonssikkerhet i høyere utdanning og forskning.

Målet belyses gjennom følgende problemstillinger:

1. Har virksomhetene sørget for at beskyttelsesverdige forskningsdata er tilstrekkelig sikret mot dataangrep?
    - 1.1. *Vil en angriper kunne stjele, manipulere eller slette forskningsdata med høy informasjonsverdi fra virksomhetene ved hjelp av offentlig kjente metoder og standardverktøy?*
    - 1.2. *Er de tekniske sikkerhetstiltakene som er etablert for å forebygge og avdekke slike angrepsforsøk i tråd med anbefalinger i anerkjente standarder?*
    - 1.3. *Er de organisatoriske sikkerhetstiltakene som er etablert for å sikre slike forskningsdata i tråd med anbefalinger i anerkjente standarder?*
2. Har styret og ledelsen i virksomhetene sørget for at informasjonssikkerhetsarbeidet skjer på en systematisk måte?
    - 2.1. *Har styret og ledelsen lagt grunnlaget for god informasjonssikkerhet ved å vedta mål og strategi for informasjonssikkerhetsarbeidet, og tildelt og kommunisert roller og ansvar for arbeidet?*
    - 2.2. *Er det utarbeidet et dokumentert ledelsessystem for informasjonssikkerhet i tråd med anbefalinger i anerkjente standarder?*
    - 2.3. *Er det etablert prosesser for risikovurdering som identifiserer informasjonssikkerhetsrisikoer og håndterer disse ved å fastsette mål og planer for risikoreduserende tiltak?*
    - 2.4. *Er det etablert prosesser for å evaluere informasjonssikkerheten, og følger styret og ledelsen opp at den kontinuerlig forbedres?*
3. Har Kunnskapsdepartementet i tilstrekkelig grad fulgt opp at arbeidet med informasjonssikkerhet i forskningsvirksomhetene under departementet er tilfredsstillende, og ivaretatt det overordnede ansvaret departementet har for informasjonssikkerheten i sektoren?
    - 3.1. *I hvilken grad har departementet fulgt opp området gjennom styringen av forskningsvirksomhetene?*

[21] Jf. definisjon i Kunnskapsdepartementet. (2017). *Nasjonal strategi for tilgjengeliggjøring og deling av forskningsdata*.

3.2. *I hvilken grad har departementets øvrige virkemiddelbruk understøttet arbeidet med informasjonssikkerhet innenfor sektoren?*

3.3. *I hvilken grad har departementet arbeidet systematisk og risikobasert med informasjonssikkerhet i sektoren?*

2 Metodisk tilnærming og gjennomføring

Problemstilling 1 og 2 omfatter alle forskningsvirksomheter som inngår i Kunnskapsdepartementets styringsmodell.[22] Problemstilling 3 omfatter også Kunnskapsdepartementet og virkemidlene til departementet, som Sikt, HK-dir og NOKUT. I tillegg ser vi på hvordan Kunnskapsdepartementet ivaretar ansvaret innen forvaltningsområdet informasjonssikkerhet for forskningsvirksomheter under departementet og for sektoren i sin helhet.

Undersøkelsesperioden er fra og med 2019, da departementet initierte den fireårige satsingen på informasjonssikkerhet. I problemstilling 1 er vi imidlertid først og fremst ute etter å få et bilde av sikkerhetssituasjonen på undersøkelsestidspunktet (2022/2023).

2.1 Metodisk tilnærming til problemstilling 1 og 2

For å belyse problemstilling 1 og 2 har vi gjennomført **undersøkelser ved til sammen ti forskningsvirksomheter** – åtte universiteter og høyskoler, ett selskap og ett forskningsinstitutt:

- Nord universitet
- Norges idrettshøgskole (NIH)
- Norges teknisk-naturvitenskapelige universitet (NTNU)
- Norsk utenrikspolitisk institutt (NUPI)
- Universitetet i Bergen (UiB)
- Universitetet i Oslo (UiO)
- Universitetet i Stavanger (UiS)
- Universitetet i Sørøst-Norge (USN)
- Universitetet i Tromsø – Norges arktiske universitet (UiT)
- Universitetssenteret på Svalbard AS (UNIS)

Vi har undersøkt de samme områdene for alle de ti virksomhetene, men har gått mer i dybden og innhentet mer data ved tre av dem. Problemstilling 1.1 har vi belyst ved å gjennomføre inntrengingstester ved disse tre.

Et sentralt metodisk grep i undersøkelsen er å sammenligne det vi har funnet i disse ti virksomhetene med **god praksis**, som framgår av anerkjente standarder for informasjonssikkerhet:

- Ved undersøkelser av sikkerhetstiltak (problemstilling 1) har vi valgt ut noen tekniske og organisatoriske tiltak som anbefales i faglige standarder, og som vi anser som sentrale for å beskytte forskningsdata og IT-systemer som lagrer eller understøtter lagring/deling av dataene. Vi har undersøkt i hvilken grad virksomhetene har implementert disse tiltakene.
- Ved undersøkelser av systematikken i virksomhetenes informasjonssikkerhetsarbeid (problemstilling 2) har vi tatt utgangspunkt i en anerkjent standard for ledelsessystemer for informasjonssikkerhet.

Standardene omtales nærmere i neste kapittel om revisjonskriterier (kapittel 3.2 og 3.3).

2.1.1 Valg av virksomheter

Ved valg av virksomheter har vi tatt utgangspunkt i alle de totalt 24 forskningsvirksomhetene under departementet. Vi har lagt vekt på følgende kriterier:

[22] Totalt 29 virksomheter under Kunnskapsdepartementet er omfattet av styringsmodellen. Av disse driver 24 forskningsvirksomhet, og er omfattet av denne undersøkelsen: Ti universiteter, fem høyskoler og seks vitenskapelige høyskoler, samt Simula Research Laboratory AS, Universitetssenteret på Svalbard AS (UNIS) og Norsk utenrikspolitisk institutt (NUPI).

- Virksomhetene må ha et stort omfang av forskning der vesentligheten er høy dersom forskningsdata kommer på avveier, slettes, eller manipuleres.
- Virksomhetene må ha *sensitive* forskningsdata (personopplysninger eller etterretnings- eller forretningssensitive data). [23]
- Det må være variasjon i det samlede utvalget i blant annet størrelse, type virksomhet og faglig profil.

De tre virksomhetene som ble valgt ut for **dybdeundersøkelse**, er [redacted]. I tillegg til at vi ønsket virksomheter med noe ulik størrelse, var vi særlig opptatt av å dekke ulike fagområder og typer sensitive forskningsdata. I noe av datainnsamlingen ved disse avgrenset vi oss til utvalgte enheter som hadde store mengder forskningsdata med høy informasjonsverdi:

[redacted]

Vi gjennomførte de tre dybdeundersøkelsene suksessivt, fra april til november 2022.

De **øvrige syv virksomhetene vi undersøkte**, er [redacted]. I utvelgelsen av disse var vi opptatt av å få større variasjon i det samlede utvalget med tanke på størrelse og type virksomhet. Undersøkelsene hos disse virksomhetene ble gjennomført fra januar til mai 2023.

Vi valgte å inkludere alle de fire universitetene som ofte kalles BOTT-universitetene (Bergen, Oslo, Tromsø og Trondheim), i det samlede utvalget fordi disse står for nesten to tredjedeler av forskningen som gjøres av virksomheter under Kunnskapsdepartementet.[24] De er dermed de mest vesentlige virksomhetene i sektoren for vårt formål.

I denne rapporten skiller vi noen steder mellom «store», «mellomstore» og «små» virksomheter. Dette er en grovkategorisering som vi baserer på blant annet antall ansatte og studenter ved virksomhetene. De store virksomhetene er BOTT-ene, de mellomstore er USN, UiS og Nord universitet, og de små er NIH, UNIS og NUPI. Det er store forskjeller også innad i disse kategoriene.

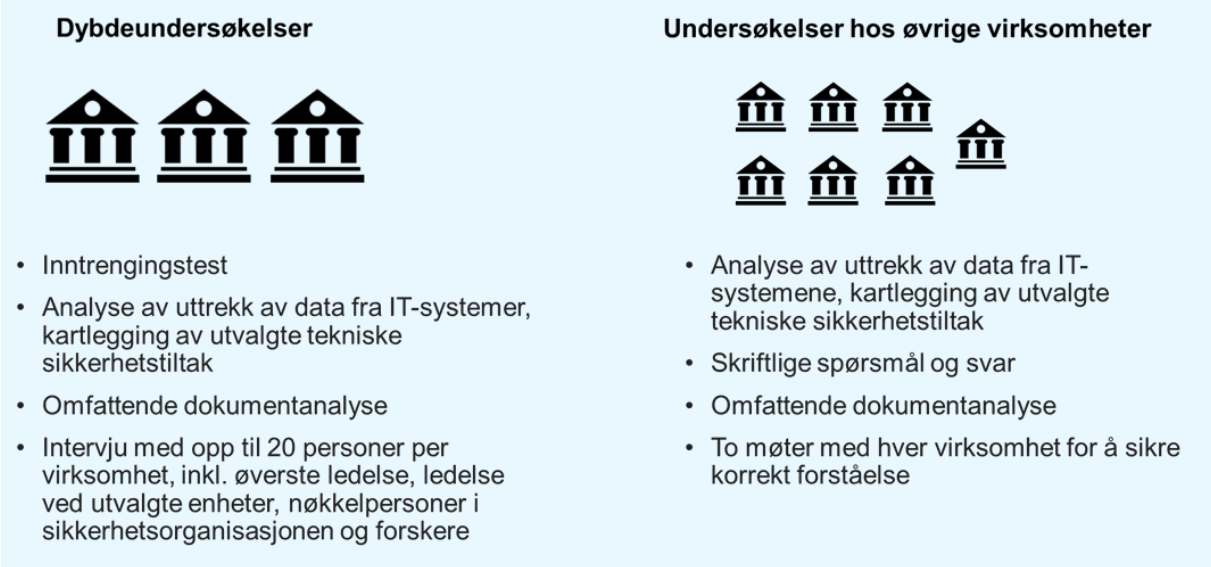
2.1.2 Metode for dybdeundersøkelser og undersøkelser hos øvrige virksomheter

Figuren nedenfor gir en oversikt over metodene som er brukt i henholdsvis dybdeundersøkelsene og undersøkelsene hos de øvrige virksomhetene.

[23] Alle virksomheter sitter på forskningsdata med høy vesentlighet for dem selv. Vi har vurdert hvilke virksomheter som har forskningsdata med høy vesentlighet for sektoren som helhet. Ved vurdering av hvorvidt virksomhetene kan ha sensitive data, har vi tatt utgangspunkt i informasjon om den faglige profilen til virksomhetenes forskning slik det er tilgjengeliggjort blant annet på deres nettsider, og holdt dette opp mot ulike kategorier av sensitive data (jf. faktaboks 1). For forskning med personopplysninger er det relativt enkelt å slå fast om det finnes slike forskningsdata. Når det gjelder andre typer sensitive forskningsdata har vi blant annet sett på om det foregår forskning i samarbeid med næringslivet og/eller oppdragsforskning, samt om det forekommer forskning innenfor fagområder som Utenriksdepartementet og/eller sikkerhetstjenestene anser at kan være av særlig interesse for fremmede stater.

[24] Disse fire institusjonene stod for 18 633 vitenskapelige publikasjoner i 2022. De andre forskningsvirksomhetene under Kunnskapsdepartementet stod til sammenligning for 9 835 vitenskapelige publikasjoner samme år. Kilde: https://www.cristin.no/statistikk-og-rapporter/nvi-rapportering/tidligere-ar/

Figur 1 Metode for dybdeundersøkelse i tre virksomheter og undersøkelser hos øvrige syv virksomheter



Inntrengingstest. I dybdeundersøkelsene har vi gjennomført en inntrengingstest (ofte kalt penetrasjonstest) for å teste om sikkerhetstiltakene i praksis hindrer en angriper fra å hente ut, manipulere eller slette forskningsdata. Vi har basert oss på allment akseptert metodikk for inntrengingstesting.[25] Kun kjente verktøy som er åpent tilgjengelig på Internett, ble benyttet. Gjennomføring av testene ble avtalt med den enkelte virksomhet før vi startet.

«Målet» i testene var å få tilgang til sensitive forskningsdata, enten via administrative rettigheter til systemene eller ved å utnytte rettigheter hos enkeltforskere. Framgangsmåten vi brukte, varierte noe mellom de tre forskningsinstitusjonene ettersom vi fulgte «minste motstands vei» mot målet.

Inntrengingstestene skulle også teste virksomhetenes evne til å oppdage aktiviteter i et dataangrep. Vi gjorde ingen forsøk på å skjule angrepene, men produserte mye nettverkstrafikk og andre kjente tegn på angrep. Vi ba om å bli orientert når forskningsvirksomhetene oppdaget aktiviteter i testen, men henstilte om at de ikke grep inn. Dette fordi formålet med kontrollene var å teste evnen til å oppdage aktiviteter i et dataangrep, ikke responsevne eller håndtering av hendelser.

Inntrengingstestene ble gjennomført før vi hadde fått uttrekk av tekniske data om virksomhetenes IT-systemer, jf. neste punkt. De ble dermed gjennomført uten kunnskap om virksomheten utover informasjon som var offentlig tilgjengelig.

Analyse av uttrekk av tekniske data fra systemer. For å vurdere om virksomhetene har etablert tilstrekkelige tekniske sikkerhetstiltak for å forebygge og avdekke angrepsforsøk, har vi trukket ut og analysert informasjon fra virksomhetenes IT-systemer. Formålet er å få et helhetlig bilde av de tekniske sikkerhetstiltakene i virksomhetene. Disse analysene utfyller dermed bildet fra inntrengingstestene – som viser hvordan konkrete svakheter kan utnyttes for å få kontroll med IT-systemer, men kun involverer et lite antall tekniske sikkerhetstiltak.

Kontrollen av tekniske sikkerhetstiltak er rettet mot virksomhetenes IT-infrastruktur som helhet, og ikke kun systemer der det lagres forskningsdata. Dette har sammenheng med at forskningsdata kan være lagret på mange plattformer, fra skytjenester til ulike servere til forskeres PC-er. Disse vil ha ulike sikringstiltak og nivåer og være svært forskjellige.

[25] Metoden vi anvendte, er satt sammen fra anerkjente kilder i bransjen, som for eksempel grunnlaget for sertifiseringen «Certified Ethical Hacker» fra EC-Council og OSSTMM 3 (The Open Source Security Testing Methodology Manual) utgitt av ISECOM (The Institute for Security and Open Methodologies).

I de tre virksomhetene hvor vi gjennomførte dybdeundersøkelser, ba vi om flere uttrekk. Et viktig uttrekk var fullstendig informasjon fra Active Directory (jf. faktaboks 3), som ga oversikt over alle brukerkontoer, maskiner, grupper og gruppemedlemskap i virksomhetenes Microsoft Windows-baserte nettverk. I tillegg ba vi om uttrekk fra stikkprøver av syv til ti utvalgte servere med Windows som operativsystem, samt tilsvarende stikkprøver fra servere med Linux-baserte operativsystem og et utvalg databaser. Utvalget i disse stikkprøvene hadde som intensjon å inkludere ulike grupper av servere som kunne gi et bilde av virksomhetens praksis. I tillegg ble det hentet ut data fra ca. 50 tilfeldig valgte klientmaskiner i virksomhetens nettverk.

Uttrekkene omtalt i forrige avsnitt inkluderte blant annet

- oversikt over alle brukeridentiteter og deres rettigheter. Disse ble analysert for blant annet å vurdere om det er satt opp systemer for å avgrense brukerrettigheter til tjenstlig behov. Vi undersøkte særlig brukeridentiteter med utvidede rettigheter som kan administrere hele eller deler av IT-infrastrukturen;
- data som viser hvilke sikkerhetsoppdateringer som er installert på de enkelte maskiner, samt hvilken versjon av ulike programvarer som ble benyttet. Dataene ble sammenlignet med hvilke oppdateringer som var tilgjengelige fra leverandøren på uttrekkstidspunktet, for å vurdere om virksomhetenes rutiner sikrer at alle relevante oppdateringer blir installert;
- data som viser konfigurasjon av maskiner og programvare. Dataene ble sammenlignet med god praksis for sikker konfigurasjon for å vurdere hvordan virksomhetenes tiltak herder systemene sine og reduserer risikoen for at dataangrep lyktes.
- data som viser hva som logges på utvalgte maskiner, ble hentet ut og sammenlignet med god praksis for å vurdere virksomhetenes grunnlag for å kunne oppdage dataangrep.

I tillegg har vi i disse tre virksomhetene skannet virksomhetenes nettverk for å kunne vurdere om nettverket har blitt delt inn i nettverkssoner basert på systemenes sensitivitet. Målet var å finne ut om det er etablert begrensinger i kommunikasjon mellom viktige soner der for eksempel forskningsdata lagres eller IT-systemer administreres, og soner med høyere risiko der studenters eller ansattes IT-utstyr befinner seg.

Vi ba også om uttrekk av data for de øvrige syv virksomhetene, men ikke like omfattende. På samme måte som omtalt ovenfor ble det innhentet uttrekk av Active Directory og fra stikkprøver av servere og klienter som benytter Microsoft Windows. Vi innhentet imidlertid ikke uttrekk fra servere basert på Linux eller fra databaser, og vi skannet ikke nettverk. I vurderingen av disse virksomhetene måtte vi derfor i noe større grad basere oss på svar på skriftlige spørsmål om sikkerhetstiltakene som var iverksatt, samt dokumenter som beskrev tiltakene (policyer, retningslinjer og rutiner), jf. neste punkt om dokumentanalyse.[26]

Dokumentanalyse. For alle de ti virksomhetene gjennomførte vi omfattende dokumentanalyse.

Både i dybdeundersøkelsene og i de øvrige syv virksomhetene har vi gjennomgått dokumenter som stiller krav til tekniske og organisatoriske sikkerhetstiltak for å beskytte forskningsdata (policyer og retningslinjer), eller som beskriver hvordan kravene skal gjennomføres i praksis (rutiner). For eksempel har vi gjennomgått dokumenter som beskriver krav til og rutiner for administrasjon av tilgangsrettigheter, klassifisering av forskningsdata etter sensitivitet eller sikker lagring av dataene. Analyser av dokumentene har vært viktige for å kunne vurdere sikkerhetstiltakene som er iverksatt.

Vi har også gjennomgått dokumenter som kan si noe om hvor systematisk virksomhetene har arbeidet med informasjonssikkerhet og personvern. Dette omfatter gjennomgang av ulike dokumenter i virksomhetenes ledelsessystemer på området. Vi har undersøkt om virksomhetene har utarbeidet en

[26] Områder hvor vi i større grad baserte oss på skriftlige spørsmål og svar: nettverkssikkerhet (jf. kap. 5.4), logging og overvåkning (jf. kap. 5.5) og sikker konfigurasjon av IT-systemer (jf. kap. 5.3.2).

overordnet policy med tydelige sikkerhetsmål og sikkerhetsstrategi og planer for arbeidet, og om organisering og ansvarsfordeling syntes å være tydelig og hensiktsmessig. Videre har vi undersøkt om det forelå rutiner for

- gjennomføring av risikovurderinger
- evalueringer og revisjoner
- håndtering av sikkerhetsavvik og -hendelser
- ledelsens gjennomgang

I tillegg innhentet vi dokumentasjon som var egnet til å si noe om hvordan systemene fungerer i praksis – risikovurderinger og handlingsplaner for å håndtere risiko, revisjoner og evalueringer, oversikter over avvik og sikkerhetshendelser, dokumentasjon av ledelsens gjennomgang, ledermøtereferater, årsrapporter mm. Vi undersøkte også om vi kunne finne spor av det ledelsen beslutter, samt de risikovurderinger og kontroller som gjennomføres, i de konkrete sikkerhetstiltakene. I tillegg innhentet vi dokumenter som kunne belyse hvordan styret har ivaretatt sitt ansvar.

Vi samlet alle kvalitative data, inkludert intervjureferater nevnt i neste punkt, i analyseverktøyet NVivo. Vi brukte dette verktøyet til systematisk gjennomgang av dataene og søk/oppslag.

Intervjuer. Ved de tre utvalgte virksomhetene gjennomførte vi totalt 54 intervjuer. Vi gjennomførte tre typer intervjuer:

- Vi gjennomførte **virksomhetsintervjuer** med representanter for øverste administrative ledelse, samt ledere ved to utvalgte enheter ved hver institusjon. [redacted][27] I etterkant av disse intervjuene fikk intervjuobjektene tilsendt referatet for å gjennomgå og verifisere det.
- Vi **intervjuet nøkkelpersonell** i den sentrale sikkerhetsorganisasjonen og ute på de nevnte enhetene. Vi intervjuet blant andre informasjonssikkerhetsledere, personvernombud, ledere for sentral IT-avdeling eller seksjon for IT-drift og representanter for lokale IT-driftsmiljøer. Det viktigste formålet med intervjuene var å få klarhet i hvordan arbeidet foregikk i praksis. Opplysninger fra disse intervjuene ble verifisert gjennom en skriftlig oppsummering av undersøkelsen ved hver virksomhet, se nærmere omtale i punkt 2.1.3.
- Vi gjennomførte **kvalitative intervjuer** med representanter for totalt 13 forskningsprosjekter med data som var beskyttelsesverdige av ulike årsaker. Alle disse prosjektene ble hentet fra de utvalgte enhetene nevnt ovenfor.

Ved hver av de øvrige syv virksomhetene gjennomførte vi to oppfølgingsmøter med nøkkelpersonell i den sentrale sikkerhetsorganisasjonen for å sikre korrekt forståelse: ett møte hvor vi gjennomgikk observasjoner og spørsmål knyttet til tekniske sikkerhetstiltak, og ett møte hvor vi gjennomgikk observasjoner og spørsmål knyttet til organisatoriske sikkerhetstiltak og systematikken i arbeidet.

Skriftlige spørsmål. Vi stilte skriftlige spørsmål til alle de ti virksomhetene som inngår i undersøkelsen. For de syv virksomhetene som ikke inngikk i dybdeundersøkelsen, og hvor vi ikke gjennomførte intervjuer, måtte vi i større grad basere oss på skriftlige spørsmål til virksomhetene.

Gjennomgang av sekundærdata. I tillegg til dette har vi gjennomgått sekundærdata fra HK-dir om alle de ti forskningsvirksomhetene. Direktoratet gjennomfører årlige kartleggingsmøter med virksomhetene der de blant annet opplyser om nye informasjonssikkerhets- og personverntiltak. Det lages referater fra møtene, og HK-dir utarbeider anbefalingsbrev til den enkelte virksomheten.

[27] [redacted]

2.1.3 Tilbakemelding om tekniske svakheter og kvalitetssikring av analyser

Alle de ti forskningsvirksomhetene fikk umiddelbart tilbakemeldinger om svakheter som ble avdekket gjennom tekniske kontroller:

- De tre virksomhetene i dybdeundersøkelsene ble informert om alle svakheter vi fant gjennom inntrengingstestene, like etter at disse var gjennomført.
- Alle de ti virksomhetene fikk en presentasjon av svakheter som vi avdekket gjennom kartlegging av tekniske sikkerhetstiltak. I tillegg oversendte vi detaljerte underlagsdata om dette til alle virksomhetene.

I tillegg utarbeidet vi en skriftlig oppsummering til den enkelte virksomhet for gjennomgang, der vi inkluderte våre foreløpige analyser av virksomhetens tekniske sikkerhetstiltak, organisatoriske sikkerhetstiltak, samt systematikk i informasjonssikkerhetsarbeidet. Dette gjorde vi for alle de ti virksomhetene. Hensikten med dette var å kvalitetssikre analysene.

I disse analysene sammenstilte vi det som framgikk av tekniske tester og gjennomgang av tilsendte dokumenter, med det som framgikk av intervjuer og møter med virksomhetene. Vi inkluderte ikke informasjon fra kvalitative intervjuer med forskere i oppsummeringene. Vi ba alle virksomhetene om å påpeke eventuelle faktafeil eller forhold vi hadde misforstått, samt å opplyse om forhold de mente at analysen vår la for stor eller for liten vekt på. Alle virksomhetene har gitt en tilbakemelding på dette, de fleste skriftlig.

2.2 Metodisk tilnærming til problemstilling 3

I denne problemstillingen har vi sett på hvordan departementet har ivaretatt det overordnede ansvaret de har for informasjonssikkerhet i sektoren. Vi har vært særlig opptatt av hvordan departementet har fulgt opp og støttet opp under informasjonssikkerhetsarbeidet i forskningsvirksomhetene under departementet.

Dokumentanalyse. For å se hvordan Kunnskapsdepartementet har fulgt opp forskningsvirksomheter gjennom styringen, har vi gjennomgått tildelingsbrev fra Kunnskapsdepartementet til forskningsvirksomhetene som omfattes av undersøkelsen for de siste fire årene. Vi har også gjennomgått annen dokumentasjon på departementets etatsstyring og eieroppfølging som omhandler informasjonssikkerhet, herunder også departementsinterne notater som beskriver oppfølgingen.

For å vurdere hvordan departementet har understøttet informasjonssikkerhetsarbeidet i virksomhetene i undersøkelsesperioden 2019–2022, har vi blant annet gjennomgått

- referater fra møter mellom departementet, HK-dir og Sikt
- dokumentasjon på departementets styringsmodell for informasjonssikkerhet og personvern
- dokumentasjon fra årlige risiko- og tilstandsvurderinger, samt etterfølgende dialog mellom departementet og HK-dir
- dokumentasjon på resultater av fireårssatsingen, samt
- dokumentasjon om Uninett Cert / Cybersikkerhetssenteret for forskning og utdanning (eduCSC) og tjenestene de leverer til sektoren

Intervju. Vi har gjennomført virksomhetsintervjuer med Kunnskapsdepartementet, HK-dir og Sikt for å få utfyllende informasjon om forholdene nevnt ovenfor.

Vi har også brukt intervjuer med ledelsen i de tre virksomhetene i dybdeundersøkelsen til å få deres syn på departementets styring og virkemiddelbruk.

Spørsmål til utvalgte virksomheter. For å få mer informasjon om hvordan departementets styring og virkemiddelbruk fungerer, stilte vi skriftlige spørsmål om dette i brev til de syv øvrige forskningsvirksomhetene.

Vi har også sendt skriftlige spørsmål til NTNU, UiO og UiB om deres eieroppfølging av utvalgte underliggende selskaper som behandler forskningsdata (teknologioverføringsselskaper og NORCE).

3 Revisjonskriterier

3.1 Forskningsdata som skal beskyttes i samsvar med lover, regler og nasjonale føringer

Forskningen som gjøres ved virksomheter underlagt Kunnskapsdepartementet, skal som hovedregel gjøres offentlig tilgjengelig. Politikken for tilgjengeliggjøring av offentlige data i Norge er beskrevet i *Meld. 22. S (2020–2021) Data som ressurs – datadrevet økonomi og innovasjon*, som ble behandlet i *Innst. 568 S (2020–2021).* Meldingen beskriver de nasjonale prinsippene for deling av data, og slår blant annet fast at offentlige data skal «åpnes når de kan og skjermes når de må».

Personopplysningsloven og personvernforordningen, helseforskningsloven, og helseregisterloven stiller krav til hvordan personopplysninger behandles i forskning. Personvernforordningen legger, ved siden av **konfidensialitet**, vekt på sikring av **integriteten** og **tilgjengeligheten** til personopplysningene som behandles.[28] Personopplysningsloven og -forordningen stiller spesielt strenge krav til behandling av *særlige kategorier av personopplysninger*.[29,30]

Eksportkontrolloven slår fast at varer og teknologi som kan ha betydning for andre lands utvikling, produksjon eller anvendelse av produkter til militært bruk, eller som direkte kan tjene til å utvikle et lands militære evne, eller som kan benyttes til å utøve terrorhandlinger, ikke må føres ut av Norge uten særskilt tillatelse.[31] For virksomhetene i høyere utdanning og forskning innebærer regelverket at de må føre kontroll med kunnskap om teknologi som har direkte eller indirekte militær relevans, slik at kunnskapen ikke overføres til ansatte, stipendiater og studenter fra visse land[32] gjennom for eksempel rekruttering og ansettelse, forskningssamarbeid, eller utveksling.[33]

I tillegg kommer lover og regler som dekker et bredere spekter av opplysninger. I samsvar med sikkerhetsloven skal informasjon ***sikkerhetsgraderes*** dersom det kan skade nasjonale sikkerhetsinteresser om den *blir kjent for uvedkommende*.

Sikkerhetsloven dekker imidlertid også informasjon som skal ligge åpent tilgjengelig, dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen *går tapt, blir endret eller blir utilgjengelig.* Informasjon er ***skjermingsverdig*** ifølge loven dersom ett av disse kriteriene oppfylles. Alle Kunnskapsdepartementets underliggende virksomheter omfattes av sikkerhetsloven, men det er ikke alle som har skjermingsverdige informasjonsverdier.[34]

Beskyttelsesinstruksen dekker informasjon som trenger beskyttelse av andre grunner enn det som framgår av sikkerhetsloven. Instruksen stiller opp to ***beskyttelsesgrader***:[35,36]

- «Strengt fortrolig» benyttes dersom det vil kunne forårsake betydelig skade for *offentlige interesser, en bedrift, en institusjon eller en enkeltperson* at innholdet i dokumentet blir kjent for uvedkommende.

[28] Personvernforordningen artikkel 32, punkt 1 bokstav b og punkt 2.
[29] Personopplysningsloven §§ 6, 7, 9 og 10, Personvernforordningen artikkel 9. I tillegg tar artikkel 10 for seg personopplysninger om straffedommer og lovovertredelser, som også er underlagt spesielle begrensinger.
[30] Særlige kategorier av personopplysninger omfatter personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
[31] Eksportkontrolloven § 1.
[32] Land underlagt eksportrestriksjoner eller land hvor det er begrunnet mistanke eller konkret informasjon om bekymringsfulle aktiviteter knyttet til utvikling og bruk av masseødeleggelsesvåpen og deres leveringsmidler.
[33] Utenriksdepartementet har utarbeidet egne retningslinjer for norske utdanningsinstitusjoners arbeid med opptak og ansettelser av utenlandske personer innenfor slike fagområder: https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/
[34] Kunnskapsdepartementet. (2021). *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*, side 33.
[35] Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen), § 4 *Om bruken av beskyttelsesgrader*.
[36] Merk at det er et absolutt vilkår for gradering etter beskyttelsesinstruksen at dokumentet må kunne unntas fra offentlighet i medhold av offentleglova, jf. instruksen § 3. Dette henger sammen med at instruksen ikke har hjemmel i formell lov og derfor ikke utgjør en selvstendig hjemmel for unntak fra innsyn etter offentleglova. Kilde: *NOU 2016: 19 Samhandling for sikkerhet − Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*, side 155.

- «Fortrolig» benyttes dersom det vil kunne skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson at innholdet i dokumentet blir kjent for uvedkommende.

Når virksomhetene samarbeider med bedrifter og andre institusjoner, kan de i noen tilfeller også inngå avtale om at forskningsdataene skal beskyttes. For eksempel inngår virksomhetene i noen tilfeller fortrolighetsavtaler med eksterne parter hvis forskningsdataene kan ha kommersiell verdi.

I den avsluttende fasen av et forskningsprosjekt stilles det også særskilte krav til hvordan forskningsdata skal håndteres, for eksempel at data skal arkiveres. Arkivloven skal sikre arkiver som har stor kulturell eller forskningsmessig verdi, eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon. Offentlige organer plikter å ha arkiv som er ordnet og innrettet slik at dokumentene er sikret som informasjonskilder for samtid og ettertid.[37]

3.2 Krav til sikkerhetstiltak for å beskytte forskningsdata

Virksomhetene som omfattes av undersøkelsen, har selv ansvaret for informasjonssikkerheten og personvernet i egen forskning.[38] I Meld. St. 27 (2015–2016) *Digital agenda for Norge* står det at virksomhetsledelsen skal gjøre nødvendige tiltak for å sikre at risikoen er begrenset til et forsvarlig nivå.[39]

Regjeringen lanserte i 2019 en *Nasjonal strategi for digital sikkerhet*, som omtales i Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*. I Innst. 275 S (2020–2021) viser justiskomiteen til strategien og registrerer at regjeringen vil følge opp denne. Et av de overordnede målene i strategien er at norske virksomheter digitaliserer på en sikker og tillitvekkende måte og beskytter seg bedre mot uønskede digitale hendelser. I den nasjonale strategien er det utarbeidet ti anbefalte tiltak som virksomheter bør følge for å styrke den digitale sikkerheten. Tiltakene gjengis i meldingen.[40]

Lovverket stiller konkrete krav til virksomhetenes sikkerhetstiltak og sikkerhetsnivå. Det benyttes ulike begreper i lovgivningen:

- Sikkerhetsloven § 4-2 slår fast at virksomhetene skal iverksette ***forebyggende sikkerhetstiltak*** basert på vurdering av risiko. I samsvar med § 4-3 skal virksomheter gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et ***forsvarlig sikkerhetsnivå***.
- Personvernforordningen artikkel 32 og 24 stiller krav om at virksomheter som har ansvar for behandling av personopplysninger (behandlingsansvarlig), skal gjennomføre ***tekniske og organisatoriske tiltak*** for å oppnå ***et sikkerhetsnivå som er egnet med hensyn til risikoen***.

Stortinget har ved behandling av flere stortingsmeldinger lagt vekt på betydningen av opplæring og kompetanseheving.[41] I tillegg stilles det krav om slike tiltak i ulike lovverk:

- I sikkerhetsloven § 4-1 stilles det krav om at virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse.
- I personvernloven/personvernforordningen stilles det krav om holdningsskapende tiltak og opplæring av personell som håndterer personopplysninger.

[37] Lov om arkiv (arkivloven) § 1 og § 6.
[38] Meld. St. 38 (2016–2017) *IKT-sikkerhet, et felles ansvar*, side 19.
[39] Meld. St. 27 (2015–2016) *Digital agenda for Norge*, side 150.
[40] Meld. St. 5 *(2020–2021) Samfunnssikkerhet i en usikker verden*, faktaboks på side 81. Blant annet anbefales det at virksomheter kartlegger verdikjeder, informasjonsverdier, utstyr og brukertilganger, sørger for kontroll på nettverk og systemkomponenter, sikker konfigurasjon og tilgangskontroller, samt iverksetter tiltak for å sikre e-post og data og tjenester på internett (websikkerhet). Det anbefales også at virksomhetene kartlegger egen sikkerhetskultur, og gjennomfører tiltak for at ansatte har nødvendig informasjon, kunnskap og ferdigheter til å opprettholde ønsket sikkerhetsnivå. Videre anbefales det at virksomhetene stiller krav til sikkerheten hos leverandører av IKT-tjenester og -produkter.
[41] Det legges vekt på dette i *Innst. 275 S (2020–2021)* til *Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden,* samt *Innst. 187 S (2017–2018)* til *Meld. St. 38 (2016–2017) IKT-sikkerhet, et felles ansvar.* For eksempel står det i sistnevnte at: «Flertallet mener kunnskap om IKT-sikkerhet er avgjørende for bevisstgjøring og forebygging, og at denne type kunnskap er av stor betydning for å fremme en kultur for sikker adferd.» Side 4.

- I forskningsetikkloven stilles det krav om at forskningsinstitusjoner gir nødvendig opplæring av ansatte i anerkjente forskningsetiske normer (herunder konfidensiell behandling av personopplysninger).[42]

Begrepet «pedagogiske tiltak» brukes av og til for å beskrive slike tiltak. Vi har valgt å skille mellom tekniske og organisatoriske tiltak og har inkludert opplæring og kompetanseheving under sistnevnte.

Virksomhetene som samarbeider med bedrifter og andre institusjoner, kan avtale et høyere sikkerhetsnivå enn det som kreves i lovverket. Hver av partene har da en avtalerettslig forpliktelse overfor hverandre til å oppnå det sikkerhetsnivået man har avtalt.[43]

For å vurdere sikkerhetstiltak for å beskytte forskningsdata og IT-systemene de behandles i, er det nødvendig med mer detaljerte revisjonskriterier. Vurderingen vår av organisatoriske sikkerhetstiltak tar utgangspunkt i standarden NS-ISO/IEC 27002:2017, som gir en oversikt over alminnelig aksepterte tiltak for informasjonssikkerhet. For tekniske sikkerhetstiltak går vi ut fra at NSMs grunnprinsipper for IT-sikkerhet representerer en generelt akseptert god praksis i Norge.

3.2.1 Krav til tekniske sikkerhetstiltak

Vi tar utgangspunkt i tekniske sikkerhetstiltak som virksomhetene ifølge god praksis bør iverksette, og hvordan disse tiltakene bør implementeres. For å konkretisere anbefalingene til forskningsvirksomheten om god praksis for å oppnå et egnet sikkerhetsnivå har vi brukt NSMs grunnprinsipper for IT-sikkerhet.

Grunnprinsippene legger vekt på at virksomhetene skal ha oversikt over IT-infrastruktur og -systemer. Videre bør virksomhetene sette i verk hensiktsmessige tiltak for å sikre infrastrukturen og systemer, og de bør etablere systemer for å oppdage og håndtere hendelser som dataangrep.

Støtteverktøy for grunnprinsippene viser hvilke av de 118 anbefalte tiltakene som er viktigst å prioritere for å hindre eller oppdage dataangrep.[44] Tilsvarende oversikter over hvilke sikkerhetstiltak som er viktigst, er også gitt ut av andre aktører, for eksempel The Center for Internet Security (CIS).[45] I tråd med disse kildene har vi i denne revisjonen valgt å kontrollere følgende sikkerhetstiltak opp mot god praksis:

- **Virksomheten fører kontroll med brukerkontoer og tilgangsrettigheter**, herunder administrator- og servicekontoer (brukerkontoer som benyttes av programvare). Formålet med sikkerhetstiltakene er å hindre angripere i å få tilgang til, eller utvide tilgangen til, virksomhetens IT-infrastruktur og sensitive forskningsdata.
- **Virksomheten sørger for at brukerne autentiseres på en sikker måte** med passord og en annen faktor (for eksempel en applikasjon på brukerens mobiltelefon) når de logger på virksomhetens nettverk og tjenester. Formålet med sikker autentisering er å hindre at angripere stjeler en brukers påloggingsrettigheter og misbruker dem.
- **Virksomheten har kontinuerlig sårbarhetsstyring** gjennom å oppdatere programvare, skanne nettverk for å avdekke sårbarheter og bruke sikker konfigurasjon (herding) av maskiner og programvare. Formålet er å hindre at kjente sårbarheter i programvare gir angripere mulighet til å få tilgang til og kontroll over utstyr og programvare i virksomhetene.

[42] Av veiledningsmateriellet utarbeidet av De nasjonale forskningsetiske komiteene framgår det at en av de forskningsetiske normene er at de som gjøres til gjenstand for forskning, i utgangspunktet har krav på at personlig informasjon blir behandlet konfidensielt.
[43] Avtaleloven setter de grunnleggende reglene for inngåelse av avtaler, og hovedregelen er at partene fritt kan velge hva avtalen skal inneholde, med mindre avtalens innhold i seg selv er ulovlig.
[44] Støtteverktøy for NSMs grunnprinsipper for IKT-sikkerhet 2.0.
[45] CIS Controls utgitt av CIS er en internasjonalt anerkjent anbefaling for beste praksis for tekniske sikkerhetstiltak, hvor det også vises hvilke tiltak en virksomhet bør prioriteres å etablere.

- **Virksomheten deler IT-nettverket inn i soner**, begrenser datatrafikken mellom disse sonene og fører kontroll med utstyr som kan koble seg til nettverket. Formålet er å hindre at en angriper kan få et fotfeste i virksomhetens nettverk ved å koble sitt utstyr til nettverket, og å hindre tilgang til systemer med sensitive forskningsdata dersom angriperen faktisk lyktes med å få et fotfeste i nettverket.
- **Virksomheten logger og overvåker**. Virksomheten samler inn, forvalter og analyserer data fra nettverk og enheter med mål om å oppdage uønskede hendelser. Slik skal virksomheten kunne oppdage, forstå og legge grunnlag for å kunne håndtere angrep.

I noen tilfeller er det nødvendig å bruke mer detaljerte kriterier for å undersøke om virksomhetene følger god praksis. Det gjelder for eksempel vurdering av hvilke innstillinger som bør vurderes for sikker konfigurasjon av et system, eller hvilke hendelser som bør logges. I slike tilfeller har vi basert god praksis på anbefalinger fra CIS eller leverandører.

3.2.2 Krav til organisatoriske sikkerhetstiltak

Når vi har vurdert organisatoriske sikkerhetstiltak, har vi tatt utgangspunkt i standarden NS-EN ISO/IEC 27002:2017. Ut fra standarden har vi valgt ut noen sikkerhetstiltak som er viktige for å beskytte forskningsdata og IT-systemene de behandles i:

- **Virksomheten har oversikt over informasjonsverdier i forskning.** Standarden anbefaler at virksomheten identifiserer informasjonsverdier og skaffer seg oversikt over disse. Den anbefaler også at informasjon klassifiseres i samsvar med blant annet juridiske krav, verdi og sensitivitet.[46]
- **Virksomheten har rutiner for sikker behandling av forskningsdata.** Standarden anbefaler at regler for akseptabel bruk av informasjonsverdier identifiseres, dokumenteres og implementeres.[47] Virksomhetene i undersøkelsen bør blant annet ha etablert regler/rutiner for håndtering, klassifisering og lagring av forskningsdata.
- **Virksomheten lærer opp og bevisstgjør forskere og andre.** Standarden anbefaler at ansatte og andre med tilgang til informasjonsverdier bør gjøres oppmerksom på reglene. Standardene anbefaler også å iverksette nødvendige tiltak for bevisstgjøring og opplæring om informasjonssikkerhet, herunder at ansatte får oppdateringer om rutiner som er relevant for deres jobbfunksjon.[48]
- **Virksomheten ivaretar eierskap og forvaltning av IT-systemer i forskning.** Ifølge standarden er det viktig at virksomhetene har oversikt over IT-systemer og -utstyr som brukes, og at det er avklart hvordan virksomheten skal ivareta eierskap, forvaltning og drift av systemene.[49]
- **Virksomheten følger opp informasjonssikkerhet i leverandørforhold.** Standarden anbefaler å definere og implementere prosesser og prosedyrer å håndtere informasjonssikkerhetsrisikoene ved bruk av leverandørers produkter eller tjenester. Standarden anbefaler at alle relevante krav til informasjonssikkerhet avtales med leverandøren og dokumenteres.[50]

3.3 Krav til ledelse og systematikk i virksomhetenes arbeid med informasjonssikkerhet

For å velge de riktige sikkerhetstiltakene og oppnå og opprettholde et sikkerhetsnivå som oppfyller kravene i lovverket, må virksomhetene ha en systematisk tilnærming. Ledelsen må sørge for dette ved

[46] NS-EN ISO/IEC 27002:2017: punkt 8.1.1 og 8.2.1.
[47] NS-EN ISO/IEC 27002:2017: punkt 8.1.3.
[48] NS-EN ISO/IEC 27002:2017: punkt 7.2.2.
[49] NS-EN ISO/IEC 27002:2017: punkt 8.1.1 og 8.1.2.
[50] NS-EN ISO/IEC 27002:2017: punkt 15.

å etablere et ledelsessystem − som også kan omtales som kvalitetssystem, styringssystem eller internkontrollsystem – for informasjonssikkerhetsarbeidet. Ledelsessystemet skal sette planlegging, gjennomføring (de konkrete tiltakene), kontroll/evaluering og oppfølging av informasjonssikkerhetsarbeidet i system.

Flere lover/regelverk pålegger virksomhetene å ha et ledelsessystem for informasjonssikkerhet. Blant annet stilles det krav om dette i eForvaltningsforskriften, sikkerhetsloven[51] og personvernforordningen. tillegg stilles det mer generelle krav til virksomhetenes internkontroll i regelverket for økonomistyring i staten (*reglementet for økonomistyring i staten* og *bestemmelser om økonomistyring i staten*). De viktigste kravene i nevnte lover og regler kan oppsummeres slik:

- Virksomhetens leder har ansvaret for sikkerhetsarbeidet.[52]
- Sikkerhetsmålene og sikkerhetsstrategien skal danne grunnlaget for virksomhetens styring og kontroll på informasjonssikkerhetsområdet.[53]
- Det skal utarbeides et ledelsessystemet for informasjonssikkerhet basert på anerkjente standarder. Ledelsessystemet bør være en integrert del av virksomhetens helhetlige kvalitetssystem.[54]
- Virksomhetene skal regelmessig vurdere risikoen, og risikovurderingene skal danne grunnlag for iverksetting av sikkerhetstiltak.[55]
- Det skal gjennomføres regelmessige kontroller/evalueringer av sikkerhetstilstanden/sikkerhetstiltakene, og disse skal følges opp.[56,57]

Både i selskapene, ved universiteter og høyskoler og i forskningsinstituttet NUPI er styret det øverste organet. For alle disse typene virksomheter har styret det overordnet ansvar for at institusjonene drives i overensstemmelse med gjeldende lover, forskrifter og regler, og å føre tilsyn med den daglige ledelsen, herunder hvordan ledelsen ivaretar informasjonssikkerhet.[58]

For å vurdere systematikken i informasjonssikkerhetsarbeidet i virksomhetene har vi tatt utgangspunkt i NS-ISO/IEC 27001:2017. Dette er en anerkjent standard for ledelsessystemer for informasjonssikkerhet, som Digitaliseringsdirektoratet (Digdir) anbefaler offentlige organer å benytte.[59] Standarden dekker områdene som er nevnt i oppsummeringen av regel- og lovkrav ovenfor, men er mer konkret og utfyllende. Standarden framhever flere momenter, som vi legger til grunn som kjennetegn ved et systematisk informasjonssikkerhetsarbeid. Disse momentene er

- **mål, strategi, og plan for arbeidet.** Ifølge standarden bør den øverste ledelsen blant annet sikre at kravene i ledelsessystemet integreres i virksomhetens prosesser, og at det oppnår tiltenkte resultater. Den øverste ledelsen bør videre etablere en *overordnet informasjonssikkerhetspolicy* som inneholder blant annet informasjonssikkerhetsmål, og standarden stiller krav til planlegging for å nå målene.[60]

[51] Av *Styringsdokument for arbeid med sikkerhet og beredskap i Kunnskapsdepartementets sektor* framgår det at «alle departementets underliggende virksomheter omfattes av sikkerhetsloven og skal ha et dokumentert styringssystem for sikkerhet, uavhengig av om virksomheten har skjermingsverdige verdier».
[52] Sikkerhetsloven § 4-1 om sikkerhetsstyring.
[53] eForvaltningsforskriften § 15. Reglement for økonomistyring i staten § 9 stiller konkrete krav til planlegging, gjennomføring og oppfølging innenfor virksomhetenes ansvarsområder.
[54] eForvaltningsforskriften § 15, Sikkerhetsloven § 4-1. Reglement for økonomistyring i staten § 14 stiller et mer generelt krav om at virksomhetene etablerer systemer og rutiner som har innebygd intern kontroll, bl.a. for å sikre tilfredsstillende måloppnåelse og resultater, samt effektiv ressursbruk.
[55] Sikkerhetsloven § 4-2 og § 4-4, personvernforordningen artikkel 24 og 32.
[56] Sikkerhetsloven § 4-1 om sikkerhetsstyring, personvernforordningen artikkel 24 og 32. Artikkel 32 sier at virksomhetene, dersom det er egnet, bør ha «en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er». Reglementet for økonomistyring i staten § 16 stiller et mer generelt krav om at alle virksomheter skal sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater innenfor hele eller deler av virksomhetens ansvarsområde og aktiviteter
[57] I Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*, faktaboks 8.2 på side 81, anbefales det også at virksomheter kartlegger sikkerhetskulturen i egen virksomhet, for å danne grunnlag for opplæringstiltak rettet mot ansatte.
[58] Lov om universiteter og høyskoler § 9-1, aksjeloven § 6-13.
[59] I eForvaltningsforskriften står det at organet som Kommunal- og distriktsdepartementet peker på, skal gi anbefalinger til offentlige organer om internkontroll innenfor informasjonssikkerhet. Digdir fyller denne rollen og har i referansekatalogen for IT-standarder anbefalt at ISO/IEC 27001 legges til grunn.
[60] NS-EN ISO/IEC 27001:207 punkt 5.1, 5.2 og 6.2. Ved planlegging av hvordan målene skal oppnås, anbefales det at virksomheten fastsetter hva som skal gjøres, hvilke ressurser som blir nødvendige, hvem som har utføringsansvaret, når det skal være fullført, og hvordan resultatene skal evalueres

- **organisering og avklaring av roller og ansvar.** Hensiktsmessig organisering av arbeidet, samt avklaring av hvem som har hvilke roller og ansvar, er viktige forutsetninger for et effektivt informasjonssikkerhetsarbeid. I tråd med standarden bør ledelsen sikre at de nødvendige ressursene for ledelsessystemet for informasjonssikkerhet er tilgjengelige, og at ansvar og myndighet for roller som er relevante for informasjonssikkerheten, er tildelt og kommunisert.[61]
- **krav til sikkerhetstiltak.** For å understøtte en overordnet policy med sikkerhetsmål bør det utarbeides temaspesifikke policyer som pålegger implementering av sikkerhetstiltak. Slike policyer kan omfatte opplæring i informasjonssikkerhet, tilgangskontroll, konfigurering av systemer eller sikkerhetsovervåking. Policyene skal sikre at det ikke blir opp til den enkelte ansatte i virksomheten hvordan dette gjøres.[62]
- **risikovurdering og håndtering.** Ifølge standarden bør virksomheten utarbeide prosesser for risikovurdering på informasjonssikkerhetsområdet, gjennomføre risikovurderinger i tråd med prosedyrene, utarbeide planer for håndtering av informasjonssikkerhetsrisikoene og dokumentere resultatene fra håndteringen. Virksomheten bør fastsette alle sikkerhetstiltak som er nødvendige for å håndtere risikoene[63]
- **evaluering og kontroll.** Ifølge standarden bør virksomheten evaluere informasjonssikkerheten og virkningen av ledelsessystemet gjennom systematisk måling, og det bør gjennomføres interne revisjoner med planlagte intervaller for å gi informasjon om ledelsessystemet for informasjonssikkerhet.[64]
- **avviks- og hendelseshåndtering.** Ifølge standarden bør virksomheten reagere på avvik og, der det er nødvendig, iverksette tiltak for å korrigere avviket og håndtere konsekvensene.[65] NS-ISO 27002:2017 anbefaler også at hendelseslogger som registrerer informasjonssikkerhetshendelser, bør produseres, oppbevares og gjennomgås regelmessig.
- **ledelsens gjennomgang.** Den øverste ledelsen bør gjennomgå ledelsessystemet for informasjonssikkerhet med planlagte mellomrom, og vurdere blant annet status for tiltak fra tidligere gjennomganger, endringer i relevante eksterne og interne forhold, samt informasjon som gjør det mulig å vurdere oppnåelse av sikkerhetsmålene (som avvik og korrigerende tiltak, overvåkings- og måleresultater, resultater fra revisjoner, resultater fra risikovurderinger).[66]

Standarden forutsetter at et ledelsessystem tilpasses virksomheten. Virksomhetene i denne undersøkelsen er svært ulike med tanke på ressurser, størrelse og kompleksitet, og vi legger til grunn at dette også innebærer at de har ulike forutsetninger og behov, for eksempel ulike behov for dokumentasjon.

3.4 Krav til departementets styring og understøtting av arbeidet

I Meld. St. 38 *(2016–2017) IKT-sikkerhet − et felles ansvar* står det at hver enkelt statsråd har et overordnet ansvar for å ivareta IT-sikkerheten i egen sektor.[67] I sikkerhetsloven heter det at departementene er ansvarlige for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder.[68]

IT-sikkerhet inngår også i virkeområdet til *Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)*, der det stilles konkrete krav til departementenes styring av sikkerhetsarbeidet innenfor egen sektor. Sektorbegrepet omfatter både områder som kan

[61] NS-IEC/ISO 27001 (2017) punkt 5.1 c). og punkt 5.3.
[62] NS-EN ISO/IEC 27002:2017 punkt 5.1.1.
[63] NS-EN ISO/IEC 27001:2017 punkt 6.1.2 og 6.1.3.
[64] NS-EN ISO/IEC 27001:2017 punkt 9.1 og 9.2.
[65] NS-EN ISO/IEC 27001:2017 punkt 10.1.
[66] NS-EN ISO/IEC 27001:2017 punkt 9.3.
[67] Meld. St. 38 (2016–2017) *IKT-sikkerhet − et felles ansvar*, side 19, jf. Innst. 187 S (2017−2018)..
[68] Sikkerhetsloven § 2-1.

styres direkte av departementet, slik som områder som ivaretas av underlagte etater og virksomheter, og områder hvor styringsmulighetene er mer begrensede.[69]

Regelverket for økonomistyring i staten (*reglementet for økonomistyring i staten* og *bestemmelser om økonomistyring i staten*) og *bevilgningsreglementet* stiller mer generelle krav til departementets styring og virkemiddelbruk. Samfunnssikkerhetsinstruksen må ses i sammenheng med disse regelverkene.

De viktigste kravene som stilles til departementet, kan oppsummeres slik:

- **Det er krav om å følge opp virksomhetenes informasjonssikkerhetsarbeid.** Departementet må følge opp at underliggende virksomheter jobber for å nå mål og oppfylle krav på informasjonssikkerhetsområdet. Departementet må gi føringer på området gjennom styringsdokumenter og styringsdialog og sørge for at virksomhetene gir dem et tilstrekkelig informasjonsgrunnlag for styringen.[70] Mer generelt har de overordnet ansvar for at virksomhetene bruker ressurser effektivt, og at det gjennomføres kontroll med virksomhetene.[71]
- **Det er krav om å avklare roller, samt hensiktsmessig organisering og virkemiddelbruk.** Departementet må gjøre nødvendige avklaringer om sentrale roller og ansvarsområder på informasjonssikkerhetsområdet.[72] Departementet må også sørge for at den overordnede organiseringen og virkemiddelbruken på området er ressurseffektiv.[73] Veilederen til samfunnsikkerhetsinstruksen *anbefaler* at departementet også vurderer hensiktsmessige virkemidler overfor aktører i sektoren der departementet mangler direkte styringslinjer.[74]
- **Det er krav om risikobasert styring av informasjonssikkerhetsområdet.** Departementet skal utarbeide mål for samfunnssikkerhetsarbeidet i sektoren (inkludert IT-sikkerhetsarbeidet), utarbeide og vedlikeholde systematiske risiko- og sårbarhetsanalyser, ta stilling til sikkerhetsnivået i egen sektor samt iverksette nødvendige kompenserende tiltak.[75] Departementet skal også sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater. Hvor ofte og i hvilken utstrekning et område som informasjonssikkerhet bør evalueres, må bestemmes ut fra faktorer som risiko og vesentlighet, samt kvalitet og omfang av øvrig rapportering.[76]

Departementets ansvar for forebyggende sikkerhetsarbeid innebærer blant annet å identifisere og holde oversikt over grunnleggende nasjonale funksjoner (GNF)[77] innenfor sitt ansvarsområde samt over virksomheter som har vesentlig betydning for slike funksjoner eller for nasjonale sikkerhetsinteresser.[78] Ifølge sikkerhetsloven skal departementet også fatte vedtak om at loven helt eller delvis skal gjelde for virksomheter innenfor sitt ansvarsområde, blant annet dersom disse behandler sikkerhetsgradert informasjon.[79] Ifølge loven skal slike vedtak meldes inn til sikkerhetsmyndigheten.

Kunnskapsdepartementet igangsatte i 2019 et fireårig informasjonssikkerhetsprogram for høyere utdanning og forskning (2019–2022). Av Prop. 1 S (2018–2019) går det fram at programmet skulle

[69] Kommentardelen til samfunnssikkerhetsinstruksen, punkt 2, kapittel IV. Veileder til samfunnsikkerhetsinstruksen, side 5.
[70] Veileder til samfunnssikkerhetsinstruksen side 13–14, Bestemmelser om økonomistyring i staten, kapittel 1.3.
[71] Bestemmelser om økonomistyring i staten, kapittel 1.3.
[72] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen), IV. Krav til departementenes arbeid med samfunnssikkerhet.
[73] I henhold til bestemmelser om økonomistyring i staten, kapittel 1.2, har departementet ansvar for organiseringen av sitt ansvarsområde gjennom opprettelse og avvikling av underliggende virksomheter, og flytting av ansvarsområder mellom underliggende virksomheter. I henhold til reglement for økonomistyring i staten § 4-8 har ansvarlig departement et overordnet ansvar for å sikre at statlige midler brukes effektivt. Bevilgningsreglementet § 10 sier at utgiftsbevilgningene skal disponeres på en slik måte at ressursbruk og virkemidler er effektive i forhold til de forutsatte resultatene.
[74] Veileder til samfunnsikkerhetsinstruksen, side 13.
[75] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen).
[76] Reglement for økonomistyring i staten § 16, bestemmelser om økonomistyring i staten, kapittel 1.6.3.
[77] GNF defineres i § 1-5 i loven som «*tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.*»
[78] Sikkerhetsloven § 2-1.
[79] Sikkerhetsloven § 1-3.

forbedre evnen til å forebygge, oppdage og håndtere trusler mot forskningsnettet, og inkludere tiltak som analyseverktøy og kompetanseheving.[80]

[80] https://www.regjeringen.no/contentassets/70b764ab133b4703929bdd51d0a51fc2/nn-no/pdfs/prp201820190001_kddddpdfs.pdf

4 Inntrengingstest mot tre forskningsinstitusjoner

Inntrengingstestene omtalt i dette kapitlet viser hvordan svakheter kan utnyttes for å få kontroll over IKT-infrastruktur. Vi har gjennomført slike tester ved de tre forskningsinstitusjonene i dybdeundersøkelsen – henholdsvis [redacted]. Testene er basert på metoder og verktøy enkelt tilgjengelig på Internett.

Oppsummering

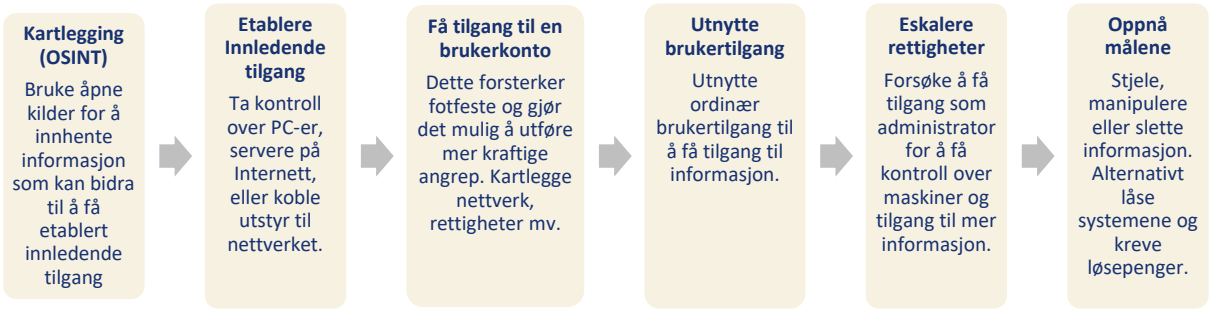
- Under inntrengingstestene fikk vi ved [redacted] tilgang som domeneadministrator, som gir full kontroll over virksomhetenes Windows-baserte IKT-infrastruktur. Med slik tilgang kunne vi tildele oss selv alle ønskede rettigheter og skaffe oss tilgang til all informasjon, inkludert sensitiv forskningsinformasjon, som var lagret i nettverket.
- På den tredje forskningsinstitusjonen ([redacted]) fikk vi kontroll med de fleste klientmaskiner, men ikke servere og de sentrale delene av institusjonens IT-infrastruktur som er bedre beskyttet. Vår tilgang ga muligheter til å hente ut informasjon lagret lokalt på PC-er og på eiernes skylagring. Tilgangen kunne videre vært brukt til målrettede angrep mot forskere med kunnskap og tilgang til sensitiv informasjon, for eksempel ved å endre sikkerhetsinnstillinger på maskinen og/eller legge inn skadevare som fanger opp alt som tastes på maskinen eller all lyd rundt maskinen.
- Det er stor variasjon i hvor aktivt de tre virksomhetene i dybdeundersøkelsen arbeider med overvåking, innsamling og analyser av logger. Få eller ingen av aktivitetene i inntrengingstestene ble oppdaget på to av de tre forskningsinstitusjonene. [redacted] oppdaget inntrengingstesten den fjerde testdagen, og de fleste aktivitetene i angrepene ga spor i logger som virksomheten samlet inn. Gjennom analyse av disse loggene hadde [redacted] mulighet for å danne et bilde av hvordan angrepet utartet seg og hvilke systemer som var berørt av angrepet.

4.1 Funn fra gjennomføringen av inntrengingstest mot de tre forskningsinstitusjonene i dybdeundersøkelsen

Formålet med å simulere dataangrep er å identifisere potensielle svakheter i sikkerhetstiltak og vise hvordan disse kan utnyttes av en angriper. [redacted] Målet har vært å få kontroll over virksomhetens IKT-infrastruktur og tilgang til sensitive forskningsdata.

Figur 2 gir en oversikt over og beskrivelse av fasene i revisjonens simulerte angrep mot de tre forskningsinstitusjonene i dybdeundersøkelsen. I kapittel 4.2.1 - 4.2.6 beskrives resultatene fra de enkelte fasene.

Figur 2 Faser i et dataangrep



4.1.1 Kartlegging fra åpne kilder (OSINT[81])

Informasjon om forskningsinstitusjonenes IT-miljø ble hentet inn fra Internett som et grunnlag for inntrengingstesten. Nettsidene til virksomhetene i dybdeundersøkelsen gir informasjon om for eksempel ansatte i IT-avdelingen, hvilke systemer som er bruk, krav til passord mv. [redacted].[82]

Vi gjennomførte en passordspray [redacted]
Passordspray innebærer at vi forsøkte å logge inn med det samme passordet på alle brukerkontoene vi hadde funnet. [redacted]

[redacted].[84]

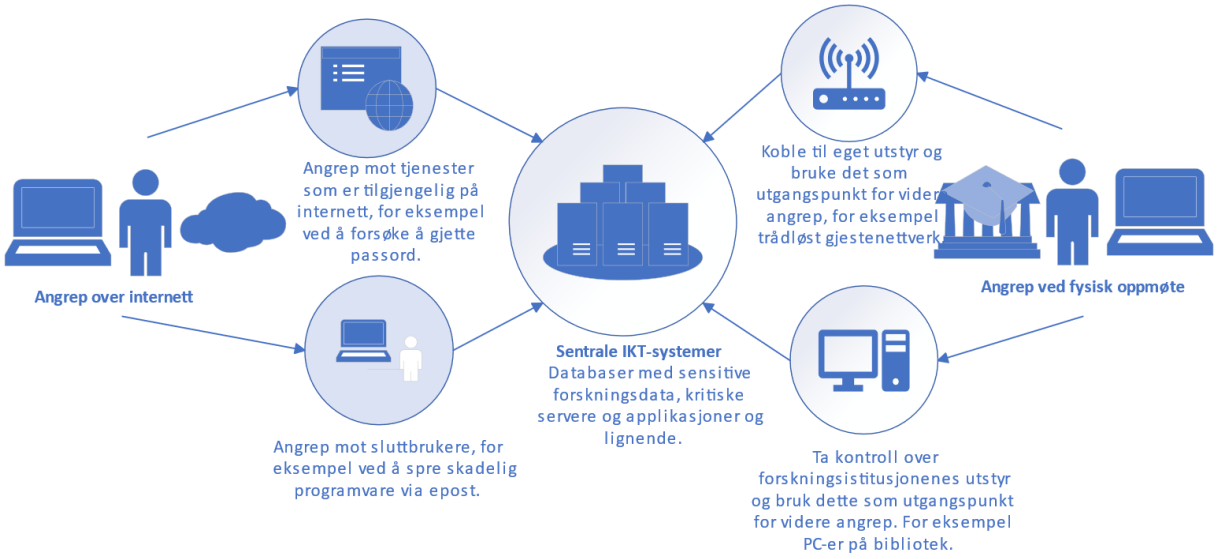
4.1.2 Etablere innledende tilgang

Mange dataangrep starter med at angripere forsøker å etablere et innledende fotfeste i virksomhetens IKT-systemer. Målet er ikke å ta full kontroll over IKT-systemene i første omgang, men å sette seg i en posisjon hvor kartlegging og videre angrep er mulig. En angriper kan forsøke å etablere innledende fotfeste på flere ulike måter, for eksempel:

- utnytte teknologiske sårbarheter i servere som er tilgjengelig på internett, f. eks servere for virksomhetens nettsider
- lure ansatte til å kjøre skadelig programvare som gir angriperen kontroll over deres PC-er
- manipulere ansatte til å gi fra seg brukernavn og passord, og deretter logge på virksomhetens systemer med disse
- koble til utstyr i trådløse nettverk eller fysiske nettverkskontakter i ubeskyttede områder
- utnytte offentlig tilgjengelige PC-er som ikke krever pålogging

[81] Open source intelligence
[82] [redacted]
[83] [redacted]
[84] [redacted]

Figur 3 Ulike metoder for å etablere innledende tilgang



[redacted]

4.1.3 Få tilgang til en brukerkonto

I forbindelse med etablering av innledende fotfeste og kartlegging av IKT-miljøet er det vanlig at angripere forsøker å få tilgang til en brukerkonto. I første omgang er det tilstrekkelig med en hvilken som helst brukerkonto - selv helt ordinære kontoer som studentkonter eller gjesteforskere har tilgang til informasjon og funksjonalitet som angripere kan utnytte for å kartlegge domenet. For eksempel har en ordinær konto i de fleste IKT-miljøer tilgang til felles filområder og informasjon om øvrige kontoer og deres tilgangsrettigheter.

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Faktaboks 2 Kryptering og hashing av passord

Kryptering er en to-veis funksjon der et passord blir omformet til en ugjenkjennelig kode som kan reverseres dersom man har en nøkkel. Hashing derimot, er en en-veis funksjon, ofte brukt til autentisering, hvor det hashede passordet ikke kan konverteres tilbake til klartekst. Det er vanlig at systemer lagrer og kommuniserer passord som hashede verdier.

Når du logger inn på et nettsted skapes hashen på nytt fra passordet du har skrevet inn. Denne hashen blir deretter sammenlignet med den som ligger i databasen. Dersom den er identisk, vet systemet at du har skrevet inn riktig passord og du er dermed autentisert.

Knekking av passordhasher benytter samme fremgangsmetode som for å sjekke om et passord er gyldig. Man kan enten prøve alle mulige tall- og bokstavkombinasjoner til vi finner et passord som produserer korrekt hash. Dette kalles *brute force*. Eller man kan benytte ordlister for å generere hasher fra ordbøker eller for eksempel passord som er lekket på internett. Dette kalles *dictionary attack*. Dersom angriperen har fått lastet ned passordhasher, kan programvare for å knekke passord teste millioner av mulige passord på kort tid.[86]

[redacted]

[85] [redacted]

[86] Hvor mange passord som kan testes per sekund avhenger av type passordhash og angriperens maskinvare. Det er mulig å teste flere milliarder potensielle passord per sekund ved enkle typer passordhasher. Dersom det er mer kompliserte typer passordhasher kan det testes noen tusen passord per sekund.

[87] [redacted]

[88] [redacted]

[redacted]

Passordhasher ble hentet ut fra institusjonenes nettverk ved bruk av verktøyene nevnt over[89], og relativt enkle passord resulterte i at vi fikk knekt en rekke passordhasher og fikk tilgang til brukernavn og passord. Omfattende informasjon om brukeres rettigheter, gruppetilhørighet mv. ble hentet ut fra Active Directory ved alle tre institusjonene ved bruk av verktøy lastet ned fra internett.[90]

[redacted]

4.1.4 Utnytte brukertilgang

Med kontroll over ansattes og studenters brukerkontoer ønsket vi å utnytte disse til å kartlegge virksomhetenes IT-infrastruktur for å finne svakheter og få mer kontroll over maskiner i infrastrukturen. Tilgang til brukerkontoer ble brukt til å:

- Hente ut oversikt over alle brukerkontoer og deres rettigheter, brukergrupper og maskiner i forskningsinstitusjonenes IT-nettverk.[94]
- Skanne alle maskiner tilknyttet virksomhetens nettverk som vi nådde for å se muligheter for å koble seg til maskiner og om maskinene hadde åpenbare svakheter.[95]

Ved [redacted] gjorde skjerming av mange servere i nettverket at vi ikke fikk skannet en stor andel av serverne som virksomheten anvender. Ved de to andre virksomhetene fikk vi skannet større deler av IT-infrastrukturen.

Gjennomgang av resultatene fra skanningen av nettverkene gjorde også at vi identifiserte en del informasjon som var tilgjengelig for alle brukere eller store grupper av brukere og som kan utnyttes av en angriper. Vi fant blant annet:

- server med forskningsdata som var lagret av en rekke studenter
- personlige brukermapper for ansatte som var konfigurert feil slik at alle brukere ved virksomheten hadde tilgang til informasjon lagret her
- en server med sikkerhetskopi av et stort volum av data fra et virtuelt miljø og en server som var tilgjengelig for alle i nettverket
- informasjon om mange IT-systemer, hvordan disse konfigureres og driftes

[redacted]

89 [redacted]
90 [redacted]
91 [redacted]
92 [redacted]
93 [redacted]
94 [redacted]
95 [redacted]

[redacted]

4.1.5 Eskalere rettigheter

Hensikten med å eskalere rettigheter er å forsøke å få tilgang som administrator for å få kontroll over maskiner og tilgang til mer informasjon. Angripere utnytter svakheter i oppsett, konfigurasjon eller programvare til systemene.

For å få tilgang til brukerkontoer med høyere rettigheter prøvde vi ut fra den kartlagte IT-infrastrukturen å finne svakheter som ga oss bedre kontroll og flere tilganger. I første omfang søkte vi etter muligheter for å kontrollere enkelte maskiner ved å finne passord til en administrator). I neste omgang forsøkte vi å utvide dette ved å hente ned og knekke passord til brukerkontoer som ga kontroll over flere maskiner. Vi forsøkte også å finne svakheter i tilgangsstyring som kunne gi mer omfattende rettigheter og utnytte svakheter i konfigurasjon. Målet var til slutt å få full kontroll over hele IT-infrastrukturen.[96]

Svakhetene ved de ulike virksomhetene var litt forskjellige, slik at veien videre for mer kontroll også varierte:

- Ved [redacted] vi full kontroll over alle maskiner i virksomhetens nettverk ved å utnytte svakheter i tilgangsstyring. Alle ansatte og studenter kunne her melde seg selv inn i en gruppe som ga tilgang til lokalt administratorpassord for alle Windows-maskiner. Med slik tilgang på servere kunne vi deretter hente ut passordhasher og vi klarte å knekke et passord til en brukerkonto som hadde full kontroll på virksomhetens Windows-nettverk.
- Ved [redacted] ble det funnet tre ulike veier som ga full kontroll over hele IT-infrastrukturen:
  - Den enkleste veien var å få kontroll over en brukerkonto [redacted] som var gitt rettigheter som ga full kontroll over nettverket og hadde et svakt passord. [redacted]
  - En annen vei var å utnytte en sikkerhetskopi av en server som alle brukere i nettverket hadde tilgang til (jf. punkt 4.1.4). [redacted]
  - En tredje vei var å utnytte en brukerkonto vi hadde funnet passordhashen til [redacted] Passordet var relativt enkelt å knekke og kontoen hadde rettigheter som ga full kontroll over en server. [redacted]
- Ved [redacted] oppnådde vi ikke full kontroll over hele IT-infrastrukturen fordi viktige servere og brukerkontoer var bedre beskyttet. Vi fikk imidlertid full kontroll over de fleste PC-ene ved virksomheten. [redacted]

96 [redacted]
97 [redacted]
98 [redacted]

Alle de konkrete svakhetene som ble funnet og utnyttet for å få kontroll med maskiner og IT-infrastruktur ble raskt formidlet til virksomheten. IT-avdelingene foretok raskt tiltak som utbedret konkrete svakheter som ble identifisert.

4.1.6 Oppnå målene

Vi lyktes i å få kontroll over nettverkene til to av de tre forskningsinstitusjonene [redacted] og med dette tilgang til forskningsdata som lagres her. Med slik kontroll hadde det også vært mulig å utplassere løsepengevirus eller annen skadevare dersom motivasjonen hadde vært finansiell eller sabotasje. Med slik tilgang kunne vi tildele oss selv alle ønskede rettigheter og skaffe oss tilgang til all informasjon, inkludert sensitiv forskningsinformasjon, som var lagret i nettverket. Ved å benytte de anskaffede brukernavnene og passordene til både administratorer og forskere ved [redacted] klarte vi å logge oss inn på blant annet maskiner og skytjenester som tilhørte forskere.

Ved [redacted] ble det gjort forsøk på å få kontroll med sentrale servere og virksomhetens domene i løpet av inntrengingstestingen uten at dette lyktes. Enkelte av passordhashene vi innhentet kunne gitt oss mer kontroll, men vi klarte ikke å knekke dem i løpet av perioden.

Videre oppnådde vi å få tilgang som lokal administrator [redacted], som blant annet tilhørte forskere. Dette ga mulighet til å se og hente ut alle data som lå lagret lokalt på maskinen og på eierens skylagring, [redacted]. I tillegg til noe forskningsdata, inkludert strategisk informasjon om forskningsaktiviteter og organisering av forskningsenheter, fant vi også en del personlig informasjon fra brukere. Med lokal tilgang har man adgang til å lese og endre all informasjon som den enkelte forsker har. Det vil si at lokal tilgang er en mer inkrementell fremgangsmåte enn domeneadministrator ved at man tar over forskernes tilgang maskin for maskin heller enn hele infrastrukturen på en gang.

Ved å skanne nettverket for tilgjengelige tjenester og systemer, oppdaget vi forskningsdata som omhandlet problemstillinger knyttet til rus og vold, og inkluderte personopplysninger, som var lagret med tilgang for alle [redacted]. Ved [redacted] fikk vi med samme metode tilgang på lønns- og personaldata som lå åpne. Tilsvarende sensitiv informasjon som lå åpent for alle ansatte/studenter, fant vi ikke ved [redacted]

Alle de tre virksomhetene benytter forskningsplattformer som er utviklet spesielt for håndtering av sensitive forskningsdata, for eksempel TSD (jf. punkt 6.2.1). Målrettede angrep på sikre forskningsplattformer kunne ha vært et mulig mål for revisjonen, men ble ikke testet grunnet begrenset tid. Men med bakgrunn i informasjonen vi fant på PC-er med lokal administratortilgang, kunne sosial manipulasjon mot utvalgte forskere for å få tilgang til disse tjenestene ha lyktes. Selv tjenester som er beskyttet med to-faktor autentisering kan være sårbare mot vellykkede angrep ved at angriperne lurer ansatte til å godta to-faktor forespørselen.

4.2 Forskningsinstitusjonenes evne til å oppdage angrep

Det er stor variasjon i hvor aktivt de tre undersøkte virksomhetene arbeider med overvåking, innsamling og analyser av logger. Få eller ingen av aktivitetene ble oppdaget ved to av de tre virksomhetene [redacted] oppdaget angrepet den fjerde dagen av inntrengingstesten.

[redacted]

[redacted]

[redacted]

[redacted]

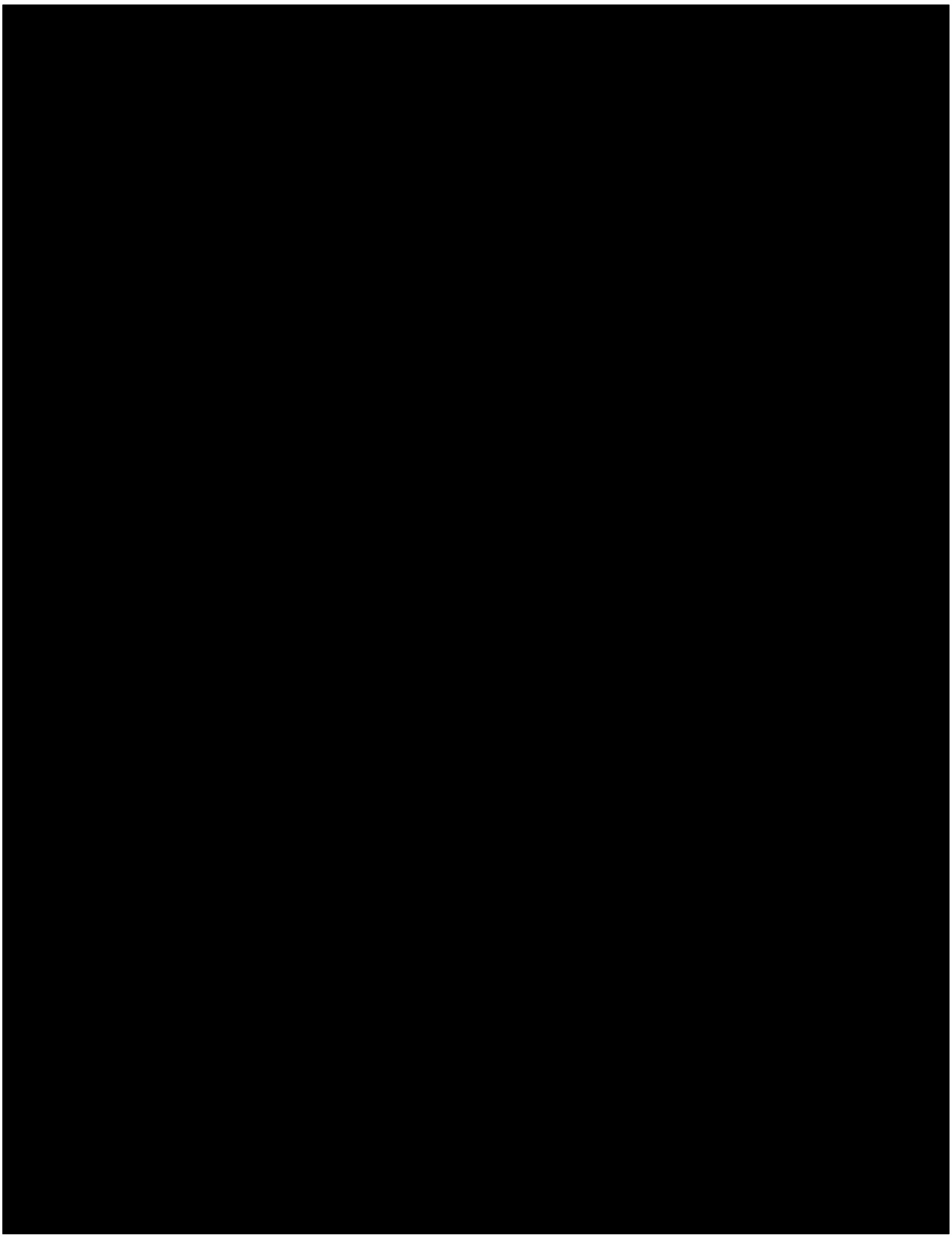
[redacted]

99 [redacted]

4.3 Hvorfor angrepene lyktes

Svakheter i informasjonssikkerhetskontrollene som vi **utnyttet** i inntrengingstesten kan grovt grupperes i 5 kategorier. Tabellen under viser i hvilke institusjoner forskjellige angrepsteknikker lyktes.

Tabell 1 Feil eller mangler i sikkerhetsarbeidet som resulterer i vellykkede dataangrep.



Tabellen viser at det er nær sammenheng mellom en virksomhets sikkerhetsarbeid og risiko for at datainnbrudd lykkes. I organisasjoner hvor man arbeider systematisk med innføring av tekniske kontroller har man større muligheter for å avverge og minimere omfang av angrep. I kapittel 5 beskrives forskningsinstitusjoners implementerte sikkerhetstiltak.

De tre virksomhetene ble informert om alle svakheter vi fant gjennom inntrengingstestene umiddelbart etter at disse var gjennomført. Virksomhetene gjennomførte raskt tiltak for å lukke de konkrete sårbarhetene som ble utnyttet for å få tilgang i testene. I etterkant har virksomhetene planlagt og til dels gjennomført en rekke tiltak for å forbedre tekniske sikkerhetstiltak og redusere risiko for at nye sårbarheter oppstår, jf. punkt 5.6.4.

5 Virksomhetenes tekniske sikkerhetstiltak for å beskytte forskningsdata

I dette kapitlet beskriver vi i hvilken grad de undersøkte forskningsvirksomhetene følger anbefalinger for tekniske sikkerhetstiltak som er viktig for å forebygge at dataangrep lyktes, og oppdage de angrep man ikke klarer å forebygge. I tillegg til de tre virksomhetene hvor vi gjennomførte inntrengingstester, inkluderer dette kapitlet også fakta om syv andre forskningsvirksomheter.

Relevante revisjonskriterier

For å hindre at angrep lykkes, må virksomheter iverksette en rekke sikkerhetstiltak som sammen kan redusere risiko. God praksis[100] når det gjelder sikkerhetstiltak, innebærer bl.a. at virksomhetene har

1. en tilgangsstyring som gir kontroll med brukerkontoer, herunder administrator- og servicekontoer, og tilgangsrettigheter.
2. sikker autentisering av brukere ved bruk av passord og en annen faktor ved pålogging til virksomhetens nettverk og tjenester.
3. kontinuerlig sårbarhetsstyring gjennom oppdatering av programvare, skanning av nettverk for å avdekke sårbarheter og sikker konfigurasjon (herding) av maskiner og programvare.
4. en inndeling av virksomhetens IKT-nettverk i soner ut fra hvor sensitive systemene og dataene er for virksomheten, begrenser datatrafikk mellom disse sonene og har kontroll over utstyr som koble seg til nettverket.
5. logging og overvåking - Innsamling, forvaltning og analyse av data fra nettverk og enheter.

Vi tar for oss status på hver av disse områdene i kapittel 5.1 til 5.5. Hva som er definert som «god praksis» for hvert av områdene er utdypet i tekstbokser i innledningen til de ulike punktene.

Oppsummering

- Nivået på sikkerhetstiltakene i forskningsvirksomhetene varierer betydelig. Sentrale anbefalinger i NSMs Grunnprinsipper for IKT-sikkerhet følges ikke av mange virksomheter. Dette kan føre til at forskningsdata blir manipulert eller sensitive data blir eksponert.
- Flere av virksomhetene har mange brukerkontoer med høye rettigheter og benytter ikke ulike brukerkontoer for ulike driftsoperasjoner som anbefalt. Dette gjør det lettere for en angriper å eskalere rettigheter og få kontroll med all IKT-infrastrukturen når et fotfeste er etablert.
- Krav til passord varierer, og det er ofte ikke satt høyere krav til passord for kontoer som har høye rettigheter. Det er bra at tofaktor-autentisering er innført mange steder, [redacted]
- De fleste virksomhetene har på plass rutiner for sikkerhetsoppdatering av programvare for å fjerne kjente sårbarheter, [redacted]

[100] Nasjonal sikkerhetsmyndighets (NSM) Grunnprinsipper for IKT-sikkerhet v. 2.0 og anbefalinger for grunnleggende IKT-sikkerhet utarbeidet av The Center for Internet Security («CIS Controls»)

- Universitetene og høyskolene i undersøkelsen er åpne virksomheter, samtidig som det er svakheter i sikkerhetstiltak for å beskytte egne nettverk.
- [redacted]
- [redacted]
- [redacted]

5.1 Tilgangsstyring

Tilgangsstyring handler om å ha kontroll og oversikt over brukere som gis tilgang til IT-systemer og informasjonen som er lagret her. Vi ser mest på tilganger som administrator siden disse har høye privilegier og kan kontrollere IT-systemene.

Faktaboks 3 God praksis for tilgangsstyring

Som god praksis for kontroll med brukerkontoer og tilgangsrettigheter har vi lagt til grunn følgende anbefalinger:

- Tildeling og bruk av utvidede rettigheter bør minimeres til kun det som er nødvendig for å gjennomføre oppgavene, både for kontoer som benyttes av administratorer/sluttbrukere og servicekontoer.[101]
- Bruk av rollen domeneadministrator, som gir svært omfattende rettigheter, bør særskilt begrenses til et minimum.[102]
- Det bør etableres ulike kontoer til ulike driftsoperasjoner, selv om det kanskje er samme person som reelt sett utfører oppgavene.[103]
- Administrator-rettigheter bør ikke tildeles sluttbrukere.[104]
- Brukerkontoer bør deaktiveres når behovet for kontoen faller bort, og kontoer som ikke har blitt brukt på lenge bør detekteres og følges opp.[105]

Kilde: NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0, punkt 2.6.

5.1.1 Flere virksomheter har mange brukerkontoer med høye rettigheter

Personer som arbeider med drift og utvikling av IKT-systemer må ha flere rettigheter enn vanlige brukere i IKT-systemer for å utføre oppgaver som for eksempel installering av programvare, konfigurering av systemer eller for å rette feil ved automatiske jobber som kjører på en server. De tildeles derfor utvidede tilgangsrettigheter. Slike kontoer er attraktive mål for en angriper fordi det gir kontroll over IT-systemer og/eller IT-infrastruktur.

[101] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.1 b).
[102] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.5 b).
[103] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, tiltak 2.6.5 a).
[104] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, tiltak 2.6.4 a).
[105] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.3 d).

Domeneadministrator er rettigheten som vi i kapittel 4 har lagt til grunn gir full kontroll over Windows-nettverk og maskinene i dette (jf. punkt 4.1.). Mange kontoer med rettigheter som domeneadministrator og mye bruk av disse gjør det lettere for en angriper å få kontroll over en virksomhets IKT-infrastruktur. [redacted]

Tabell 2 Antall domeneadministratorer og egne kontoer for ulike driftsoperasjoner

[redacted]

Kilde: Analyse av uttrekk av Active Directory mottatt fra virksomhetene. Tabellen viser status på det tidspunkt virksomheten ble revidert

[redacted]

106 [redacted]
107

[redacted]

Faktaboks 4 Administrasjon av brukere og rettigheter i Active Directory og Entra ID

Active Directory (AD) er en katalogtjeneste fra Microsoft hvor det blant annet defineres brukerkontoer, grupper, maskiner og tilgangsrettigheter. AD benyttes i nesten alle virksomheter som har et antall Windows-maskiner, inkludert alle i denne undersøkelsen.

Brukeres tilgangsrettigheter defineres ofte i AD ved medlemskap i ulike grupper som gir rettigheter til maskiner, programmer etc. Det er flere standard grupper som domeneadministratorer for kontroll med alt i domenet, Account operators for brukeradministrasjon og backup operators for sikkerhetskopiering.

Active Directory må driftes av den enkelte virksomhet. **Microsoft Entra ID**, kjent som Azure Active Directory på undersøkelsestidspunktet, er en skyløsning med tilsvarende funksjonalitet. Alle virksomheter i denne undersøkelsen har hybridløsninger der både lokal AD og skybaserte Entra ID benyttes.

I Entra ID er det en rekke predefinerte roller som gir rettigheter til å administrere tjenester, maskiner, brukerkontoer etc. Global Administrator er den høyeste rettigheten med full kontroll over ressursene knyttet til Entra ID.

Antallet kontoer med rettighet som domeneadministrator kan ses i sammenheng med om det er innført **egne brukerkontoer for ulike driftsoperasjoner**. Målet med å bruke egne kontoer for ulike operasjoner er å minimere konsekvensen dersom en konto eller maskin blir kompromittert. Jo mer inndelt rettighetene er, jo mindre blir konsekvensene dersom en konto blir kompromittert. Men høy inndeling krever også mer av virksomhetens administratorer, som må bytte mellom ulike brukerkontoer når det gjennomføres ulike arbeidsoppgaver. Vi har sett på om det er egne kontoer for drift av:

- alle objekter i et Windows-nettverk basert på Active Directory (domene) (jf. beskrivelse i faktaboks 4)
- de enkelte serverne i nettverket
- klientmaskinene som anvendes av brukerne i nettverket

[redacted]

[redacted]

[redacted] har gjennomført tiltak for å redusere risiko knyttet til at det ikke er innført egne brukerkontoer for ulike driftsoperasjoner. Her settes maskiner opp slik at passordhasher (jf. faktaboks 3) ikke lagres på servere og kun kryptert passord for den siste brukeren lagres på klienter. Dette hindrer en angriper fra å hoppe fra maskin til maskin for å samle inn mange krypterte passord, som et grunnlag for å oppnå høyere rettigheter (jf. kap. 4.1.5).

[redacted] bruker hybride modeller hvor katalogtjenesten for tilgangsstyring både ligger i skyen (**Microsoft Entra ID)** og lokalt i Active Directory (AD). Rollen Global Administrator i Entra ID tilsvarer domeneadministrator i AD og vil gi full kontroll over dette systemmiljøet. Dersom mange kontoer er tildelt denne rollen, vil det være lettere for en angriper å oppnå rettigheten. [redacted]

Dersom brukerkontoer for administratorer brukes på tvers av Entra ID og AD vil det innebære at en angriper som får kontroll over (ressurser på) en plattform, også vil kunne få kontroll på den andre. Analyse av uttrekk viser at alle virksomhetene i undersøkelsen som utgangspunkt har etablert separate brukerkontoer for administrasjon av AD og Entra ID. [redacted]

Funksjonaliteten «Privileged Identity Management» i Entra ID gir muligheter for bedre kontroll med rettigheter som administrator. Funksjonaliteten gir mulighet for at rettighetene kun tildeles for et begrenset tidsrom, og for at tildelingen av rettighetene må godkjennes av definerte brukere. Noen av virksomhetene, som Universitetene i Bergen og Tromsø, hadde tatt i bruk funksjonaliteten og noen andre vurderte dette på undersøkelsestidspunktet.

5.1.2 Servicekontoer gis ofte høyere tilgangsrettigheter enn nødvendig

I likhet med menneskelige brukere trenger programmer og tjenester som kjører i IKT-systemer en identitet og tilgangsrettigheter for å utføre sine oppgaver – til dette formålet opprettes servicekontoer. Slike kontoer har mye til felles med vanlige brukerkontoer, for eksempel at det er mulig for en person å logge inn på kontoen hvis vedkommende kjenner passordet. Servicekontoer kan ha store tilgangsrettigheter og de må derfor beskyttes mot misbruk på lik linje med andre viktige brukerkontoer (administratorkontoer, jf. punkt 5.2.1).

Analyse av uttrekk viser at servicekontoer i mange tilfeller gis mye rettigheter. [redacted]

- [redacted]
- [redacted]

[redacted]

Servicekontoer tildeles ofte høye rettigheter fordi man ikke vet nøyaktig hvilke rettigheter som er nødvendige for at et program skal fungere, og det er da enklere å gi høye rettigheter. At man ikke vet nøyaktig hvilke rettigheter som er nødvendig kan skyldes at programmet er satt opp langt tilbake i tid uten god dokumentasjon, at det er satt opp av konsulenter uten nødvendig kunnskapsoverføring eller at dokumentasjonen fra leverandør er uklar.

[redacted]

En metode som kan gi sikrere bruk av servicekontoer i et Windows-miljø er bruk av «Group Managed Service Accounts» (gMSA). Ved bruk av gMSA blir passord håndtert automatisk av Microsoft Windows, slik at ingen av de ansatte som drifter IT-systemene behøver å kjenne passordene.
[redacted]

5.1.3 En del ordinære brukerkontoer har rettigheter som lokale administratorer

Alle brukere av IT-systemer trenger en brukerkonto for å kunne logge på maskinen, nettverket eller en tjeneste. Brukere som ikke skal administrere disse maskinene eller tjenestene kalles ofte sluttbrukere, og har en «ordinær» brukerkonto som brukes til alle gjøremål. Også IT-ansatte har en ordinær brukerkonto, da arbeidsoppgaver som krever spesielle rettigheter kun bør gjennomføres med egne administratorkontoer (jf. forrige punkt).

Lokal administrator har full kontroll over en enkelt maskin (server eller klient) og rettigheten gir for eksempel mulighet til å installere programvare eller endre konfigurasjon av denne maskinen. Dersom sluttbrukere gis denne rettigheten, kan for eksempel sluttbrukeren bli lurt til å laste ned skadevare eller installere programvare som ikke er godkjent i virksomheten og dermed heller ikke blir oppdatert i tråd med rutinene (jf. punkt 5.3.1).

[redacted]

[redacted]

Som grunnlag for forskning ønskes ofte spesiell programvare, og med stor bredde i fag kan det være mye ulik programvare som ønskes. Også laboratorieutstyr kan kreve egen programvare og eget IT-utstyr. Det har derfor vært tradisjon i sektoren at noen fakultet, institutt eller forskergrupper drifter eget utstyr eller har administrative rettigheter på servere eller klienter, jf. punkt 6.5. Analyse av innhentede data viser at omfanget av slike løsninger er mindre enn tidligere, og ingen av virksomhetene i undersøkelsen gir sluttbrukere administrative rettigheter på eget utstyr som standard.

[110] Opplyst i møte mellom Riksrevisjonen og [redacted]

Noen av virksomhetene[111] har valgt å løse presset for å få administrative rettigheter ved å etablere løsninger der sluttbrukere kan bli tildelt rettighet som lokal administrator for en kortere periode. Sluttbrukeren kan da i denne perioden installere den programvaren som er ønsket eller utføre andre oppgaver som krever administrative rettigheter. For å få tildelt administrative rettigheter for en periode må sluttbrukeren som regel oppgi årsaken til at dette ønskes, og i noen løsninger kreves en forhåndsgodkjennelse fra ansatte i IT-avdelingen. Slike løsninger reduserer risiko for alvorlige konsekvenser når en bruker trykker på en lenke til skadevare på en webside eller i en e-post, siden rettigheten kun innehas en kort periode. Løsningene reduserer imidlertid i liten grad risiko for at programvare som installeres av sluttbrukere ikke oppdateres regelmessig (jf. punkt 5.4.1). De reduserer også i liten grad risiko for at brukeren som en villet handling installerer programvare eller utfører handlinger som ikke er godkjent.

5.1.4 Brukerkontoer for ansatte og studenter deaktiveres ofte når behov opphører, men dette gjelder i mindre grad andre brukerkontoer

Manglende kontroll på brukerkontoer som det ikke lenger er behov for er et vedvarende problem, og NSM har pekt på at det er mange eksempler på at ubrukte kontoer til leverandører og tidligere ansatte har blitt misbrukt av en angriper eller utro tjener. [112] Selv ubrukte kontoer med svært begrensede rettigheter kan være nyttige for en angriper.

For **ansatte og studenter** har mange av virksomhetene etablert systemer hvor brukerkontoer styres ut fra meldinger fra lønnssystem og sektorens Felles studentsystem (FS). Denne automatiseringen reduserer risiko for at brukerkontoer opprettes på manglende grunnlag eller ikke blir deaktivert når noen forlater en stilling eller et studiested. Også i nytt felles system for Identitets- og tilgangsstyring (IAM) i sektoren, som er under innføring, legges disse koblingene til grunn.[113] Et av hovedmålene med systemet er å redusere usikkerhet rundt data til grunn for å gi, endre og fjerne tilganger ved at personer registreres likt ved de ulike institusjonene.

Analyse av uttrekk indikerer at virksomhetene har mer utfordringer med å håndtere **«tilknyttede» personer**. Dette kan være gjesteforskere, gjesteforelesere, timelærere, IT-konsulenter, stipendiater og andre med en «løsere» tilknytning til virksomheten som har fått tildelt en brukerkonto. [redacted] har for eksempel pekt på utfordringen med å styre tilganger til gjesteforelesere som kun er aktive periodisk, kanskje bare en gang i året.[114] I en åpen sektor er det en del brukerkontoer innen denne kategorien. [redacted]

Utfordringen ble også sett i forbindelse med innføring av nytt felles identitets- og tilgangsstyringssystem i sektoren.[115] Sikt har observert at tilknyttede personer kan ha relativ lemfeldig håndtering, spesielt når det er noen som «må» inn raskt.[116] [redacted] Prosjektet for innføring av det nye fellessystemet har gjennom krav til korrekte og nøyaktige grunndata avdekket en betydelig mengde med duplikater og mangelfulle identiteter fordi prosessene i den initiale registreringen har vært varierende og til tider mangelfulle. Sikt presiserer at dette ikke er en systemutfordring, men en prosedyreproblematikk.

Siden automatikken ved håndteringen av brukerkontoer for studenter og ansatte reduserer risiko, har flere av virksomhetene ikke etablert **rutiner for periodisk gjennomgang** av brukerkontoer og

[111] Løsningene omtalt i dette avsnittet er hentet fra [redacted]
[112] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.
[113] Sikts tilsvar av 7. juni 2023.til spørsmål om IAM, reist av Riksrevisjonen i brev av 6. juni 2023,
[114] Møte mellom [redacted] og Riksrevisjonen om tekniske sikkerhetstiltak 13. april 2023.
[115] Sektoren er i regi av Sikt i ferd med å innføre et felles system for identitetshåndtering som grunnlag for tilgangsstyring, jf. https://sikt.no/tjenester/felles-iam
[116] Sikts tilsvar av 7. juni 2023.til spørsmål om IAM, reist av Riksrevisjonen i brev av 6. juni 2023,

tilganger.[117] Automatikken vil imidlertid ikke gjelde alle brukerkontoer, for eksempel ikke «tilknyttede» personer som omtalt i forrige avsnitt, administrator-kontoer eller servicekontoer som programmer benytter for å logge seg på IKT-systemer. [redacted] har opplyst at de har eller er i ferd med å innføre forbedringer etter at internrevisjoner hadde pekt på utfordringer. Også [redacted] var på undersøkelsestidspunktet i ferd med å forbedre rutiner for bedre kontroll med brukerkontoer og tilganger.

[redacted]

5.2 Brukerautentisering

Autentisering er prosessen for å bekrefte en påstått identitet. Bruker må i en tradisjonell autentisering oppgi et passord for å bekrefte sin identitet og får deretter tilgang til et system.

Faktaboks 5 God praksis for sikker autentisering av brukere

Som god praksis for sikker autentisering av brukere ved pålogging til en virksomhets systemer har vi lagt til grunn følgende anbefalinger:

- Bruk et sentralt verktøy til å kontrollere passord-kvaliteten opp mot virksomhetens sikkerhetskrav, som et minimum bør man hindre bruk av vanlige ord og navn på norsk og engelsk, samt årstall og årstider.[118]
- Tofaktor-autentisering med bruk av for eksempel smartkort, sertifikater eller engangspassord bør benyttes for å autentisere brukere, som et minimum for brukerkontoer som har tilgang til kritiske data eller systemer, samt brukere med driftsoppgaver. [119]
- Der tofaktor-autentisering ikke støttes bør brukerkontoer bli pålagt å bruke sterke passord på systemet.[120]

Kilde: NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0, punkt 2.6.

5.2.1 Krav til passord varierer, men er ofte svakere enn anbefalt

Passord er den tradisjonelle metoden for å bekrefte identitet når noen skal ha tilgang til et system. Dersom det velges svake passord, kan en angriper gjette passordet eller knekke en passordhash (enveiskryptering av passordet som formidles mellom systemer i et IKT-nettverk, jf. faktaboks 4.). I inntrengingstestene våre utnyttet vi svake krav til passord (jf. punkt 4.1.5).

[117] Mottatt informasjon viser at [redacted] ikke hadde slike rutiner. [redacted] hadde ikke rutiner på undersøkelsestidspunktet, men var i prosess for å innføre slike rutiner.
[118] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.3.
[119] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.7.
[120] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.7 a), jf. NSMs råd og anbefalinger om passord https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord.

Passordets lengde er den viktigste faktoren som bestemmer styrken.[121] Anbefalinger om passordlengde i bransjen varierer, men 12-14 tegn anses som et minimum.[122] Kravene til passord i virksomhetene i undersøkelsen framgår av tabell 3.

Tabell 3 Krav til passord for ordinære brukere

Kilde: Analyse av uttrekk av data og informasjon mottatt fra de enkelte virksomheter. Tabellen gjengir kravet på undersøkelsestidspunktet.

Tabell 3 viser at kravene til passord i virksomhetene varierer. I sektorens nye felles system for Identitets- og tilgangsstyring, som er i ferd med å innføres, legges det til grunn et poengsystem for å bestemme krav til lengde for passord. Her settes krav til 12 tegn dersom flere ulike typer tegn benyttes, mens det må velges et lengre passord dersom færre ulike typer tegn velges.

[121] Jf. NIST Special Publication 800-63B, appendix A: «Password length has been found to be a primary factor in characterizing password strength» (https://pages.nist.gov/800-63-3/sp800-63b.html

[122] Nettvett.no det anbefaler å benytte en frase som er så lang som mulig, minst fem ord eller 16 tegn (https://nettvett.no/passord/). NSM viser til anbefalingene om passord gitt av nettvett.no (https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord). Leverandøren Microsoft legger til grunn at passord bør være minst 12 tegn langt, men at 14 eller mer er langt bedre (https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb)

[123]

[124]

[125]

[redacted] Både [redacted] har satt krav til lengre passord i etterkant av inntrengingstesten.

Servicekontoer[126] og brukerkontoer med administrative rettigheter benyttet av driftspersonell er attraktive mål for angripere fordi disse kontoene ofte har mer rettigheter enn ordinære brukere. Det kan settes egne passordpolicyer med høyere krav for disse gruppene for å sikre disse kontoene spesielt. Analyse av uttrekk viser at dette ikke er vanlig i sektoren. [redacted] har ikke egne krav for denne type kontoer.[127] Av de øvrige er det kun [redacted] som har en policy med strengere krav [redacted] som omfatter de fleste brukerkontoer for administrator. Ved [redacted] er det egne passordpolicyer for administratorer, men disse omfatter kun en liten del av disse (vanligvis i hovedsak domeneadministratorer). Ved [redacted] er det en egen policy som omfatter de fleste administratorer, men hvor kravene til passord er svakere enn for ordinære brukerkontoer [redacted]

En angriper vil ofte forsøke å finne passord til brukerkontoer ved å gjette hva et passord kan være. Programmer automatiserer og effektiviserer slike angrep slik at et passord kan prøves for flere tusen brukerkontoer på noen få minutter, jf. punkt 4.1.3. Hvor mange gjettinger som en angriper kan foreta avgrenses av hvilken grense som er satt med hensyn til antall mislykkede påloggingsforsøk før en konto låses. Som det framgår av tabell 3 varierer dette sterkt mellom virksomhetene. [redacted] Når det tillattes mange forsøk kan en angriper gjøre mer intensive forsøk på å gjette passord, og risikoen øker dermed for at angriperen vil lykkes med å finne gyldige passord.

[redacted]

5.2.2 Tofaktorautentisering er i ferd med å bli innført

Tofaktorautentisering innebærer at det kreves *noe man har* (for eksempel et smartkort eller en applikasjon på mobiltelefon) ved siden av *noe man husker* (et passord som må oppgis) for å logge på et IT-system. Dette gjør det vanskeligere for en angriper å få kontroll på en brukerkonto da det ikke er nok bare å knekke eller gjette et passord. Innføring av slik autentisering er noe alle virksomheter i undersøkelsen har arbeidet med de siste årene. Ofte er dette omfattende arbeid da de fleste av virksomhetene har både omfattende portefølje av systemer med ulike autentiseringsmekanismer og mange brukere.

Alle virksomheter omfattet av undersøkelsen har opplyst at løsninger for tofaktorautentisering er innført eller er i ferd med å bli innført for mange tjenester. Imidlertid var det ingen av virksomhetene som hadde innført slik autentisering for alle tjenester. Tjenester knyttet til Microsoft 365, inkludert kontorstøtteapplikasjoner som Office-pakken, e-posttjeneste og skytjenester, er omfattet ved alle virksomheter, men hva som omfattes ellers varierte på undersøkelsestidspunktet.

[redacted]

[126] Servicekontoer er brukerkontoer som programmer benytter for å logge på IT-systemer.
[127] Det gjelder [redacted]
[128] [redacted]

[redacted]

5.3 Sårbarhetsstyring

Angripere utnytter ofte sårbarheter i programvare for å få tilgang til og kontroll over IKT-systemer. Utnyttelse av programvaresårbarheter har vært årsaken til en stor del av aktiviteten NSM har registrert mot norske IT-nettverk de siste årene.[129] God sårbarhetsstyring forsøker å oppdage og avhjelpe sårbarhetene før disse kan utnyttes i et angrep.

Faktaboks 6 God praksis for å styre og redusere sårbarheter i IT-systemer

Som god praksis for å styre og redusere sårbarheter i en virksomhets IT-systemer og -infrastruktur har vi lagt til grunn følgende anbefalinger:

- Sikkerhetsoppdateringer fra IT-leverandører som fjerner kjente sårbarheter bør installeres så fort som mulig.[130]
- Virksomheter bør herde systemer og programvare eksempelvis ved å ta bort funksjonalitet det ikke er tjenstlig behov for, gjennomgå innstillinger for sikkerhet og fjerne standardpassord.[131]
- For å sikre at alle viktige sårbarheter blir behandlet, er beste praksis å skanne alle systemer for sårbarheter jevnlig med egne verktøy og ha rutiner for å gjennomføre tiltak som reduserer sårbarheten.[132]
- Sårbarhetsskanning anbefales gjennomført både eksternt fra Internett og internt i virksomhetens nettverk, samt med og uten brukerrettigheter.[133]

Kilde: NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0, punkt 2.3 og 3.1, samt Center for Internet Security: CIS Controls, version 8, punkt 7.5 og 7.6.

5.3.1 Sikkerhetsoppdateringer gjennomføres regelmessig, men med noen unntak

Undersøkelsen har omfattet uttrekk av informasjon fra en stikkprøve av Windows-baserte klientmaskiner og servere for å gi grunnlag for å vurdere om sikkerhetsoppdateringer blir gjennomført regelmessig. Analyse av uttrekk viser at virksomhetene har rutiner for dette og gjennomfører månedlige oppdateringer i samsvar med leverandøren Microsofts frekvens for å utgi oppdateringer.

Det forekommer imidlertid noen unntak fra hovedregelen om månedlig oppdatering, og omfang av avvik varierer noe mellom virksomhetene. Som oftest er dette noen enkeltstående maskiner hvor oppdatering feiler og dette ikke blir plukket opp av manuell oppfølging. Tabell 4 viser andelen av klientmaskiner i stikkprøver hvor Microsoft Windows ikke var fullt ut oppdatert. Tallene viser at dette

[129] Nasjonal sikkerhetsmyndighet: Risiko 2023, s. 19.
[130] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, tiltak 2.3.1.
[131] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.3.
[132] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 3.1.1.
[133] Center for Internet Security: CIS Controls, version 8, punkt 7.5 og 7.6.

gjelder ti til femten prosent av maskinene [redacted]

Tabell 4 Oppdatering av Microsoft Windows på klientmaskiner

[redacted]

Kilde: Uttrekk av historikk fra oppdatering av Microsoft Windows på en stikkprøve av klienter. Tallene viser andel klienter som ikke er oppdatert verken i uttrekksmåneden eller måneden før.

Det er også noen eksempler på oppdateringer av programvare på klientmaskiner fra andre leverandører som ikke har blitt omfattet av systemer for sikkerhetsoppdatering. For eksempel kan det gjelde Adobe Flash Player, som ikke støttes av leverandøren lenger, eller utdaterte utgaver av Java. Der dette er funnet er det enkeltstående tilfeller og ikke systematisk for en virksomhet.

Selv om det er relativt få maskiner med utdatert programvare som er i aktivt bruk ved virksomhetene, vil disse være mål for angripere. [redacted]

En årsak til at gammel programvare anvendes er at noe spesialprogramvare som brukes ved institusjonene ikke kan kjøre på nyere operativsystem. Dette kan for eksempel gjelde laboratorieutstyr som produsenten ikke har sertifisert for nyere operativsystem. Maskiner basert på programvare som ikke kan oppdateres er sårbare for angrep dersom de ikke isoleres i nettverket slik at angripere ikke kan nå maskinene. Noen av virksomhetene har nevnt isolasjon i nettverket som et tiltak for å redusere risiko.

[redacted]

5.3.2 IT-systemer er i liten grad konfigurert for økt motstandsdyktighet mot angrep

Det er vanlig at IKT-systemer leveres fra produsenter eller forhandlere med en konfigurasjon som gjør det enkelt for kunden å komme i gang med å bruke funksjonalitet, men ofte med svakere sikkerhet. Hvis systemene tas i bruk uten å endre konfigurasjonen vil det mest sannsynlig eksistere sårbarheter som kan utnyttes av angripere.

[134] [redacted] har forklart at antallet skyldes at en del maskiner hadde eldre utgave av operativsystemet og disse ble vist som oppdaterte i virksomhetens verktøy for å styre sikkerhetsoppdateringer selv om de reelt ikke var det.
[135] [redacted]

Som en del av dybdeundersøkelsen av tre virksomheter har vi sammenlignet konfigurasjon av et utvalg programvare opp mot god praksis.[136] Uttrekk fra utvalg av systemer ble hentet ut og sammenlignet med anbefalingene.

[redacted]

Hvordan konsulenter/leverandører setter opp utstyr kan også ofte ha betydning for spesielt utstyr som anskaffes av de større virksomhetene, jf. punkt 6.6 om leverandøroppfølging. Enkelte av virksomhetene har opplyst at de har tatt i bruk sikkerhetsstandarder ved installasjon av noen typer programvare for at konfigurasjon av programvare skal være mer motstandsdyktig mot dataangrep.[138]

[redacted]

5.3.3 Virksomhetene har kommet kort med skanning av IT-utstyr for å fjerne sårbarheter

For at en virksomhet skal unngå sårbarheter i sine systemer, må den behandle en konstant strøm av oppdateringer av programvare, råd om hvordan man skal forholde seg til sikkerhet fra leverandører, samt andre meldinger om trusler og sårbarheter som har blitt oppdaget. Dette er krevende å holde oversikt over. For en angriper kan det være nok å finne én sårbarhet som ikke er behandlet.

Ekstern sårbarhetsskanning vil kunne finne sårbarheter som er synlige og kanskje kan utnyttes fra Internett. Siden det er mange trusselaktører på Internett er det høy risiko for at disse sårbarhetene blir

[136] Utgangspunkt har vært «benchmarks» fra Center for Internet Security for Microsoft Windows, ulike versjoner av Linux og databaser basert på Microsoft SQL Server. Disse «benchmarks» gir konkrete anbefalinger for sikker konfigurasjon av ulik programvare basert på anerkjent beste praksis i bransjen. Se https://www.cisecurity.org/cis-benchmarks

[137] [redacted]

[138] For eksempel opplyser [redacted] at det benyttes en mal utviklet i det amerikanske forsvaret (Security Technical Implementation Guides (STIG)) for installasjon av maskiner [redacted]. [redacted] har også nevnt at sikkerhetsstandarder fra leverandører som Microsoft og [redacted] i noe grad er brukt ved utrulling av maskiner.

[139] [redacted]

[140] [redacted]

forsøkt utnyttet. Bare en mindre del av virksomhetens infrastruktur bør derfor være synlig fra Internett. Som en del av prosjektet for opprettelse av Cybersikkerhetssenteret i Sikt ble det først testet ekstern sårbarhetsskanning av alle virksomheter i sektoren i 2021. Fra 2022 gjennomføres ukentlig ekstern sårbarhetsskanning med rapportering til virksomhetene. [redacted]

Innhentet dokumentasjon og svar viser at rapportene fra den eksterne sårbarhetsskanningen blir behandlet systematisk av virksomhetene som inngår i undersøkelsen, og sårbarhetene blir lukket. Noen sårbarheter kan ta noe tid å lukke, avhengig av kompleksiteten i den sårbare løsningen og hva som må gjøres for å redusere sårbarheten. Rapportene fra Sikt viser at enkelte sårbarheter går igjen over lengre tid. Virksomhetene har opplyst at dette i noen tilfeller er sårbarheter som ikke er reelle, hvor skanningen viser feil resultat. Enkelte virksomheter har tatt opp problemstillingen om å fjerne eller markere disse på rapportene fra skanningen for å vise et mer reelt resultat og forenkle gjennomgangen av rapportene.

Faktaboks 7 Sårbarhetsskanning

En sårbarhetsskanner er programvare som undersøker om maskiner, nettverk eller applikasjoner har kjente sårbarheter. Programmet benyttes for å finne sårbarheter som skyldes mangelfull sikkerhetsoppdatering eller usikker konfigurasjon. Ved å skanne et helt nettverk vil en virksomhet få et helhetlig bilde av egen risiko på området.

Sårbarhetsskanning kan gjennomføres fra Internett, og vil da kunne avsløre sårbarheter som kan utnyttes fra Internett. Skanning kan også gjennomføres internt i virksomhetens nettverk. Det vil gi informasjon om sårbarheter som kan utnyttes av angripere som allerede har et fotfeste innenfor virksomhetens nettverk.

Tre viktige momenter for resultater ved gjennomføring av sårbarhetsskanning:

- Om skanning gjennomføres uten autentisering eller ut fra en brukerkonto med rettigheter som administrator. Bruk av rettigheter som administrator vil gi en grundigere skanning.
- Omfanget av enheter som skannes. Dersom enheter unntas fra skanning er det risiko for at sårbarheter ikke oppdages. På den annen side kan skanning gi enkelte gamle enheter problemer.
- Oppfølging av avdekkede sårbarheter. I større nett må det forventes et stort antall sårbarheter og det er viktig at det er rutiner for å prioritere oppfølging av disse.

Intern sårbarhetsskanning vil kunne vise sårbarheter som er synlige for og kan utnyttes av en angriper som allerede har et fotfeste på innsiden av virksomhetens nettverk.[141] Det er færre trusselaktører på innsiden, men det vil være et langt større spekter av mulige sårbarheter.

[redacted]

[141] Segmentering av nettverk bør redusere hva en bruker i virksomhetens nettverk kan nå i nettverket, slik at hvilke sårbarheter som er synlige vil variere avhengig av bruker. Jf. punkt 5.5.2.

Når en virksomhet starter med sårbarhetsskanning, vil det vise en stor mengde sårbarheter. Etter hvert som virksomheten arbeider med resultatene vil antallet reduseres ved at sårbarheter avhjelpes og «falske positive»[142] merkes.

[redacted]

Virksomhetene prioriterer hvilke sårbarheter som skal følges opp. Programvare som benyttes for sårbarhetsskanning kategoriserer sårbarhetene som kritiske, høy, medium og lav risiko.

[redacted]

Ingen av [redacted] gjennomfører sårbarhetsskanning med en autentisert brukerkonto med administrative rettigheter. Fordelen med å benytte en brukerkonto med administrative rettigheter er at sårbarhetsskanningen vil gi et mer komplett bilde (identifisere flere sårbarheter) og resultatene vil være mer nøyaktige (færre tilfeller som ikke er reelle). God praksis tilsier at skanning både med og uten administrative rettigheter bør gjennomføres.[144]

[redacted]

Enkelte av virksomhetene har nevnt at andre verktøy kan identifisere sårbarheter. Et slikt eksempel er [redacted] som allerede er installert på mange servere og klientmaskiner. En slik løsning vil ikke kunne identifisere sårbarheter ved nettverksutstyr, skrivere, laboratorieutstyr mv. Det kan imidlertid være en enklere metode for å få oversikt over sårbarheter på administrerte klienter og servere hvor denne modulen er installert. Maskiner ført inn i nettverket utenom vanlige rutiner vil ikke bli omfattet.

[redacted]

5.4 Nettverkssikkerhet

En angriper som prøver å få tilgang til et IT-system vil først forsøke å koble seg til virksomhetens nettverk, og deretter forsøke å nå IT-systemet som er målet. Her ser vi på tiltak for å hindre fremmede å koble seg til forskningsvirksomhetens nettverk, og tiltak som skal hindre angripere å bevege seg rundt i nettverket for å nå sensitive IT-systemer.

[142] Falske positive er et varsel om at det foreligger en sårbarhet, men hvor sårbarheten ikke er reell.
[143] [redacted]
[144] Det forutsettes at virksomheten har rutiner og systemer som sikrer trygg håndtering av brukernavn og passord som benyttes til skanningen.
[145] Center for Internet Security: CIS Controls v.8, side 5-6 og 28. Sårbarhetsskanning er plassert i implementasjonsgruppe 2.

Faktaboks 8 God praksis for å sikre nettverk

Som god praksis for å sikre virksomhetens nettverk har vi lagt til grunn følgende anbefalinger:

- Det bør benyttes løsninger som sikrer at kun PC-er og andre enheter godkjent av virksomheten kan koble seg til dens nettverk, for eksempel en NAC-løsning (Network Access Control). [146]
- Det anbefales at enheter identifiseres sikkert og unikt med for eksempel sertifikater.[147]
- En virksomhet bør dele sitt nettverk opp i ulike soner for bedre å kunne beskytte utstyr med ulik grad av sensitivitet og behov for tilgang. Eksempelvis er det vanlig å separere egne soner for systemadministrasjon, servere, klienter driftet av virksomheten og gjeste-klienter. Kommunikasjon mellom disse sonene anbefales kontrollert og begrenset.[148]

Kilde: NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0, punkt 1.2, 2.2, 2.5 og 2.6

5.4.1 Kontroller med enheter som forsøkes koblet til nettverket

Virksomhetene må sikre sine lokale nettverk, blant annet ved å etablere løsninger som gjør at det kun er PC-er og andre enheter godkjent av virksomheten som kan koble seg til nettverket. [redacted]

Faktaboks 9 Autentisering av enheter (NAC-løsning)

En NAC-løsning (Network Access Control) skal bidra til å sikre at kun godkjente enheter kobles til virksomhetens nettverk. For å oppnå dette er det viktig å få bekreftet med rimelig sikkerhet hvilken enhet som prøver å koble seg til. Dette tilsvarer bekreftelsen av identitet som gjøres for vanlige brukere, hvor angivelse av et passord skal gi nødvendig sikkerhet. Metodene for å bekrefte hvilken enhet det er kan variere. En anbefalt løsning er at enheten utstyres med et digitalt sertifikat. Når en enhet kobles til nettverket, vil det skje en utveksling av sertifikater med en kontrollenhet som sikrer at det er en godkjent enhet.

Ved siden av autentisering kan også andre aspekter ved enheten kontrolleres av en NAC-løsning før den blir koblet til nettverket, for eksempel om den har anti-virus med gyldig signatur, og policyer for sikkerhet kan settes i verk. Enheter som ikke autentiseres vil ikke få tilgang til nettverket og plasseres ofte i egne karantenenett som skal gi minimale muligheter.

[redacted]

[146] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 1.2.
[147] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 2.6.6 a).
[148] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, tiltak 2.2.3 og 2.5.
[149] [redacted]

[redacted]

[redacted]

5.4.2 Flere virksomheter arbeider med å stramme inn muligheter til å kommunisere på tvers av soner i IKT-nettverk med ulik grad av sensitivitet

God separasjon av soner gjør det vanskeligere for en angriper å utvide sine tilganger og få tak i for eksempel viktige forskningsdata.

[redacted] Alle virksomheter har inndelt nettverket i for eksempel egne soner for ansattes PC-er, studenters utstyr og servere, og begrenset kommunikasjonen mellom sonene, men løsningene har hatt svakheter.

I de tre virksomhetene som inngikk i dybdeundersøkelsen [redacted] Alle tre virksomheter jobber med tiltak for bedre kontroll med nettverket i etterkant av inntrengingstesten. Også i de øvrige virksomhetene gjennomføres forbedringer for å bedre kontrollen på kommunikasjon i nettverkene.

Utstyr hvor administratorer drifter IKT-infrastruktur bør beskyttes i en egen sone da tilgang til slikt utstyr kan gi en angriper tilgang til informasjon om IKT-infrastruktur og muligheter for å angripe den. Svar fra virksomhetene viser at [redacted][151] ikke hadde egen sone for utstyr for administrasjon av IT-systemer. [redacted] arbeidet på undersøkelsestidspunktet også med å forbedre sin løsning for å beskytte dette utstyret i nettet.

[redacted]

Flere av virksomhetene har egen infrastruktur for å lagre sensitive data. Disse synes bedre beskyttet nettverksmessig. Se punkt 4.1.6.

150 [redacted]

151 [redacted]

5.5 Logging og overvåkning

Ikke alle dataangrep kan hindres. Det er derfor viktig at virksomheter, gjennom systematisk innhenting og analyse av data fra mange systemer, har kapasitet til å oppdage dataangrep og andre sikkerhetshendelser.

Faktaboks 10 God praksis for logging og overvåkning

Som god praksis for innhente tilstrekkelige sikkerhetsdata og overvåke virksomhetens IT-infrastruktur, slik at sikkerhetshendelser kan bli oppdaget, har vi lagt til grunn følgende anbefalinger:

- Virksomheten bør samle inn tilstrekkelige sikkerhetsrelevante data til å oppdage sikkerhetshendelser tidlig, forstå hendelser, kunne gjenopprette til normaltilstand og hindre gjentakende hendelser.[152]
- Virksomheten bør systematisert prosessere innsamlede data for å kunne avdekke og forstå sikkerhetshendelser. For at sikkerhetsrelevant data skal kunne brukes effektivt bør de sentraliseres og konsolideres for å kunne vurderes, analyseres og dermed gjøre det mulig å reagere riktig på sikkerhetstruende hendelser. [153]
- Virksomheten bør være i stand til å finne kjente trusler i egen infrastruktur, ha kompetanse til å benytte automatiserte verktøy og forstå hvordan verktøyene kan utnyttes best mulig. [154]

Kilde: NSMs Grunnprinsipper for IKT-sikkerhet, versjon 2.0, punkt 3.2 og 3.3

5.5.1 De fleste virksomheter logger vesentlig mindre enn hva god praksis tilsier[155]

Hva som logges er viktig for å gi et grunnlag for analyse som kan avdekke angrep mot en virksomhets infrastruktur. Manglende eller feilaktig konfigurering av logger vil ifølge NSM kunne medføre at angripere kan skjule sin tilstedeværelse, skadevare og aktiviteter.[156]

For å få en oversikt over hva som logges fra Microsoft Windows-baserte servere i de ulike virksomhetene, har vi gjort et uttrekk fra en stikkprøve av servere ved alle virksomhetene. Uttrekkene av hva som logges er sammenlignet med anbefalinger om sikkerhetslogging fra leverandøren Microsoft (MS) og bransjeorganisasjonen Center for Internet Security (CIS). Anbefalingene fra MS og CIS har mye felles, men avviker på noen punkter.

Figur 4 viser i hvilken grad serverne i stikkprøvene følger anbefalingene.

[152] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 3.2.
[153] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 3.2.
[154] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 3.3.
[155] Logging kan ha forskjellige formål. Her omtales kun logging som kan gi grunnlag for å oppdage dataangrep. Logging for for eksempel driftsformål er ikke vurdert.
[156] NSMs Grunnprinsipper for IKT-sikkerhet versjon 2.0, punkt 3.2, jf. tiltak 2.4.4 og 3.1.3..

Figur 4 Logging på server - samsvar med anbefalinger

Kilde: Analyse av uttrekk fra virksomhetenes IT-systemer

-
-
-

Variasjonen indikerer at flere av virksomhetene ikke har enhetlige rutiner for oppsett av Windows-servere og at mangler i rutiner resulterer i at det logges lite på enkelte servere.

For å få et bredere bilde av hva som logges innhentet vi ved de tre virksomhetene i dybdeundersøkelsen også stikkprøver av hva som ble logget fra enkelte Linux-servere og fra Microsoft SQL Server-databaser.

-

[157] Anbefalinger gitt av Center for Internet Security i Benchmarks for de ulike versjoner av Linux.

- [redacted]

5.5.2 [redacted]

Dette punktet omtaler virksomhetenes infrastruktur, ressurser og kompetanse for å overvåke sin egen IKT-infrastruktur basert på logger og andre data som hentes fra IKT-utstyr *innenfor* virksomhetenes egen IKT-infrastruktur.

God overvåkning basert på analyse av logger for å oppdage og følge opp relevante sikkerhetshendelser er en krevende oppgave.

[redacted]

Noen virksomheter arbeidet på undersøkelsestidspunktet med å forbedre sin overvåkningskapasitet. [redacted]

Ved siden av virksomhetenes egen overvåkning av sin IT-infrastruktur, overvåker Cybersikkerhetssenteret i Sikt trafikk som flyter *inn og ut* av virksomhetene[160]. Men Sikt har ikke mulighet til å oppdage hendelser basert på informasjon innenfor virksomhetens infrastruktur. Enkelte

[158] [redacted]
[159] [redacted]
[160] Eventuelt trafikk inn og ut til en av virksomhetens lokasjoner.

av virksomhetene er også tilknyttet Nasjonal sikkerhetsmyndighets VDI-nettverk, som på lignende måte som Sikts Cybersikkerhetssenter overvåker trafikk inn og ut av virksomheter.

[redacted]

5.6 Gjennomgående trekk fra kontroll av tekniske sikkerhetstiltak

5.6.1 [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

5.6.2 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.6.3 Drift utenfor IT-avdelingen kan vanskeliggjøre gjennomføring av sikkerhetstiltak

Forskere i virksomheter som inngår i undersøkelsen ønsker ofte tilgang til spesialisert utstyr og programvare som ikke alltid passer med standard oppsett av IT-systemer fra en sentral IT-avdeling. Dette har skapt ønsker fra brukere om å ha tilgang som lokal administrator på eget utstyr (jf. punkt 5.1.3), og er en av årsakene til at noe IT-utstyr driftes lokalt i institutter eller fakultet (jf. punkt 6.5.2).

Friheten til å installere utstyr som man ønsker kan stå i en konflikt til regelverket for informasjonssikkerhet som gir virksomheten som helhet ansvar for at personopplysninger og annen sensitiv informasjon beskyttes. [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

5.6.4 Flere tekniske sikkerhetstiltak er gjennomført de seneste årene

Oppmerksomheten om risiko knyttet til dataangrep i samfunnet har økt betraktelig de siste årene etter hvert som trusselnivået har økt. Ifølge NSM har for eksempel antallet alvorlige cyberoperasjoner mot norske myndigheter og virksomheter tredoblet seg fra 2019 til 2021.[161] Angrepet mot UiT i 2020 bidro også til forståelse av risiko i sektoren. Undersøkelsen viser at økt oppmerksomhet på risikoen har resultert i forbedringer i tekniske sikkerhetstiltak de seneste årene, hvorav noen trekk er gjennomgående:

- Tofaktorautentisering er innført eller i ferd med å bli innført for de fleste tjenester ved alle virksomheter (jf. punkt 5.2.2).
- Ekstern sårbarhetsskanning har blitt etablert av Sikt og flere av virksomhetene har startet intern skanning for å identifisere sårbarheter som kan utnyttes i et angrep (jf. punkt 5.3.3)
- De fleste virksomhetene har forbedret systemer og rutiner for å oppdatere programvare for å fjerne kjente sårbarheter (jf. punkt 5.3.1). Dette gjelder særlig programvare fra Microsoft.

Undersøkelsen viser også at flere virksomheter har planer for ytterligere forbedringer for å håndtere det økende trusselnivået, blant annet for tekniske sikkerhetstiltak (jf. punkt 7.1.2).

De tre virksomhetene som inngikk i dybdeundersøkelsen har alle, i etterkant av våre undersøkelser, planlagt og til dels gjennomført en rekke tiltak.[162] Disse virksomhetene etablerte raskt tiltak med henblikk på å lukke de konkrete svakhetene som ble påpekt etter inntrengingstestene og analyse av uttrekk, og har planer for mer grunnleggende tiltak som kan redusere risiko for at sårbarheter oppstår på noe lengre sikt. Virksomhetenes tiltak inkluderer:

- [redacted] har blant annet ryddet i brukerkontoer og tilganger og økt krav til autentisering gjennom lengre passord og økt bruk av tofaktorautentisering. Virksomheten skal arbeide videre med å innføre rollebasert tilgangskontroll og en ny sonemodell for bedre nettverkssikkerhet.[163]
- [redacted] har blant annet satt sterkere krav til autentisering med lengre passord og bruk av tofaktorautentisering i flere situasjoner og vil jobbe videre med forbedringer i nettverkssikkerhet og mot en bedre overvåkning.[164]
- [redacted] har blant annet forbedret nettverkssikkerhet ved å få på plass en ny brannmur og har ryddet i brukerkontoer og tilganger. Tofaktorautentisering er i ferd med å bli innført for flere tjenester.[165]

[161] Nasjonal sikkerhetsmyndighet: Risiko 2023 - Økt uforutsigbarhet krever høyere beredskap, side 18.
[162] Alle de tre virksomhetene holdt presentasjoner for oss våren 2023, der de redegjorde for tiltak som var iverksatt etter våre undersøkelser. Vi fikk tilsendt presentasjonene i etterkant som dokumentasjon.
[163] Presentasjon [redacted] i møte med Riksrevisjonen 9. juni 2023.
[164] Oversikt over status for tiltak oppdatert per 8. august 2023 mottatt [redacted]
[165] Presentasjon [redacted] i møte med Riksrevisjonen 19. juni 2023.

6 Virksomhetenes organisatoriske sikkerhetstiltak for å beskytte forskningsdata

I dette kapittelet beskriver vi i hvilken grad de ti undersøkte forskningsinstitusjonene har implementert utvalgte organisatoriske sikkerhetstiltak som er viktige for å beskytte forskningsdata.

Disse tiltakene henger tett sammen med de tekniske sikkerhetstiltakene beskrevet i forrige kapittel. Dersom forskere, veiledere og studenter lagrer sensitive data på feil sted – for eksempel på områder som mange har tilgang til, eller med mindre sikre lagringsløsninger – kan det i praksis slå beina vekk under de tekniske sikkerhetstiltakene. I en del tilfeller må brukere også gjøre noe aktivt utover å lagre dataene på rett sted, for eksempel å selv administrere hvem som skal ha tilgang til områder, kryptere filer med sensitiv informasjon eller ta i bruk koblingsnøkkel for å pseudonymisere persondata. Dette kan ses på som et «ekstra lag» med beskyttelse som gjør det vanskeligere for en angriper å utnytte tilgang til dataene.

Relevante revisjonskriterier

God praksis[166] når det gjelder organisatoriske sikkerhetstiltak, innebærer at virksomheten blant annet

- har oversikt over informasjonsverdier i forskning
- implementerer rutiner for sikker behandling av forskningsdata
- sørger for hensiktsmessig organisering for å sikre at rutiner etterleves, og gjennomfører opplæring og bevisstgjøring av forskere og andre
- avklarer eierskap og sikrer god forvaltning av IT-systemer i forskning
- etablerer rutiner for oppfølging av leverandører av IT-systemer

Oppsummering

- Virksomhetene mangler helhetlig oversikt over hvilke forskningsdata som skal beskyttes.
- De fleste virksomhetene gir føringer om at data skal klassifiseres og lagres ut fra dataenes konfidensialitet. Det gis i større grad føringer for behandling av personopplysninger i forskning, og i mindre grad for behandling av forretningssensitiv informasjon og data som kan være av interesse for fremmede stater.
- Få virksomheter har planer for opplæring i informasjonssikkerhet og personvern. Virksomhetene tilbyr i varierende grad kurs og annen opplæring av forskere, veiledere og studenter. Opplæringen er i liten grad obligatorisk, og virksomhetene opplever at det er behov for mer opplæring.
- Alle virksomhetene tilbyr noe administrativ støtte innenfor informasjonssikkerhet og personvern hvor forskere, veiledere og studenter kan få hjelp ved behov.
- IT-systemer driftet lokalt i fakulteter, institutter og lignende omfattes ofte ikke av virksomhetenes sentrale retningslinjer og rutiner. [redacted] Lokal IT-drift er fortsatt utbredt ved de store universitetene. Særlig ved [redacted] sikkerhetsutfordringer forbundet med dette.
- Oppfølgingen av informasjonssikkerheten hos leverandørene er begrenset, og mange virksomheter etterlyser felles oppfølging av IT-tjenester som er felles for sektoren.

[166] NS-ISO/IEC 27002:2017.

6.1 Oversikt over informasjonsverdier i forskning

Oversikt over hva slags forskningsdata som behandles, er nyttig for å kunne ta gode beslutninger om hvordan IT-systemene som behandler informasjonen, bør sikres, og for å kunne vite hvilke data som er påvirket ved et eventuelt angrep. Kunnskapsdepartementet stiller i *policy for informasjonssikkerhet og personvern i høyere utdanning og forskning* eksplisitt krav om at virksomhetene skal kartlegge informasjonsverdiene sine.

6.1.1 Virksomhetene stiller krav om egen oversikt over informasjonsverdier

Virksomhetene har ulike typer informasjonsverdier, og det kan være ulike grunner til at forskningsdataene er beskyttelsesverdige. Forskningsdata kan være sensitive fordi de inneholder personopplysninger, er forretningssensitive eller kan være av interesse for fremmede stater.[167] Det er også en risiko for at data som hver for seg ikke er sensitive, vil kunne være det hvis de sammenstilles. Data kan også være beskyttelsesverdige av andre grunner, for eksempel kan store datamengder som er samlet inn over lengre tid, ha en høy økonomisk verdi.

Ni av ti virksomheter stiller en form for krav om oversikt over informasjonsverdier. Hos fem av disse er kravet inkludert i overordnede dokumenter i ledelsessystemet.[168] Andre krever kun oversikt over hvilke personopplysninger som behandles, eller de har rollebeskrivelser i underliggende dokumenter som nevner at for eksempel dekaner eller instituttleder har ansvar for å ha oversikt over hvilke informasjonsverdier eller IT-løsninger enheten er ansvarlig for.

En av virksomhetene stiller ikke noe konkret krav om oversikt over informasjonsverdier, men stiller krav om at administrerende direktør skal ha oversikt over forskningsprosjekter gjennom virksomhetens prosjektadministrasjonssystem.[169]

Ved de tre virksomhetene der vi gjennomførte dybdeundersøkelse, intervjuet vi til sammen ti ledere for enheter som gjennomfører forskning. En del av disse uttrykte at det var uklart hva som var forventningen fra sentralt hold til hvilken oversikt de skulle ha over informasjonsverdier i forskning ved sin enhet. Av de ti virksomhetene i undersøkelsen er det bare to som fra sentralt hold har konkretisert hva slags oversikter virksomheten skal ha.[170]

6.1.2 De fleste virksomhetene har en relativt god oversikt over personopplysninger i forskningsprosjekter gjennom Sikts personverntjenester

De fleste virksomhetene har en virksomhetsavtale med Sikt om å bruke Sikts personverntjenester og har derfor relativt god oversikt over personopplysninger i forskning. Tilnærmet alle virksomhetene har avtale om å melde prosjekter inn til Sikt.

Gjennom personverntjenestene bistår Sikt virksomhetene med å etterleve det lovpålagte kravet om å dokumentere alle behandlinger av personopplysninger i forskning. Virksomhetene har tilgang til protokoll over alle behandlinger gjennom Institusjonsportalen (tidligere meldingsarkivet).

[redacted] har sitt eget system, [redacted], hvor alle prosjekter som inneholder personopplysninger, er registrert. Også [redacted] har valgt å protokollføre selv, istedenfor å bruke Sikts personverntjenester.

[167] Nasjonal sikkerhetsmyndighet (2023) angir i *Nasjonal trusselvurdering 2023* hvilke fremvoksende teknologier og forskningsområder som kan være av særlig interesse for fremmede stater. Fremvoksende teknologier: 3D-printere, kvantedatamaskiner, kunstig intelligens, maritim autonomi, bioteknologi og avansert overvåkningsteknologi. Forskningsområder: metallurgi, nanoteknologi, cybersikkerhet, kryptografi, robotikk og autonomi, bioteknologi, kjemi, mikro-elektromekaniske systemer, akustikk og kjernefysikk.

[168] [redacted]

[169]

[170] [redacted] jf. omtale nedenfor i 6.1.3.

Virksomhetene har ikke komplett oversikt over prosjekter som behandler personopplysninger. Bortsett fra [redacted] (se 7.5.1 *Evaluering og kontroll*) kontrollerer virksomhetene i undersøkelsen i liten grad om prosjekter meldes inn til Sikt. Sikt peker i intervju på at oversiktene i Institusjonsportalen ikke er fullstendige, og at de er kjent med at det er mørketall. De opplyser at de har sett en økning i antallet innmeldinger fra enkelte virksomheter som har gjennomført bevisstgjøringstiltak.

6.1.3 Virksomhetene har begrenset oversikt over andre informasjonsverdier knyttet til forskning

Utover oversikten over personopplysninger hos Sikt [redacted] har virksomhetene vi har undersøkt, svært begrenset oversikt over informasjonsverdier i forskning.

Av virksomhetene i undersøkelsen er det kun [redacted] som har gjennomført kartlegginger av informasjonsverdier knyttet til forskning. Dette gjøres ved at alle enhetene rapporterer årlig til en [redacted][171] Enhetene sender inn oversikt over informasjonsverdier, hva slags informasjon det gjelder, hvilket system den lagres i, trusselaktører og klassifisering. [redacted] vurderer det slik at rapporteringen fra enhetene gir et helhetlig bilde av hvilke informasjonsverdier virksomheten forvalter, hvilke trusler disse kan utsettes for, og hvilke sårbarheter som må håndteres. Universitetet mener rapporteringen gir et godt grunnlag for analyser og i økende grad kan brukes som grunnlag for risikovurderinger.[172]

[redacted] oppga at de har oversikt over hvilke temaer og prosjekter institusjonens forskere befatter seg med. Samtidig påpeker de at det er vanskelig å holde oversikt over informasjon som kan være av interesse for andre stater, og at det ikke føres oversikt over alle nettverk forskerne har kontakt med.

Enkelte virksomheter har konkrete planer om å etablere bedre oversikt over informasjonsverdier.[173] Noen av virksomhetene har egne prosjektstyringsverktøy som skal gi en oversikt over forskningsprosjekter, for eksempel

- [redacted] prosjektstyringsverktøy, [redacted], hvor det skal føres oversikt over forskningsprosjekter. Verktøyet dekker imidlertid ikke alt, og det er ingen kategorisering av data etter konfidensialitet i systemet.
- [redacted] verktøy [redacted], hvor det er obligatorisk å registrere alle helseforskningsprosjekter. Dette verktøyet har også en integrasjon mot Sikts database, slik at prosjekter registrert hos Sikt også havner i [redacted]. Enhetene har ulike retningslinjer for andre forskningsprosjekter, og det varierer hvor stor andel av den samlede forskningsporteføljen som registreres i [redacted]

Flere av virksomhetene i undersøkelsen forvalter kunnskap innenfor fagområder som anses som særlig relevante ut fra eksportkontrollregelverket, og/eller besitter utstyr som er underlagt regelverket (se faktaboks 11).

[171] [redacted]
[172] Kilde: Oppsummering av undersøkelser ved [redacted].
[173] [redacted] har det som et eget punkt i sin handlingsplan at det skal etableres en prosedyre for forvaltning av informasjonsverdier, mens [redacted] opplyser at det skal utvikles et verktøy for registrering og forvaltning av alle prosjekter som skal gi en bedre oversikt.

Faktaboks 11 Eksportkontroll, ulovlig kunnskapsoverføring og internasjonale sanksjoner

- Eksportkontrollregelverket skal blant annet hindre at kunnskap som kan bidra til spredning av masseødeleggelsesvåpen og leveringsmidler for slike våpen, overføres til visse land. I praksis innebærer regelverket at det kreves lisens for å eksportere visse varer, teknologi og tjenester fra Norge. Regelverket gjelder i alle sammenhenger der lisenspliktig kunnskap eksporteres ut av landet.
- Dette regelverket må sees i sammenheng med regelverket om gjennomføring av internasjonale sanksjoner, som blant annet legger begrensninger på varer og teknologi som kan selges eller overføres til land underlagt sanksjoner og restriktive tiltak.
- Både PST og Etterretningstjenesten har i sine årlige trusselvurderinger omtalt hvordan enkelte land fordekt forsøker å få tak i kunnskap fra Norge til militære formål. Dette gjøres blant annet ved å plassere og rekruttere egne borgere i avanserte utdannings- og forskningsmiljøer.
- Eksempler på områder hvor disse reglene kommer til anvendelse i kunnskapssektoren er ved ansettelser og gjesteopphold, ved rekruttering av studenter, ved forskningssamarbeid og ved deling av informasjon og forskningsresultater med utenlandske institusjoner, samt ved annen tilgjengeliggjøring av slik informasjon og ved deltakelse eller gjennomføring av kurs og konferanser.
- I mars 2022 ble det sendt ut på høring et forslag til endringer i regelverket for eksportkontroll som blant annet skal tydeliggjøre praktiseringen av kontroll med kunnskapsoverføring. Forslaget anbefaler at forskningsvirksomhetene kartlegger fagområder i egen virksomhet der det kan overføres lisenspliktig kunnskap, samt at de utarbeider oversikt over lisenspliktig utstyr og teknologi i egen virksomhet.[174]

Kilde: https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/kontroll_kunnskap/id2952406/, https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/

Ingen av virksomhetene har fullstendig kartlagt kunnskapsområder og utstyr som er underlagt eksportkontrollregelverket.[175] Imidlertid har flere av virksomhetene begynt et slikt arbeid.[176] En av disse er [redacted]

Flere virksomheter uttrykker i intervju og i svarbrev at det generelt er utfordrende å vite hvilket nivå man skal legge seg på når det gjelder oversikt over informasjonsverdier i forskning, og flere nevner at det er uklarheter rundt forventningene til verdioversikt.[180] Flere nevner at det er uklart både hva oversikten skal inneholde, og om den bør være sentral for hele virksomheten eller mer desentralisert. En virksomhet uttrykte bekymring over at en sentral oversikt over alle informasjonsverdier kan utgjøre en risiko ved at den blir en informasjonskilde for eventuelle angripere.

Flere virksomheter etterlyser klarere føringer fra sentrale aktører, som Sikt ved Cybersikkerhetssenter for utdanning og forskning (eduCSC) eller HK-dir, i form av retningslinjer eller veiledning, for å sørge for en felles forståelse i sektoren av hva man bør ha oversikt over, og hvordan. eduCSC gjennomførte to webinarer om eksportkontroll og verdivurdering i henholdsvis slutten av 2022 og starten av 2023, jf. omtale i kapittel 8.3.3.

[174] https://www.regjeringen.no/no/dokumenter/eksportkontrollforskrift/id2905352/?expand=horingsnotater
[175] Kommer frem i oppsummeringen av webinaret, samt svarbrevene fra virksomhetene.
[176] [redacted] har påbegynt slike kartlegginger. [redacted] har igangsatt kartlegging i 2022 og opprettet et eksportkontrollteam som skal støtte instituttene i kartleggingen deres, ved [redacted] startet med å kartlegge utstyr (ikke data enda).
[177] [redacted]
[178] [redacted]
[179] [redacted]
[180] Blant annet [redacted]

6.2 Retningslinjer og rutiner for sikker behandling av forskningsdata

6.2.1 Nesten alle virksomhetene gir føringer til ansatte og studenter om klassifisering og sikker lagring av forskningsdata

Alle virksomhetene med unntak av [redacted][181] gir føringer i retningslinjer og/eller på brukerrettede støttesider om at virksomhetens informasjonsverdier skal klassifiseres etter konfidensialitet. Det vanligste er at virksomheten har utarbeidet en **klassifiseringsguide** som er tilgjengeliggjort på brukerrettede støttesider.

Disse ni virksomhetene opererer med fire konfidensialitetsklasser. Disse er basert på sektorveilederen UFS 136.[182] Dette er de fire klassene[183]:

- Åpen (grønn) er informasjon som kan være tilgjengelig for alle uten særskilte tilgangsrettigheter.
- Intern (gul)[184] er informasjon som trenger en viss beskyttelse med kontrollerte tilgangsrettigheter.
- Fortrolig (rød) er informasjon som, hvis den blir kjent for uvedkommende, kan forårsake skade for offentlige interesser, institusjonen, enkeltpersoner eller samarbeidspartnere.
- Strengt fortrolig (svart) er informasjon som, hvis den blir kjent for uvedkommende, kan forårsake betydelig skade for offentlige interesser, institusjonen, enkeltpersoner eller samarbeidspartnere.

Videre gir virksomhetene føringer for lagring i **lagringsguider** eller tilsvarende oversikter som angir hvilke lagringsløsninger det er tillatt å bruke for hver konfidensialitetsklasse. [redacted] skiller seg fra de andre virksomhetene ved at konfidensialitetsklassene ikke omtales på institusjonens brukerrettede støttesider rettet mot forskere. [redacted], som ikke opererer med de fire konfidensialitetsklassene, gir føringer for lagring av data i introduksjonsdokumenter som gis til studenter, ansatte og gjesteforskere ved onboarding.[185]

Det er stor variasjon mellom virksomhetene i antallet tillatte lagringsløsninger, og virksomhetene har ulik tilnærming til hvorvidt de tillater lagring av forskningsdata lokalt eller på flyttbare enheter (se faktaboks 12 for en oversikt over de vanligste lagringsløsningene).

[181] [redacted] gir føringer for lagring av data i introduksjonsdokumenter til nyansatte og studenter, men det gis ingen føringer om sikring av data som ikke skal være kjent for allmennheten.
[182] UNINETT. (2017). *UFS 136: Veiledning i klassifisering av informasjon*. Veilederen ble utarbeidet av UH-sektorens sekretariat for informasjonssikkerhet ved UNINETT og sist oppdatert i 2017. Sekretariatet finnes ikke lenger, og ansvaret for å utarbeide beste praksis-fagspesifikasjoner ligger nå hos Sikt. Sikt (ved Cybersikkerhetssenter for forskning og utdanning) har utarbeidet et utkast til ny sektorstandard for klassifisering av informasjon som per juni 2023 var sendt på høring til virksomhetene i sektoren.
[183] Begrepene fortrolig og strengt fortrolig, og definisjonen på disse, er hentet fra *beskyttelsesinstruksen.* UFS 136 krever imidlertid ikke at data klassifisert som fortrolig eller strengt fortrolig skal behandles som forutsatt i beskyttelsesinstruksen § 12.
[184] Ved [redacted] brukes benevnelsen «beskyttet/gul», mens [redacted] bruker benevnelsen «begrenset».
[185] Der framgår det blant annet at «egne data» skal lagres [redacted], mens «felles data» skal lagres på fellesdisk. I praksis lagres forskningsdata primært [redacted].

Faktaboks 12 De vanligste løsningene for lagring og behandling av forskningsdata i de ti virksomhetene

Lokal disk i sluttbrukerens PC eller **flyttbare disker.** For «fortrolige» data er det ofte krav om at disse diskene krypteres slik at data ikke kommer på avveier dersom disken/PC-en stjeles eller mistes.

Fellesområder i lagringssystemer som driftes av virksomhetens IT-avdeling med definerte tilgangsrettigheter for (grupper av) brukere. Utover tradisjonell fillagring brukes også nettbaserte fillagringsløsninger som Microsoft SharePoint med lagring på virksomhetens servere.

Skylagring (lokal eller ekstern). De fleste virksomhetene bruker skylagring beregnet for at flere skal bruke dataene, ofte knyttet til [redacted]. I forbindelse med dette brukes også personlig skylagring knyttet til den enkelte bruker gjennom [redacted], [redacted] Det er en trend at mer flyttes over i skylagring, men sektoren er ikke helt ferdig med fellesdisker, flyttbare disker og lignende.

Tjeneste for sensitive data (TSD) er utviklet av UiO og tilbys hele sektoren. Seks av de ni virksomhetene som gir føringer for klassifisering og lagring, oppgir TSD som en tillatt løsning for behandling av fortrolige eller svært fortrolige data.[186]

HUNT Cloud er en skytjeneste ved NTNU for behandling av sensitive data. Tjenesten leveres også til andre virksomheter.

Andre egenutviklede løsninger for fortrolige/svært fortrolige data. Av de fire virksomhetene som ikke oppgir TSD[187], har to[188] utviklet egne løsninger for å dekke dette behovet. Tre av virksomhetene som oppgir TSD, har i tillegg egenutviklede løsninger for fortrolige eller svært fortrolige data.[189]

Kilde: Virksomhetenes lagringsguider.

Ut fra et sikkerhetsperspektiv vil det være enklere for dem som drifter IT-systemene, å sikre data i et fåtall sentralt driftede tjenester. I tillegg vil det være enklere for en bruker å ha færre valg å forholde seg til. På den annen side kan det oppleves utfordrende for brukerne dersom deres foretrukne løsning ikke er blant de tillatte alternativene. I noen av intervjuene ble det trukket fram at IT-enhetene fryktet å få mye motstand fra brukerne om de begrenset hvilke lagringsløsninger som var tillatt.

[redacted] av virksomhetene som har gått lengst i å begrense hvilke lagringsløsninger som er tillatt til lagring av forskningsdata. Virksomheten lister i sin veileder kun fire lagringsløsninger for forskningsprosjekter: [redacted]. I motsetning til de andre virksomhetene tillater ikke virksomheten lagring av forskningsdata på fellesområder og [redacted]. Fortrolige (røde) data tillates [redacted] med tilleggssikring, mens strengt fortrolige (sorte) data kun er tillatt å lagre i TSD. Som nevnt i kapittel 4 fikk vi gjennom inntrengingstest mot [redacted] tilgang til alle data lagret [redacted].

Virksomhetene har gjort ulike vurderinger av sikkerheten i [redacted] og om de skal tillate lagring av fortrolige data her. Fem av de ni virksomhetene som opererer med konfidensialitetsklasser, tillater dette, mens fire tillater det ikke.[190] Virksomhetene som tillater lagring av fortrolige data i [redacted], forutsetter at brukerne krypterer dataene. Disse virksomhetene har også tatt i bruk [redacted]

[186] [redacted]
[187] [redacted]
[188] [redacted]
[189] [redacted] løsning er imidlertid ikke oppgitt i lagringsguiden da virksomheten anbefaler TSD framfor denne. [redacted] løsning, [redacted], avvikles og flyttes til TSD i løpet av 2023.
[190] Virksomhetene som tillater lagring av fortrolige data i [redacted] tillot ikke dette da vi besøkte dem, men lagringsguiden deres som er publisert på internett og ble oppdatert i 2023, viser at virksomheten hadde innført dette i ettertid. Virksomhetene som ikke tillater det, er [redacted].

[redacted]

6.2.2 Nesten alle virksomhetene har utarbeidet rutiner for behandling av personopplysninger i forskning

Personvernregelverket stiller strenge krav til behandling av personopplysninger. For å hjelpe forskere og andre til å overholde disse kravene har alle virksomhetene unntatt [redacted] utarbeidet egne retningslinjer/rutiner for behandling av personopplysninger i forskning[191] og/eller brukerrettede støttesider om temaet.[192] Rutinene omfatter for eksempel prosjektleder- og linjeansvar i forskningsprosjekter som behandler personopplysninger, bruk av Sikts personverntjenester[193] og føringer for gjennomføring av personvernkonsekvensvurderinger.

[redacted] opplyste i intervju at de forsøker å unngå å gjennomføre forskning som omfatter personopplysninger, fordi de har begrenset kapasitet til å følge opp personvern i forskningsprosjekter.

6.2.3 Virksomhetene gir i mindre grad føringer om behandling av sensitiv forskning som ikke omfatter personopplysninger

Vår gjennomgang av virksomhetenes retningslinjer og brukerrettede informasjon om informasjonsklassifisering og lagring viser at det gjennomgående er mindre veiledning rundt klassifisering og lagring av beskyttelsesverdig informasjon som ikke omfatter personopplysninger.

- Eksportkontroll er først og fremst relevant for virksomheter med teknisk-naturvitenskapelige forskningsmiljøer. Seks av virksomhetene nevner data underlagt eksportkontroll som eksempel på fortrolige data[194], [redacted].[195] [redacted]
- Forretningssensitiv informasjon kan finnes i forskningsprosjekter som gjennomføres i samarbeid med eller på oppdrag fra industrien. Det kan også finnes i forskningsprosjekter som kan resultere i kommersialisering eller patentering. Forretningssensitiv informasjon er ikke eksplisitt nevnt som eksempel hos noen av virksomhetene. Noen virksomheter nevner imidlertid taushetsbelagt informasjon som et eksempel på fortrolige data[196], og noen nevner forskningsdata og datasett av stor økonomisk verdi som eksempler på strengt fortrolige data[197].

Dermed er det mindre støtte å hente for forskere som håndterer informasjon underlagt eksportkontroll eller forretningssensitiv informasjon. Flere – både forskere, ansatte ved fakulteter eller institutter samt nøkkelpersonell i den sentrale sikkerhetsorganisasjonen – ga i intervju uttrykk for at trengs mer støtte i form av veiledning, opplæring eller fagnære klassifiserings- og lagringsguider.[198]

[redacted] opplyste også at deres pågående arbeid med ansvarlig internasjonalt samarbeid vil heve bevisstheten ved enhetene rundt hvilke vurderinger som må gjøres når man samarbeider med forskere eller institusjoner i andre land, herunder såkalte «risikoland». Virksomheten viste til at en del av arbeidet omfatter å vurdere behovet for å utarbeide støttesider med brukerrettet informasjon om hvilke forhold man må være oppmerksom på når man samarbeider med forskere/institusjoner fra ulike land, slik virksomheten opplyser at allerede er utarbeidet om samarbeid med Kina.

[191] [redacted] utarbeidet egne retningslinjer.
[192] [redacted] har utarbeidet brukerrettede støttesider.
[193] Alle virksomhetene unntatt [redacted] har avtale med Sikt om bruk av deres personverntjenester.
[194] [redacted]
[195] Enkelte fakulteter ved de undersøkte virksomhetene hadde imidlertid utarbeidet noen egne rutiner på området, bl.a. [redacted]
[196] [redacted]
[197] [redacted]
[198] Dette ble bl.a. trukket fram ved [redacted]

Vi ser eksempler i virksomhetenes retningslinjer og brukerrettede informasjon om informasjonsklassifisering og lagring på at føringene som gis kan oppleves uklare. Et eksempel som går igjen i flere av virksomhetenes lagringsguider, er at særlige kategorier av personopplysninger[199] oppgis som eksempel på røde data, mens *store mengder* særlige kategorier personopplysninger oppgis som eksempel på svarte data. Hva som menes med «store mengder», framgår imidlertid ikke.

Uklarhet om hvilke typer data som skal klassifiseres i de ulike kategoriene kan øke sjansen for at forskere gjør ulike tolkninger, noe som i neste omgang øker risikoen for at enkelte velger lagringsløsninger med for lavt sikkerhetsnivå.

Dybdeintervjuene med forskere indikerer at det er varierende grad av kjennskap til klassifisering av informasjon. Alle forskerne vi intervjuet, hadde et bevisst forhold til hvilke lagringssteder de har valgt for sine forskningsdata, men dette hang ikke nødvendigvis sammen med føringene i virksomhetens retningslinjer og rutiner. Noen forskere pekte på at informasjonsklassifisering kunne være vanskelig. Dette betyr ikke at forskerne er uforsiktige i sin omgang med beskyttelsesverdige forskningsdata, men indikerer at de er avhengig av at virksomhetene gjennomfører tiltak som bevisstgjøring og opplæring.

6.3 Opplæring og bevisstgjøring av forskere, veiledere og studenter

6.3.1 Få av virksomhetene har egne planer for opplæring innenfor informasjonssikkerhet og personvern

Enkelte av de ti forskningsvirksomhetene har handlingsplaner for arbeidet med informasjonssikkerhet og personvern, som også inneholder opplæringstiltak.[200] Ingen av virksomhetene har egne opplæringsplaner som angir hvilke opplæringsaktiviteter som skal gjennomføres av hvem, hvor ofte opplæring skal gjennomføres, og hva den skal inneholde.

[redacted] er den eneste virksomheten i undersøkelsen som har utarbeidet en retningslinje for arbeid med sikkerhetskultur og opplæring innenfor informasjonssikkerhet. På tidspunktet vi gjennomførte dybdeundersøkelsen ved [redacted], var denne ikke fulgt opp. [redacted] oppgir at de i etterkant av undersøkelsen har kartlagt eksisterende opplæring, behovet for opplæring, tilgjengelige ressurser og laget en opplæringsplan og plan for arbeidet med sikkerhetskultur. Nye ansatte og studenter skal nå få grunnleggende opplæring allerede ved semesterstart[201].

Som omtalt i kapittel 7.2 er ansvaret for opplæring ved en del av virksomhetene ikke klart plassert.

6.3.2 Virksomhetene gjennomfører en del enkeltstående opplæringstiltak, men lite er obligatorisk

Alle virksomhetene som inngår i undersøkelsen, bortsett fra de to minste[202], tilbyr i varierende omfang kurs til sine ansatte:

- De fleste virksomhetene deltar i Sikkerhetsmåneden i oktober[203]. Omfanget av aktiviteter varierer, men involverer hovedsakelig at det sendes ut «nano-kurs» til alle ansatte. Nano-kursene handler om informasjonssikkerhet generelt, men ikke informasjonssikkerhet i forskning spesielt.

[199] Begrepet «særlige kategorier personopplysninger» er hentet fra personvernforordningen og omfatter opplysninger om rasemessig eller etnisk opprinnelse; politisk oppfatning; religion; filosofisk overbevisning; fagforeningsmedlemskap; genetiske opplysninger biometriske opplysninger (når behandlingsformålet er å entydig identifisere noen); helseopplysninger; seksuelle forhold og seksuell legning.

[200] [redacted].

[201] Presentasjon holdt av [redacted] 19.06.2023.

[202] [redacted]

[203] [redacted] har ikke deltatt i Sikkerhetsmåneden, mens [redacted] valgte å ikke delta i 2022 men har planer om å delta i 2023. [redacted] erstattet fra 2022 sikkerhetsmåneden med en holdningskampanje hvor 12 nanokurs sendes fordelt ut over hele året.

- Seks av de ti virksomhetene opplyser at de tilbyr e-læringskurs og/eller webinarer.[204] Noen av disse dreier seg om informasjonssikkerhet og personvern generelt, mens andre dreier seg om personvern i forskning eller mer konkrete temaer som datahåndteringsplaner, behandling av forskningsdata og e-postsikkerhet
- Enkelte virksomheter trekker fram at opplæring i informasjonssikkerhet og personvern til en viss grad inngår i introduksjonskurs for nyansatte, oppstart av nye prosjekter, samt metodekurs eller etikk-kurs på masterstudier eller ved oppstart av doktorgradsutdanning. Andre påpeker at det er begrenset med informasjon om temaet på disse kursene.
- Ved enkelte virksomheter presenterer IT-avdelingen, personvernombudet eller andre relevante personer temaer relatert til informasjonssikkerhet og personvern for enheter ved virksomheten på forespørsel eller der de ser behov.
- Ved fem av virksomhetene har studenter og ansatte tilgang til Personvernspillet og Forskningsetikkspillet via Sikresiden.no[205]. Av disse var det bare [redacted] som hadde tatt i bruk Personvernspillet på undersøkelsestidspunktet.
- Noen virksomheter bruker intranett til bevisstgjøring og publiserer nyhetssaker på intranett både i forbindelse med sikkerhetsmåneden og ellers gjennom året. Noen har også egne sider for forskere på nettside/intranettside med en god del informasjon om både personvern og informasjonssikkerhet, og lenker til forskjellige guider og retningslinjer.

Med noen få unntak er ikke opplæring i informasjonssikkerhet og personvern obligatorisk i virksomhetene. Unntakene er [redacted], som har et obligatorisk kurs i informasjonsklassifisering, og [redacted] hvor e-læringskurs i personvern er obligatorisk for alle ansatte ved fakultetene som tilbyr dette kurset[206], og også for studenter ved enkelte fakulteter. [redacted] nettkurs for ansatte og studenter er ikke obligatorisk, men ansatte som ikke gjennomfører kurset får halvårlig påminnelse på e-post.[207]

6.3.3 Virksomhetene peker selv på at det er behov for mer opplæring

Selv om de fleste virksomhetene tilbyr noe kurs og opplæring innenfor informasjonssikkerhet og personvern, viser undersøkelsen at det er et behov for mer opplæring.

Behovet for mer opplæring trekkes gjennomgående fram i internrevisjonsrapporter. Videre trekker personvernombudene i sine rapporter fram at det er behov for mer kompetanse og opplæring. [redacted] sender spørreskjema til enhetene årlig om blant annet kunnskap og bevissthet om informasjonssikkerhet og personvern (jf. 7.5.2 Evaluering og kontroll). I svarene blir det påpekt at det er behov for mer opplæring. I HK-dirs risiko- og tilstandsrapport for 2023 er ett av de fem foreslåtte tiltakene «styrking av opplærings- og kompetansetiltak innen informasjonssikkerhet og personvern».

I intervjuer i dybdeundersøkelsen påpeker enkelte av forskerne at selv om det finnes mye informasjon på internett/intranett, er informasjonen ikke tilgjengelig nok. Noen av forskerne var for eksempel ikke klar over at virksomheten hadde en lagringsguide eller klassifiseringsguide. Videre påpeker flere forskere at selv om de får en gjennomgang ved oppstart av nye prosjekter, er det lite formalisert opplæring. Det kom i tillegg fram i en rekke intervjuer med både ledere og nøkkelpersonell at det er mindre krevende å sørge for at studenter, doktorgradsstipendiater og nyansatte gjennomfører opplæring, enn at erfarne forskere gjør det. En av grunnene som oppgis, er at man kan inkludere informasjonssikkerhet og personvern i oppstartskurs og metodekurs, men at erfarne forskere har vanskeligere for å ta seg tid til å delta på kurs.

[204] [redacted]
[205] [redacted]
[206] Alle fakulteter bortsett fra [redacted]
[207] [redacted] opplyser at nettkurset skal gjøres obligatorisk høsten 2023, muligens i forbindelse med sikkerhetsmåneden.

6.4 Administrativ støtte til forskerne innenfor informasjonssikkerhet og personvern

Forskningsvirksomhetene har gitt prosjektledere et ansvar for informasjonssikkerhet og personvern i sine prosjekter. Ved alle virksomhetene i undersøkelsen finnes det også andre roller og funksjoner som støtter oppunder prosjektlederens ansvar.

Ved alle virksomhetene i undersøkelsen kan forskere få hjelp fra **sentrale støttefunksjoner**, enten gjennom egne kontaktpunkter som er opprettet for å håndtere spørsmål om håndtering av forskningsdata, via felles brukerstøtte/IT-hjelp eller ved å henvende seg til funksjoner eller enkeltroller som har fått ansvar til å gi slik støtte (se faktaboks).[208]

Faktaboks 13 Eksempler på sentrale støttefunksjoner

[redacted]
Ved [redacted] blir mange henvendelser om informasjonssikkerhet og personvern i forskning behandlet av [redacted] ble etablert i 2020, opprinnelig for å være en tjeneste med rådgivning om publisering av åpne forskningsdata. Tjenesten ble imidlertid utvidet til å omfatte informasjonssikkerhet og personvern etter at det kom uventet mange henvendelser om dette.

Prosjektinitieringsmøter
Ved xxxxx utgjør prosjektinitieringsmøter et fast kontaktpunkt mellom forskere og det administrative støttepersonellet. Prosjektinitieringsmøtene er fast rutine for alle forskningsprosjekter ved xxxxx med unntak av for mindre leveranser. I møtene deltar blant annet prosjektleder, administrasjonssjef/sikkerhetsansvarlig eller assisterende administrasjonssjef og personvernombud. Her kartlegges og identifiseres typene informasjon som prosjektet skal behandle i løpet av prosjektperioden, herunder om prosjektet skal samle inn personopplysninger. Prosjekter som behandler personopplysninger, får videre støtte av xxxxxx personvernombud.[209]

Jurister
Flere av virksomhetene oppgir også at forskere som har behov, kan få hjelp av jurister som er ansatt i sentraladministrasjonen eller forskningsavdelingen ved behov.[210] Dette er for eksempel relevant ved inngåelse av kontrakter i oppdrags- eller bidragsforskning.

Kilde: Riksrevisjonens undersøkelse i de ti virksomhetene.

Alle virksomhetene unntatt [redacted][211] har egne **personvernombud**, som også kan bistå forskere med personvernspørsmål. Det varierer mellom virksomhetene om personvernombudet har full eller delt stillingsprosent. Åtte av virksomhetene har ansatt personvernombud, mens [redacted] bruker eksternt personvernombud.[212]

Alle virksomhetene unntatt [redacted] har **avtale om personverntjenester med Sikt**. Prosjektledere som melder sine forskningsprosjekter til Sikts personverntjeneste, kan få bistand fra en personvernrådgiver

[208] [redacted] har etablert egne felles kontaktpunkter med egne e-postadresser hvor forskere kan sende spørsmål om håndtering av forskningsdata. Ved [redacted] kan forskere sende sine henvendelser til hhv. felles brukerstøtte og IT-hjelp. Ved [redacted] kan forskere henvende seg til informasjonssikkerhetsrådgiver. Ved [redacted] er det i praksis administrasjonssjefen som er kontaktpunkt for ansatte/forskere/studenter som har spørsmål om informasjonssikkerhet og personvern. Administrasjonssjefen henviser videre ved behov, for eksempel til IT-medarbeiderne. Ved [redacted] kan forskere få støtte fra Universitetsbiblioteket. Utover dette kan forskere få støtte fra egne informasjonssikkerhets- og personvernkontakter ved enhetene, jf. omtale nedenfor.
[209] Dersom prosjektet skal behandle persondata, blir behandlingen fulgt opp av det interne personvernombudet. Personvernombudet følger opp og påser at prosjektlederen og andre overholder rutinene for personvern i forskning, som at prosjektlederen utarbeider en datahåndteringsplan, sender inn meldeskjema til Sikt og strukturerer systemet slik vedkommende har beskrevet i datahåndteringsplanen. Personvernombudet følger også opp arkivering og sletting ved prosjektslutt.
[210] Bl.a. ved [redacted].
[211] [redacted] har gjort en juridisk vurdering som konkluderte med at [redacted] ikke er pålagt å ha et personvernombud.
[212] [redacted]

i Sikt eller gjennom en chattetjeneste.[213] Personvernrådgiveren ved Sikt kan blant annet bistå ved gjennomføring av personvernkonsekvensvurderinger (DPIA).[214]

De fleste virksomhetene tilbyr også noe **støtte «lokalt»**, altså ute på fakulteter, institutter eller andre grunnenheter. Dette dreier seg for eksempel om ansatte som arbeider med forskningsdata eller personvern i forskningsprosjekter, systemansvarlige eller datakuratorer, samt jurister som arbeider med eksportkontroll og avtaler.

Den lokale støtten som tilbys, varierer imidlertid mellom enhetene. [redacted] er den eneste virksomheten hvor det er gitt sentrale føringer i ledelsessystem for informasjonssikkerhet og personvern om at det skal finnes støttepersonell lokalt. Virksomheten har etablert informasjonssikkerhets- og personvernkontakter ved alle fakultetene og definert hvilke oppgaver disse skal utføre. Kontaktene skal blant annet være en førstelinjefunksjon ved enhetene ut mot forskere og studenter.[215] Lignende funksjoner er også etablert ved [redacted][216], [redacted][217] og [redacted][218].

Det finnes også lokalt støttepersonell ved flere av de øvrige virksomhetene. For eksempel har [redacted] etablert et nettverk for personvern i forskning for administrativt ansatte med ansvar og/eller interesse for behandling av personopplysninger i forskning.[219]

[redacted] har også ansatt en egen sikkerhetsleder eller sikkerhetsrådgiver, som har et særskilt ansvar for blant annet informasjonssikkerhet.[220] Flere av de andre fakultetene har også forskningsrådgivere som kan veilede om personvern.[221] Også ved [redacted][222] og [redacted][223] har enkelte fakulteter noen ressurser som kan gi støtte til forskere.

6.5 Eierskap og forvaltning av IT-systemer og -utstyr i forskning

Det er svært ulik grad av kompleksitet i IT-infrastrukturen i de ti forskningsvirksomhetene vi har undersøkt. På den ene siden av skalaen har [redacted] en svært kompleks IT-infrastruktur, mens [redacted] representerer den andre siden. Blant de større virksomhetene varierer det også hvor stor andel av IT-infrastrukturen som driftes av den sentrale IT-avdelingen.

Det er god praksis at det **utpekes eiere av IT-systemer (systemeier)**. En systemeier har ansvaret for sikkerheten i sitt system. Det løpende ansvaret for forvaltning og drift av systemet, inkludert kontroll med sikkerheten, er som regel delegert til noen andre (for eksempel en systemansvarlig).

Alle forskningsvirksomhetene vi har undersøkt, har beskrevet eierskap til IT-systemer i ledelsessystemene sine. De fleste slår fast i et overordnet policy-dokument at det skal utpekes eiere

[213] https://sikt.no/vanlige-sporsmal-om-personvern-og-meldeskjema
[214] Dersom behandlingen av personopplysninger innebærer en relativt høy risiko for de registrertes rettigheter og friheter, må det gjennomføres en personvernkonsekvensvurdering (DPIA). Da fyller forskeren, en personvernrådgiver ved Sikt og eventuelt andre involverte ut en DPIA i fellesskap, som oversendes til forskningsinstitusjonen for godkjenning. Kilde: https://sikt.no/personvernhandbok-forskning/vurdering-av-personvernulempe-og-dpia. Ved [redacted] er det virksomhetens personvernombud som skal involveres i gjennomføringen av DPIA.
[215] I tillegg skal kontaktene bistå fakultetsledelsen med etterlevelse av ansvaret for informasjonssikkerhet og personvern.
[216] I tillegg til nettverket av personvernkontakter som gir støtte lokalt, har [redacted] etablert et nettverk for forskningsadministrativt ansatte ved enhetene. Forskningsadministrativt ansatte kan gi støtte til forskere ved sin enhet.
[217] [redacted] har såkalte [redacted] ved fakultetene, som har en førstelinjefunksjon i personvernspørsmål.
[218] Institusjonen har etablert en arbeidsgruppe med vitenskapelige representanter fra hvert institutt, i tillegg til informasjonssikkerhetsrådgiver og IT-leder, ledet av administrerende direktør. De vitenskapelige ansatte fungerer som «superbrukere» innenfor informasjonssikkerhet og personvern, og forskere kan få bistand fra disse.
[219] Nettverket skal både fungere som et forum for erfaringsdeling og informasjon og gi muligheter for kompetanseheving gjennom kurs og arrangementer.
[220] [redacted] hadde dette på undersøkelsestidspunktet.
[221] [redacted]
[222] [redacted] viser i brev til at de har en ressursperson med særlig ansvar for støtte til forskere, også når det gjelder spørsmål om informasjonssikkerhet og personvern. Ved [redacted] er den studieprogramansvarlige og en administrativ rådgiver ansvarlig for å informere om regler og at det registreres datahåndteringsplaner.
[223] [redacted] trekker i oversendelsesbrevet fram jurister ved [redacted] som blant annet gir råd og veiledning innenfor temaene informasjonssikkerhet og personvern til ledere, ansatte og studenter, som eksempel på dette. Andre fakulteter har samordnet arbeidet med informasjonssikkerhet og personvern med HMS og beredskap. [redacted] har etablert et fast informasjonssikkerhetsteam bestående av fakultetsdirektør, tre representanter fra fakultetets stab, én representant fra fakultetets seksjon for forsking, utdanning og formidling samt én representant fra ett av instituttene. [redacted] opplyste i intervju at det ikke finnes dedikert personell ved fakultetene som har ansvar for å støtte forskere innenfor informasjonssikkerhet og personvern.

av alle IT-systemer. Systemeierne har et overordnet ansvar for sikkerheten i systemene, ansvar for gjennomføring av risikovurderinger og lignende.

Som hovedregel er det virksomhetens IT-avdeling som har eierskapet til fellessystemer og -tjenester som MS Office 365, mens eierskapet til andre IT-systemer og -tjenester ligger til fakulteter, institutter eller andre enheter basert på nærhetsprinsippet. Ved [redacted], som har en relativt sett lite kompleks IT-infrastruktur, er det ikke utpekt eiere av IT-systemene, men IT-enheten har ansvaret for systemene.

Vår undersøkelse indikerer at systemeiere utenfor IT-avdelingene i varierende grad er bevisst på ansvaret de har for sikkerhet.

- De fleste virksomhetene stiller krav til at systemeiere skal gjennomføre risikovurderinger av systemene. Da vi ba virksomhetene om å oversende risikovurderinger av IT-systemer for lagring og behandling av forskningsdata, så vi at det kun unntaksvis var gjennomført risikovurderinger av løsninger som ble forvaltet og driftet ute på fakulteter og institutter.
- To av virksomhetene hadde gjennomført kartlegginger som blant annet så på bevisstheten om systemeierrollen ute på enhetene. I begge disse tilfellene fant man at bevisstheten var for lav.[224]

Ved flertallet av virksomhetene i undersøkelsen finnes det i større eller mindre grad IT-systemer og utstyr som brukes i forskning, som ikke driftes av den sentrale IT-avdelingen. Ansvaret for forvaltning og drift ligger i slike tilfeller hos et fakultet, et institutt, en forskningsgruppe eller enkeltforskere/-prosjekter.[225]

[redacted].[226] [redacted].[227]

[redacted]

Det er relativt store forskjeller mellom virksomhetene i omfanget av lokal forvaltning og drift. Ved de mindre virksomhetene dreier det seg i hovedsak om noen enkeltmiljøer/-forskere. Ved de store universitetene er lokal forvaltning og drift mer utbredt. Ved disse går imidlertid trenden i retning av sentralisering av IT-drift og/eller tydeliggjøring av krav til lokale IT-miljøer (se faktaboks).

[224] [redacted]
[225] Utstyret varierer fra noen klientmaskiner, flere servere, til laboratorieutstyr. Systemene varierer fra lagringsløsninger satt opp for enkeltforskere, til IT-infrastruktur for lagring og bearbeiding av data som benyttes i store regionale, nasjonale og internasjonale studier, som [redacted]
[226] Det er noen unntak. [redacted] stiller på ulike måter krav til sikkerheten ved lokal IT-drift.
[227] Unntaket som vi har sett, er [redacted], som har utarbeidet sitt eget ledelsessystem for informasjonssikkerhet.

Faktaboks 14 Sentralisering av IT-drift ved de store universitetene

- [redacted] har jobbet med å sentralisere IT-drift over flere år og har per i dag i dag få utfordringer med drift og forvaltning av lokal IT i forskning.
- [redacted] har noe lokal drift av IT-utstyr og -systemer som brukes i forskning.[228] Universitetet arbeider med å få på plass et rammeverk med krav og retningslinjer for tekniske sikkerhetstiltak som også vil gjelde lokal IT-drift. Ved [redacted] fakulteter er det dessuten etablert en ordning med «digitale partnere», der ansatte har delt stilling mellom IT-avdeling og fakultet. Disse har en rolle for å sikre lokale IT-systemer og -utstyr.
- [redacted] har hatt manglende kontroll på lokalt driftet IT-utstyr og -systemer på institutter og i forskningsgrupper. Universitetet har i løpet av undersøkelsesperioden skjerpet kravene til lokal drift av denne typen løsninger og har satt i gang et større prosjekt for å rydde opp.[229] [redacted] har videre vedtatt planer som blant annet innebærer mer sentralisert drift og forvaltning av IT-systemer og -utstyr knyttet til forskningsmiljøene.[230] Det er også satt inn tiltak som kan redusere sårbarhet på kortere sikt.
- [redacted] har over tid sentralisert IT-drift, men har fortsatt en ikke uvesentlig del knyttet til fakultetene og instituttene. Universitetet har gitt et røft anslag på at ca. 80 prosent av IT-systemene forvaltes og driftes av den sentrale IT-avdelingen, mens resten er driftet ved fakulteter, institutter og lignende. Universitetet anslår samtidig at rundt 80 prosent av sikkerhetshendelsene som registreres av [redacted], kan knyttes til lokal drift.

Kilde: Riksrevisjonens undersøkelse.

En annen utfordring med forskningsmiljøene er at det ikke er uvanlig at forskere ønsker administrative rettigheter på eget utstyr, slik at de kan installere programvare uten å måtte kontakte administrator. Dette er nærmere omtalt i kapittel 5.1.3.

6.6 Oppfølging av informasjonssikkerhet i leverandørforhold

Forskningsvirksomhetene under Kunnskapsdepartementet har tjenesteutsatt store deler av databehandlingen i forskning, undervisning, administrasjon og formidling.[231] For eksempel bruker mange av virksomhetene

- Microsoft 365 med kontorstøtteverktøy, Teams og [redacted]
- Sikts nettverkstjenester, inkludert trådløsnettet Eduroam
- felles studentsystem (FS)
- innloggingstjenesten Feide
- Cristin som register over forskningspublikasjoner og forskningsresultater
- eksamenssystemet Inspera
- læringsplattformen Canvas
- digital karttjenesten MazeMap

Databehandleravtaler skal sikre at personopplysninger blir behandlet i samsvar med regelverket, og sette en klar ramme for hvordan databehandleren kan behandle opplysninger.[232] Alle virksomhetene stiller krav til inngåelse av databehandleravtaler dersom eksterne skal behandle personopplysninger

[228] Det er fire større miljøer som drifter egne løsninger pga. særskilte behov: [redacted]

[229] [redacted] øremerket i 2022 fire stillinger (FTE) til [redacted], som skal kartlegge og rydde i lokal drift og forvaltning av IT-systemer og -utstyr knyttet til forskningsmiljøer.

[230] Se også omtale av dette under kapittel 7.6.2.

[231] Unit (nå HK-dir) gjennomførte i 2020 en undersøkelse av tjenesteutsetting av digitale systemer og tjenester i virksomhetene under Kunnskapsdepartementet. Undersøkelsen dekket alle de 29 virksomhetene som var omfattet av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern. Her oppga tre fjerdedeler av virksomhetene som svarte, at de hadde tjenesteutsatt 50 prosent eller mer av den samlede databehandlingen i forskning, undervisning, administrasjon og formidling. Samtlige virksomheter forventet at omfanget av tjenesteutsetting ville øke de kommende årene.

[232] Datatilsynet: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/

på vegne av dem. Krav til informasjonssikkerhet kan også inkluderes i tjenesteavtaler virksomhetene inngår med leverandørene.

Vi har bedt alle de ti virksomhetene som er undersøkt, om dokumentasjon på rutiner for oppfølging av databehandleravtaler og tjenesteavtaler med leverandører. To av virksomhetene i undersøkelsen har utarbeidet retningslinjer eller rutiner for oppfølging av informasjonssikkerheten hos leverandører.[233] Tre virksomheter[234] oppga at de hadde planer om å utvikle tilsvarende retningslinjer. For øvrig viser flere av virksomhetene til at krav om å inngå databehandleravtaler omtales i andre deler av ledelsessystemet, for eksempel retningslinjer for behandling av personopplysninger.

Mange av virksomhetene oppgir at de gjør vurderinger av informasjonssikkerhet hos leverandørene når de kjøper inn nye IT-løsninger. De gjør også risikovurderinger av IT-systemer ved innføring. Hvorvidt og hvordan vurderingene dokumenteres, varierer sterkt mellom virksomhetene, jf. kapittel 7.4. Det er imidlertid svært begrenset oppfølging av informasjonssikkerhet hos leverandørene i etterkant av dette. De fleste oppgir at de for eksempel ikke innhenter dokumentasjon fra leverandører.

De konkrete eksemplene vi har fått på oppfølging av leverandører, er i hovedsak tilfeller der det er avdekket at utstyr eller systemer har konkrete sikkerhetsproblemer. [redacted] viser til flere eksempler på dette. Når det gjelder databehandleravtaler, har flere tatt en gjennomgang av relevante leverandører etter Schrems II-dommen[235].

Virksomhetene kjøper en del av tjenestene gjennom fellesavtaler for sektoren som framforhandles og vedlikeholdes av kunnskapssektorens tjenesteleverandør Sikt. Flere av virksomhetene peker på at de har begrenset kapasitet til å følge opp informasjonssikkerhet hos leverandører, og noen gir uttrykk for at de ønsker at Sikt tar en større rolle her.[236]

Når en virksomhet innfører et nytt IT-system, må det også defineres krav til sikkerheten i systemene. Uttrekk av data fra virksomhetenes IT-systemer viser at flere virksomheter har gitt omfattende rettigheter til konsulenter og leverandører for å få hjelp med å sette opp nye systemer eller gjøre endringer i eksisterende. I mange tilfeller er det leverandører som definerer hvordan sikkerhetsinnstillinger bør være, og de konfigurerer dermed systemene ut fra egne vurderinger heller enn krav fra virksomheten.

I kontrollen av tekniske sikkerhetstiltak så vi at flere virksomheter ikke kunne svare på hvorfor omfattende rettigheter var tildelt servicekontoer, blant annet fordi systemene på et tidspunkt var satt opp av konsulenter eller leverandører, jf. punkt 5.1.2.

Særlig de mindre virksomhetene er avhengig av ekstern kompetanse for å sette opp og sikre systemer. For eksempel oppgir [redacted] at det ikke settes spesifikke krav til konsulenter når disse setter opp servere, men at de ber dem om å sette opp på en sikker måte.[237] Virksomheten oppgir at de ikke har kompetanse til å følge dette opp.

[233] [redacted] retningslinjer slår blant annet fast at leveransene regelmessig skal evalueres og revideres for å ivareta kravene til informasjonssikkerhet. [redacted] rutine omtaler tilsvarende at systemeier minst en gang i året skal sjekke om behandlingen gjøres i henhold til databehandleravtalen.

[234] [redacted]

[235] Som stiller krav ved overføring av data til land utenfor EØS-området.

[236] [redacted]

[237] Svar fra [redacted] i møte med Riksrevisjonen om tekniske sikkerhetstiltak 14. april 2023.

7 Systematikken i informasjonssikkerhetsarbeidet i forskningsvirksomhetene

I dette kapittelet beskriver vi i hvilken grad de ti undersøkte forskningsvirksomhetene arbeider systematisk med informasjonssikkerhet. Vi undersøker om virksomhetene følger god praksis for ledelsessystemer for informasjonssikkerhet. Videre sammenligner vi dem med hverandre, og vi peker på en del sammenhenger mellom manglende systematikk i arbeidet og svakheter i sikkerhetstiltak som framkommer av kapittel 4–6.

Relevante revisjonskriterier

Virksomhetene skal ha et ledelsessystem for informasjonssikkerhet som skal bygge på anerkjente standarder. God praksis for slike ledelsessystemer innebærer blant annet at ledelsen i virksomhetene:

- definerer en overordnet policy for informasjonssikkerhet i virksomheten, med mål og strategi/hovedprinsipper, og sørger for at det utarbeides planer for å nå målene
- sørger for hensiktsmessig organisering og avklaring av roller og ansvar
- stiller tydelige krav til implementering av sikkerhetstiltak
- sørger for regelmessig vurdering av risiko som grunnlag for iverksetting av sikkerhetstiltak
- sørger for kontroller/evalueringer av sikkerhetstilstanden/-tiltakene, som skal følges opp
- gjennomfører regelmessige gjennomganger av informasjonssikkerheten (ledelsens gjennomgang)

Oppsummering

- Med ett unntak har alle virksomhetene i undersøkelsen dokumentert et ledelsessystem for informasjonssikkerhet, med en overordnet policy som angir mål og strategi for arbeidet. Ikke alle virksomhetene har planer for hvordan de skal nå målene, og det varierer i hvor stor grad planene følges opp.
- Noen steder har uklare ansvarsforhold medført at viktige oppgaver ikke har blitt gjennomført.
- [redacted]
- Bare de tre største virksomhetene har utarbeidet temaspesifikke policyer som omfatter alle de fem tekniske sikkerhetstiltakene vi har sett særlig på i denne undersøkelsen.
- Det gjennomføres langt færre risikovurderinger enn virksomhetene stiller krav til i ledelsessystemene sine, og kun én av virksomhetene har risikovurdert alle relevante deler av IT-infrastrukturen. Flere virksomheter mangler gode systemer for lagring og oppfølging av risikovurderinger og mangler oversikt over det som er gjennomført.
- Det er stor variasjon i hvilke krav som stilles til kontroller og evalueringer, og om dette gjennomføres i praksis. Enkelte virksomheter gjennomfører lite eller ingen kontroll.
- De fleste har rutiner for å melde inn og håndtere avvik og hendelser innenfor informasjonssikkerhet, men det er trolig underrapportering [redacted]
- I virksomheter som gjennomfører en ledelsens gjennomgang, internrevisjoner, egne kontroller og/eller kartlegger underliggende enheter, ser ledelsen og styrene ut til å være bedre informert om status og arbeidet med informasjonssikkerhet enn ved andre virksomheter.

7.1 Mål, strategi og plan for arbeidet

7.1.1 Alle unntatt én virksomhet har et ledelsessystem for informasjonssikkerhet, med en overordnet policy som angir mål og strategi

Et ledelsessystem skal sette planlegging, gjennomføring, kontroll/evaluering og oppfølging av informasjonssikkerhetsarbeidet i system. Alle virksomhetene unntatt [redacted] hadde dokumentert et ledelsessystem for informasjonssikkerhet på undersøkelsestidspunktet. [redacted] hadde imidlertid utarbeidet et utkast til internkontroll for personvern og informasjonssikkerhet.[238]

Alle ledelsessystemene omfatter en overordnet policy definert av ledelsen som beskriver informasjonssikkerhetsmål og hovedprinsipper eller strategi for arbeidet. For øvrig har virksomhetene utarbeidet dokumenter som beskriver roller, ansvar og sikkerhetsorganisering, prosedyrer for sentrale prosesser i ledelsessystemet (som risikovurdering og -håndtering, evaluering og kontroll, og avviks- og hendelseshåndtering), og retningslinjer og rutiner for gjennomføring av sikkerhetstiltak.

Det varierer mellom virksomhetene hvor lenge de har hatt et ledelsessystem for informasjonssikkerhet, og det varierer hvor langt virksomhetene har kommet i å implementere systemene. Seks av virksomhetene [redacted] hadde utarbeidet et ledelsessystem før undersøkelsesperioden for denne undersøkelsen.[239] Fire av disse har gjort større justeringer av ledelsessystemet etter det ble etablert.[240]

De øvrige virksomhetene har utarbeidet et ledelsessystem i løpet av undersøkelsesperioden. [redacted] fikk på plass sitt ledelsessystem i 2019 og [redacted] i 2019/2020. [redacted] etablerte en policy for informasjonssikkerhet i 2017, mens øvrige dokumenter i ledelsessystemet først har kommet på plass senere. Beskrivelse av roller og ansvar kom på plass i 2021, mens virksomheten begynte å gjøre ledelsessystemet tilgjengelig for alle brukerne i 2022.[241] Virksomhetene har dermed hatt ulikt utgangspunkt for arbeidet med informasjonssikkerhet og personvern både ved starten av og i løpet av undersøkelsesperioden.

Flere av de små og mellomstore virksomhetene i undersøkelsen har brukt et sett med maler fra tidligere Uninett AS[242] for å utarbeide ledelsessystemet sitt. Malene inneholder blant annet forslag til styrende dokumenter med beskrivelse av sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisering, samt utkast til ulike retningslinjer. Noen har tatt disse i bruk uten å tilpasse dem fullt ut til virksomhetens egenart. For eksempel har to virksomheter definert rollen «sikkerhetsforum» som kun eksisterer «på papiret».[243] [redacted] pekte i intervju på at det er en gjennomgående utfordring at det kommer krav om systemer og prosedyrer som er beregnet på større organisasjoner, og at det er utfordrende å skalere disse til et nivå som er håndterbart og hensiktsmessig i en liten organisasjon som [redacted].

7.1.2 Virksomhetene har i varierende grad planer for informasjonssikkerhetsarbeidet, og noen følger opp disse i større grad enn andre

Sikkerhetsmålene og strategiene angitt i de overordnede policydokumentene er i de fleste tilfeller overordnede.[244] Hvordan virksomhetene arbeider med å nå informasjonssikkerhetsmålene, varierer

[238] [redacted] ledelsessystem går i liten grad inn på informasjonssikkerhet knyttet til [redacted] IT-systemer, og angir roller og ansvar kun på personvernområdet.
[239] [redacted] fikk på plass et ledelsessystem i 2012, [redacted] i 2015, [redacted] i 2016, og [redacted] i 2018.
[240] [redacted] reviderte sitt ledelsessystem i 2019 og [redacted] i 2020. [redacted] utvidet sitt ledelsessystem til også å omfatte personvern i 2020, mens [redacted] utvidet sitt ledelsessystem for informasjonssikkerhet og personvern til også å omfatte sikkerhet i 2022.
[241] På undersøkelsestidspunktet hadde [redacted] tilgjengeliggjort politikken og andre sentrale, styrende dokumenter og retningslinjer i kvalitetssystemet [redacted]. Ledelsessystemet ble imidlertid primært brukt av ansatte med dedikerte roller i dette.
[242] Uninett AS gikk i 2022 inn i Sikt. I perioden 2013–2018 fantes det et sekretariat for informasjonssikkerhet, etablert av Kunnskapsdepartementet og lagt til Uninett AS. Sekretariatet ga blant annet veiledning i utarbeidelse av ledelsessystem.
[243] [redacted]
[244] Sikkerhetsmålene er f.eks. at arbeidet skal være i tråd med krav i lover, forskrifter og krav fra departementet, og at personvernhensyn skal ivaretas ved behandling av personopplysninger. Strategiene er ofte hovedprioriteringer i arbeidet, som f.eks, at arbeid med informasjonssikkerhet skal være basert på risikovurderinger, at det skal settes av ressurser til arbeidet, at brukere skal gis informasjon/opplæring, mv.

betydelig mellom virksomhetene. De fleste virksomhetene har planer på et eller annet nivå, men det varierer om planene gjelder for hele eller deler av virksomheten, og om planene angir hvem som er ansvarlig – samt tidsfrister – for gjennomføringen.

Tabell 5 Forskningsvirksomhetenes planer for informasjonssikkerhet

Virksomhet	Planer for informasjonssikkerhet i perioden 2019–2022
[redacted]	Har gjennom hele perioden utarbeidet planer for informasjonssikkerhetsarbeidet på flere nivåer. De viktigste områdene og aktivitetene er beskrevet i årlig rapportering til styret, som fungerer som en overordnet plan for arbeidet påfølgende år.
[redacted]	Har gjennom hele perioden utarbeidet årsplaner for informasjonssikkerhet, som gir oversikt over aktiviteter/målsettinger som skal gjennomføres gjeldende år. Planenes format og omfang har endret seg i løpet av perioden, og blitt mer detaljerte.[245]
[redacted]	Har fra og med 2019 utarbeidet detaljerte, periodiske strategier / «veikart» og planer med utgangspunkt i informasjonssikkerhetsmålene. De utarbeidet også en lengre tiltaksliste etter en større informasjonssikkerhetshendelse i 2020.
[redacted]	Har utarbeidet årsplaner for arbeidet med informasjonssikkerhet i 2019, 2021 og 2022. Planene er overordnede og skal fange opp de viktigste tiltakene som pågår, men har i løpet av perioden blitt mer detaljerte.[246]
[redacted]	Har utarbeidet årlige tiltaksplaner for informasjonssikkerhet for 2019, 2020 og 2022. Planene omfatter særlig organisatoriske tiltak, men også noen tekniske tiltak.
[redacted]	Har utarbeidet årlige handlingsplaner, og tiltakslister basert på en risikovurdering som oppdateres årlig.
[redacted]	Har ikke et helhetlig planleggingsdokument, men elementer av planer for forbedring finnes i flere dokumenter. I 2022 ble det utarbeidet en handlingsplan for informasjonssikkerhet for en seksjon i IT-avdelingen.
[redacted]	Har ikke et helhetlig planleggingsdokument for informasjonssikkerhetsarbeidet. Det ble gjennomført en overordnet risikovurdering av informasjonssikkerheten ved virksomheten i 2020, som inneholder konkrete tiltak innenfor ti risikoområder.
[redacted]	Har ikke utarbeidet noen form for skriftlig plan som spesifiserer tiltak som skal gjennomføres for å nå informasjonssikkerhetsmålene.
[redacted]	Har ikke utarbeidet noen form for skriftlig plan som spesifiserer tiltak som skal gjennomføres for å nå informasjonssikkerhetsmålene.

Som det framgår av tabellen, hadde [redacted] ikke utarbeidet planer på virksomhetsnivå for informasjonssikkerhetsarbeidet, mens de øvrige seks hadde laget slike planer.

Virksomheten som i størst grad ser ut til å jobbe planmessig med informasjonssikkerhet, er [redacted]. De har etablert planer på flere nivåer. Informasjonssikkerhet er innarbeidet i virksomhetsplaner/årsplaner for virksomheten som helhet og IT-avdelingen som helhet, og mer detaljerte oppgaver er tatt inn i

[245] Fra og med juli 2022 er alle tekniske og organisatoriske tiltak samlet i ett verktøy, med mulighet for å se status på de ulike tiltakene.
[246] Vi har også fått ettersendt en plan for oppfølging av internrevisjon av 2023 om informasjonssikkerhet og GDPR, som styret har sluttet seg til. Denne er relativt detaljert, og viser en rekke tiltak som skal gjennomføres i 2023 og 2024.

årsplaner for enheter i IT-avdelingen. Den årlige rapporteringen til styret beskriver hva som er statusen for de viktigste eksisterende tiltakene, og hva som er behovet for nye tiltak. Det ser ut til å være god sammenheng mellom disse planene.

Blant de øvrige virksomhetene som har utarbeidet planer i perioden, ser vi at planene i varierende grad følges opp systematisk. For eksempel:

- [redacted] har som vist i tabellen utarbeidet flere konkrete planer i undersøkelsesperioden, både for informasjonssikkerhetsarbeidet som helhet og en større tiltaksliste med tekniske sikkerhetstiltak [redacted]. Den tilsendte dokumentasjonen viser ikke tydelig hvordan tiltakene i planene har blitt fulgt opp, og vi så at en del tiltak ikke var ferdigstilt. Samtidig er en del utestående tiltak tatt inn i det nye veikartet for 2023.
- [redacted] årlige tiltaksplaner inneholder flere tiltak som ikke har blitt gjennomført. Planene er ikke fullstendige, og vi fant flere eksempler på gjennomførte tiltak som ikke inngår i planene. Dette gjaldt særlig tekniske tiltak.

[redacted] gjennomførte en ROS-analyse av informasjonssikkerhet i 2020, som inneholdt anbefalinger til konkrete tiltak innenfor ti risikoområder. Denne la også opp til at det skulle utarbeides handlingsplaner innenfor risikoområdene. Risikovurderingen ble imidlertid ikke fulgt opp systematisk, og den tilsendte dokumentasjonen viser ikke hvordan forslagene er fulgt opp. I dybdeundersøkelsen ved [redacted] så vi at det på noen områder var gjennomført arbeid som så ut til å være i tråd med anbefalte tiltak,[247] mens på andre områder har virksomheten tilsynelatende stått på stedet hvil.

Hos enkelte virksomheter så vi at det var satt generelle mål eller krav til tekniske sikkerhetstiltak i de overordnede policydokumentene, uten at de hadde vurdert hva som skulle prioriteres først, eller lagt noen plan for hvordan dette skulle innføres.[248]

Gjennomgang av planene fra virksomhetene, samt annen dokumentasjon, viser mer generelt at virksomhetene hadde svært ulike utgangspunkt i starten av undersøkelsesperioden 2019–2022. Dette gjelder både ressurser til arbeidet, hvor langt virksomhetene hadde kommet med implementering av sikkerhetstiltak, og hvor systematisk de arbeidet med informasjonssikkerhet.

I etterkant av at vi gjennomførte dybdeundersøkelser ved [redacted], ga vi disse anledning til å gjøre rede for hvilke tiltak de har iverksatt etter undersøkelsen. Alle de tre virksomhetene hadde utarbeidet tiltakslister/-planer for å forbedre informasjonssikkerheten på bakgrunn av forhold som ble avdekket gjennom våre undersøkelser.[249]

7.2 Avklaring av roller og ansvar, organisering og ressurser

Alle virksomhetene i dybdeundersøkelsen har definert roller og ansvar for informasjonssikkerhetsarbeidet i sine ledelsessystemer. Ansvaret for informasjonssikkerhet og personvern følger linjen ved at enhetsledere har ansvaret for informasjonssikkerheten i sin enhet. Det overordnede ansvaret ligger hos styret og ledelsen.

[247] For eksempel tiltak for sikring av e-post, investeringer i grunnleggende tekniske sikkerhetstiltak/IKT-infrastruktur, og et prosjekt for bedre systemer for lagring av data.
[248] Et eksempel på dette var [redacted], som stilte krav om at sikring av IKT-infrastruktur skulle bygge på NSMs grunnprinsipper for IKT-sikkerhet, uten å ha gjort noen prioritering av hvilke sikkerhetstiltak som skulle innføres først.
[249] De tre virksomhetene presenterte tiltakslister/-planer for Riksrevisjonen i møter avholdt i april–juni 2023, samt oversendte planer i etterkant.

7.2.1 Enkelte virksomheter har ikke definert styrets rolle i ledelsessystemet

Kunnskapsdepartementet har i brev til virksomheter som er omfattet av departementets styringsmodell, presisert det følgende:

> «Styret har det øverste ansvaret for risikoen som knytter seg til virksomhetens informasjonsverdier, og er ansvarlig for at sikkerheten er tilpasset denne risikoen. Det er styrets ansvar å sette virksomheten i stand til å håndtere risikoen slik at denne er på et nivå som styret aksepterer.»[250]

Av policyen for informasjonssikkerhet og personvern i høyere utdanning og forskning framgår det også at departementet forventer at styret fører kontroll med informasjonssikkerheten.

Syv av virksomhetene har angitt styrets rolle og ansvar i ledelsessystemet.[251] Styrets rolle er definert på ulike måter i virksomhetene. Hos fem av disse virksomhetene står det i ledelsessystemet at styret skal stille krav til arbeidet med informasjonssikkerhet.[252]

7.2.2 Uklare ansvarsforhold har flere steder hemmet framdriften i arbeidet

Det varierer hvordan virksomhetene har organisert det **sentrale sikkerhetsarbeidet**. De fleste virksomhetene har definert en rolle som informasjonssikkerhetsleder/CISO eller tilsvarende, som har et ansvar for å koordinere informasjonssikkerhetsarbeidet.[253] I de fleste tilfellene er denne rollen plassert i IT-avdelingen. Ledere i IT-avdelingen har også oftest et overordnet ansvar for informasjonssikkerheten i virksomheten.

I de fleste virksomhetene er det noen uoverensstemmelser mellom sikkerhetsorganiseringen på «papiret» og hvordan arbeidet gjennomføres i praksis. I en del tilfeller har det skjedd endringer i praksis som ikke er reflektert i beskrivelsene i ledelsessystemet.

Noen steder er uklare ansvarsforhold en av årsakene til at oppgaver ikke ble gjennomført på undersøkelsestidspunktet. Et eksempel på dette fant vi ved [redacted]. Her var hovedansvaret for informasjonssikkerhetsarbeidet på undersøkelsestidspunktet fordelt mellom tre avdelinger i fellesadministrasjonen, men ingen var tildelt et overordnet ansvar for å ta føringen i arbeidet. Vi observerte manglende samarbeid mellom de tre avdelingene, uklarheter om hva den enkelte enhet hadde ansvar for, og uklarheter rundt hvem som skulle rapportere hva, og til hvem. [redacted] har, i etterkant av vår dybdeundersøkelse, gjort større endringer i organiseringen av området og gitt IT-avdelingen ansvar for «hele» informasjonssikkerhetsområdet.[254]

Vi observerer at det flere steder er noe uklart hvilke tekniske sikkerhetstiltak som skal implementeres (se kapittel 7.3), og hvem som har ansvaret for å følge opp at tiltakene blir iverksatt i IT-driften. Ved [redacted] er for eksempel IT-avdelingen som helhet angitt som en rolle i ledelsessystemet, i tillegg til at IT-direktør er en rolle. Ansvaret for å utvikle sikkerhetspolicy og retningslinjer med krav til tekniske sikkerhetstiltak, samt prosedyrer for å etterleve kravene i den løpende IT-driften, er gitt til IT-avdelingen som helhet. Samtidig mangler [redacted] krav til tekniske sikkerhetstiltak.

---

[250] Brev den 7. januar 2019 om Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning.

[251] [redacted] har ikke angitt styrets ansvar for informasjonssikkerhet i ledelsessystemet, men det står i innledningen til ledelsessystemet at før det gjøres endringer «av en viss karakter» i ledelsessystemet, skal de legges fram for og godkjennes av rektor eller styret. Styrets ansvar for personvern framgår av en støtteside om personvern. [redacted] har heller ikke beskrevet styrets rolle. Det framgår imidlertid at styret skal motta rapport om compliance og personvernrisiko minst en gang i året. [redacted] har ikke omtalt styrets rolle i det hele tatt.

[252] [redacted]

[253] [redacted] har definert rollen som CISO eller (informasjons)sikkerhetssjef. Ved [redacted] var det definert en informasjonssikkerhetsrådgiver, mens ved [redacted] var det definert en IT-sikkerhetsleder/IT-sikkerhetssjef. Ved [redacted] var det definert en rolle som fagansvarlig informasjonssikkerhet, men vedkommende hadde ikke en koordinerende rolle. Ved [redacted] var CISO-rollen definert, men stillingen var på undersøkelsestidspunktet ubesatt.

[254] Presentasjon i møte med [redacted] 19. juni 2023, «Status for iverksatte tiltak ved [redacted]».

Ved [redacted] er ansvaret for ledelsessystemet til sammenligning lagt til IT-sikkerhetssjef, mens ansvar for gjennomføring av tiltak er lagt til linjen/tjenesteeiere. Samtidig har IT-sikkerhetssjefen og underavdelingen for IT-drift regelmessige møter (hver 14. dag) med en agenda som forberedes, saksliste og referat. Lederen og alle seksjonslederne i underavdelingen deltar på møtene, som brukes til å gjennomgå tekniske svakheter og sårbarheter, og følge opp status for implementering av tiltak.

Når det gjelder organisatoriske sikkerhetstiltak, er det flere virksomheter hvor ansvaret for opplæring og bevisstgjøring ikke er klart plassert.[255] Ved flere virksomheter er det også uklart hvilke kontroller som skal gjennomføres, og hvem som skal gjennomføre dem. Dette temaet omtaler vi nærmere i kapittel 7.5.

I noen tilfeller var ikke virksomhetene kommet langt nok i informasjonssikkerhetsarbeidet til at alle oppgaver var plassert. Et eksempel på dette er [redacted], som på undersøkelsestidspunktet hadde gjennomført flere organisatoriske endringer for å gjøre virksomheten bedre i stand til å ivareta informasjonssikkerheten. Imidlertid hadde virksomheten ikke ennå avklart hvem som skulle ha ansvar for ulike aktiviteter og prosesser der det ikke forelå prosedyrer, slik som evaluering/revisjon, opplæring og kartlegging av informasjonsverdier.

Vi har også funnet flere eksempler på at det finnes roller som utfører viktige oppgaver, men som ikke er definert i ledelsessystemet.[256]

7.2.3 Virksomhetene har ulike forutsetninger med hensyn til tilgang til ressurser og kompetanse

Virksomhetene i dybdeundersøkelsen varierer betydelig i størrelse, noe som også gir seg utslag i hvor mye ressurser de har avsatt til arbeidet med informasjonssikkerhet og personvern. Figuren nedenfor viser hvor mange årsverk de åtte universitetene og høyskolene som er undersøkt oppgir at de har øremerket til arbeid med informasjonssikkerhet og personvern i perioden 2018–2022.[257]

[255] Dette gjaldt bl.a. [redacted] hadde utarbeidet en egen retningslinje om arbeid med sikkerhetskultur og opplæring, men på undersøkelsestidspunktet var det ikke klart hvem som i praksis skulle følge opp at retningslinjens bestemmelser ble gjennomført.

[256] Eksempler er [redacted]

[257] Det framgår av undersøkelsene i de ti virksomhetene at antall årsverk brukt på arbeidet i praksis kan avvike noe fra antall årsverk som virksomhetene oppgir at er øremerket til dette.

Figur 5 Antall årsverk øremerket til arbeidet med informasjonssikkerhet og personvern i åtte universiteter og høyskoler (2018–2022)

Kilde: Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2023.

[redacted][258] [redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted].[259]

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted][260] har hatt følgende utfordringer:

- [redacted] opplyste at de har hatt utfordringer med å tiltrekke seg ressurser med tilstrekkelig kompetanse innenfor fagområdene blant annet fordi de ikke har kunnet tilby en konkurransedyktig lønn.[261]
[redacted]
- [redacted] opplyste at de som følge av knappe ressurser vurderer å gjennomføre en tredeling av IT-tjenestene, der virksomhetens IT-ansatte står for den daglige driften, ledelse og support; mens en tredjedel settes ut som konsulenttjenester, og det resterende søkes dekket gjennom samarbeid med et større universitet.[262]

[258] [redacted]
[259] [redacted]
[260] [redacted]
[261] Ved [redacted] var stillingen som CISO ubesatt i perioden november 2021 til desember 2022, noe som hemmet framdriften i informasjonssikkerhetsarbeidet.
[262] [redacted].

[redacted]

[redacted]

[redacted] opplever også en del utfordringer. Disse utfordringene handler både om at IT-infrastrukturen er kompleks (jf. omtale i kapittel 5.6), og at selve organisasjonen er kompleks. De største virksomhetene har store, relativt selvstendige fakulteter og institutter og et større spenn i forskningsaktiviteter. Opplæring, gjennomføring og oppfølging må dermed tilpasses lokale forhold for å få god effekt. Ved [redacted] ble det også trukket fram at tunge beslutningsprosesser står i veien for at sikkerhetstiltak kan gjennomføres effektivt. Innføring av tofaktorautentisering opprinnelig fremmet i 2017/2018, og det kom opp igjen som en konkret anbefaling i den overordnede risikoanalysen i 2020. [redacted] ble imidlertid ikke ferdig med innføring for ansatte før i slutten av september 2022. [redacted] opplyste i intervju at en av årsakene til at det tok så lang tid, var at beslutningen krevde en lengre prosess som involverte større deler av virksomheten.

Blant [redacted] seg ut med et godt utgangspunkt i starten av perioden, med ressurser til arbeidet, en avklart sikkerhetsorganisering sentralt i IT-avdelingen, og rimelig god kontroll med sikring av IT-infrastrukturen. De nye tekniske sikkerhetstiltakene de har gjennomført i perioden, har ikke krevd nye øremerkede ressurser eller omprioritering av ressurser internt; det kunne løses gjennom det daglige arbeidet.

Til sammenligning [redacted] måttet omprioritere ressurser. Disse har gjennomført større «løft» i informasjonssikkerhetsarbeidet, bygget opp en sentral sikkerhetsorganisasjon og/eller gjort avklaringer om roller og ansvar. Som

Figur 5 viser, har både [redacted] hatt en betydelig økning i antall årsverk øremerket til arbeid med informasjonssikkerhet og personvern i perioden.

7.3 Krav til sikkerhetstiltak i policyer/retningslinjer

Virksomhetene i undersøkelsen har i varierende grad utarbeidet temaspesifikke policyer som setter krav til sikkerhetstiltakene som gjennomføres.

For de tekniske sikkerhetstiltakene har vi bedt om dokumentasjon på konkrete krav i retningslinjer og policyer på de fem områdene vi har undersøkt (tilgangsstyring, brukerautentisering, sårbarhetsstyring, nettverkssikkerhet, logging og overvåking). Tabellen nedenfor viser hva vi mottok.

Tabell 6 Krav til tekniske sikkerhetstiltak i de utvalgte virksomhetene

Virksomhet	Krav til tekniske sikkerhetstiltak i policyer
[redacted]	Det er i all hovedsak utarbeidet retningslinjer for de utvalgte sikkerhetstiltakene. Det mangler krav for sårbarhetsskanning og egne brukerkontoer for ulike driftsoperasjoner (men dette ligger i rutiner i IT-avdelingen).
[redacted]	Det er utarbeidet retningslinjer for de tekniske sikkerhetstiltakene.
[redacted]	Det er utarbeidet retningslinjer for de tekniske sikkerhetstiltakene.
[redacted]	Det mangler krav og retningslinjer som skal ivareta betydelige deler av de utvalgte sikkerhetstiltakene. Det er opplyst at virksomheten arbeider med disse.
[redacted]	Policyer dekker to av fem utvalgte sikkerhetstiltak (tilgangskontroll og autentisering). Det er opplyst at det arbeides med å etablere policyer.
[redacted]	Det er kun utarbeidet overordnede krav i policy som ikke dekker utvalgte sikkerhetstiltak. Noen prosedyrer beskriver hvordan man har implementert tiltak, men disse er ikke forankret i mål/policyer.
[redacted]	Det er ikke utarbeidet policyer for tekniske sikkerhetstiltak. Enkelte krav til sikkerhetstiltak er tatt inn i rutinebeskrivelser for IT-avdelingen.
[redacted]	Det er ikke policyer som dekker tekniske sikkerhetstiltak. Enkelte mer detaljerte krav er tatt inn i IT-reglementet fra 2012 og Instruks for personvern, IT og informasjonssikkerhet.
[redacted]	Det er ikke utarbeidet policyer for tekniske sikkerhetstiltak. Utkast til informasjonssikkerhetspolicy setter enkelte krav til tekniske sikkerhetstiltak, men kun på et overordnet nivå.
[redacted]	Policyer dekker noen av sikkerhetstiltakene, men har mangler innenfor blant annet tilgangskontroller og logging og overvåkning.

Kilde: Riksrevisjonens analyse av innhentede dokumenter med krav og retningslinjer for informasjonssikkerhet.

Tabellen viser at [redacted] i hovedsak har utarbeidet temaspesifikke policyer som omfatter de tekniske sikkerhetstiltakene som vi omtalte i kapittel 5. Blant [redacted] er det noen som har policyer for enkelte av tiltakene, mens enkelte andre ikke har retningslinjer for noen av områdene.

Der det ikke stilles konkrete krav, blir det i stor grad opp til den enkelte IT-ansatte å vurdere hva som er tilstrekkelig sikkerhet som skal implementeres i oppsett av systemer og lignende. Ved flere av virksomhetene ser vi en tydelig sammenheng mellom om virksomhetene har stilt krav til tekniske sikkerhetstiltak på ulike områder, og om tiltakene er implementert for de samme områdene. Undersøkelsen tyder for eksempel på at mangel på klare sikkerhetskrav ved flere virksomheter har ført til at IT-ansatte gis større tilgangsrettigheter enn nødvendig – fordi det er enklere i en travel hverdag.

Virksomhetene har også i varierende grad utarbeidet policyer/retningslinjer som stiller krav til implementering av de organisatoriske sikkerhetstiltak som vi har undersøkt. I en del tilfeller er kravene kun definert i rutiner eller i brukerrettet informasjon på nettsiden. Kort oppsummert viser undersøkelsen at nesten alle virksomhetene har definert krav til oversikt over informasjonsverdier og krav til klassifisering og lagring av data. Det er imidlertid færre virksomheter som stiller konkrete krav til opplæring og bevisstgjøring innenfor informasjonssikkerhet, til lokal forvaltning og drift av IT-systemer i forskning, eller til oppfølging av informasjonssikkerhet hos leverandører av IT-systemer. Policyer/retningslinjer med krav til organisatoriske sikkerhetstiltak, og brukerrettet informasjon om dette, er omtalt samlet i kapittel 6.

Omfanget av policyer og skriftlige rutiner må tilpasses organisasjonens størrelse og behov. Det er naturlig at omfanget av krav og retningslinjer i policyer er mindre i mindre virksomheter enn i de store universitetene. Hensikten med å ha dokumentasjon som viser ledelsens forventinger og krav til sikkerhet, er at det gir klarhet internt om hvilke krav til sikkerhet som skal implementeres. Når det mangler føringer, blir det opp til den enkelte ansatte å bestemme hvordan sikkerhetstiltak skal innrettes, og dermed hvilket sikkerhetsnivå som virksomheten skal ha. Det er også nødvendig å ha en viss grad av dokumenterte policyer og rutiner for å opprettholde ønsket sikkerhetsnivå når nøkkelressurser slutter, ved langvarige fravær og lignende.

[redacted] er virksomheten som har utarbeidet flest slike temaspesifikke retningslinjer. Virksomheten har utarbeidet 14 ulike retningslinjer, og disse dekker temaene vi har vært særskilt opptatt av i vår undersøkelse.[263] Ledelsens krav til sikkerhet kom relativt klart fram av [redacted] policydokument og de nevnte retningslinjene. Samtidig så vi at virksomheten hadde et stykke å gå for å etterleve kravene. [redacted] opplyste at de anså kravene i retningslinjene som mål som de ønsker å oppnå på sikt, og som virksomheten skal strekke seg etter.

7.4 Risikovurdering og -håndtering

Vi har undersøkt kravene virksomhetene selv stiller til risikovurdering og -håndtering, og bedt alle de ti virksomhetene om å sende oss oversikter over risikovurderinger som er gjennomført i perioden 2019–2022. Ut fra oversiktene har vi bedt om å få tilsendt et utvalg risikovurderinger. Spesielt ba vi om overordnede risikovurderinger av informasjonssikkerhet som gjelder hele virksomheten, risikovurderinger av IT-infrastruktur, og risikovurderinger av sentrale lagringsløsninger for forskningsdata.

[263] [redacted] har utarbeidet retningslinjer for arbeid med sikkerhetskultur og opplæring; avviksmelding og avvikshåndtering; behandling av personopplysninger; hendelse og krisehåndtering; klassifisering av informasjon; nettverk og informasjonsoverføring; operativ sikkerhet; risikostyring for informasjonssikkerhet; sikker utvikling; sikring av personlig IKT-utstyr; systemeier; tilgangskontroll; informasjonssikkerhet i leverandørforhold; og fysisk sikring av IKT-infrastruktur.

Faktaboks 15 God praksis for risikovurderinger

God praksis for risikovurdering og -håndtering innebærer blant annet

- å systematisk vurdere risikoen for informasjonssikkerhetshendelser som kan inntreffe, for å få et grunnlag for å vurdere hvor det burde settes inn tiltak for å oppnå ønskede resultater, forhindre eller redusere uønskede virkninger og bidra til kontinuerlig forbedring av virksomhetens informasjonssikkerhet[264]
- å utarbeide en prosess for risikovurdering av informasjonssikkerhet som sikrer at risikovurderingene gir konsistente, gyldige og sammenlignbare resultater[265]
- å oppbevare dokumentert informasjon om prosessen for risikovurdering av informasjonssikkerheten[266]
- å håndtere prioriterte risikoer ved å fastsette nødvendige sikkerhetstiltak og utarbeide en plan for håndtering av risikoene[267]

Kilde: NS-EN ISO/IEC 27001:2017 Ledelsessystemer for informasjonssikkerhet punkt 6.1.

7.4.1 De fleste virksomheter stiller høye krav til risikovurderinger i ledelsessystemet

Ni av ti virksomheter har tatt inn krav til risikostyring i dokumenter i ledelsessystemet for informasjonssikkerhet.[268] Ofte stilles det krav om at alt arbeid med informasjonssikkerhet og sikkerhetstiltak som iverksettes, skal baseres på behov som er dokumentert i risikovurderinger.

Enkelte virksomheter har avgrenset kravet til risikovurderinger av IT-systemer og tjenester i virksomhetenes ledelsessystemer ut fra vesentlighet. [redacted] har som utgangspunkt at alle systemer skal ha et minimumsnivå av felles teknisk sikring (grunnsikring) basert på beste praksis og god driftsskikk, og at sikkerhetstiltak for viktige systemer og tjenester utover dette skal baseres på risikovurderinger. [redacted] begrenser kravet til risikovurderinger til systemer som er virksomhetskritiske, eller der det behandles personopplysninger. De andre virksomhetene avgrenser ikke krav til risikovurdering på samme måte.

Videre stiller mange av virksomhetene krav om at risikovurderinger skal gjennomføres relativt ofte. For eksempel stiller [redacted] krav om at risikovurderinger av IT-systemer og -tjenester, datanettverk og infrastruktur, arbeidsprosesser og fysiske forhold skal gjennomføres hvert år. I ledelsessystemene til [redacted] er det krav om gjennomføring av slike risikovurderinger minst annethvert år.

Virksomhetene stiller også generelt krav om å gjennomføre risikovurderinger av forskningsprosjekter som benytter personopplysninger. Det er stilt krav om at det skal gjennomføres en vurdering av personvernkonsekvenser (DPIA) dersom behandling av personopplysninger gir risiko for personvernet, jf. omtale i kapittel 6.2. For mange virksomheter bistår Sikts personverntjenester med gjennomføring av DPIA i forskningsprosjekter.

De fleste virksomhetene har utarbeidet **støttemateriale** for gjennomføring av risikovurderinger. Dette støttematerialet er delvis utformet som retningslinjer for hvordan risikovurderinger skal gjennomføres. Det inkluderer også maler for risikovurdering, som ofte inkluderer veiledning for vurdering og aksept av risiko. Noen virksomheter har også veiledning for gjennomføring av risikovurderinger av informasjonssikkerhet på ulike støttesider på nettside eller intranett.

[264] NS-EN ISO/IEC 27001:2017 punkt 6.1.1.
[265] NS-EN ISO/IEC 27001:2017 punkt 6.1.2.
[266] NS-EN ISO/IEC 27001:2017 punkt 6.1.2.
[267] NS-EN ISO/IEC 27001:2017 punkt 6.1.3.
[268] [redacted] har ikke på stilt krav til risikostyring. Det forelå imidlertid på undersøkelsestidspunktet et utkast til et styringsdokument hvor det framgikk at krav og behov til informasjonssikkerhet skal være risikobasert, og at risikovurderinger skal gjennomføres.

7.4.2 Det er stor variasjon i omfanget av gjennomførte risikovurderinger, og kun én av virksomhetene har risikovurdert alle relevante deler av IT-infrastrukturen

Mottatt dokumentasjon viser at det gjennomføres risikovurderinger på ulike nivåer i virksomhetene – fra overordnede risikovurderinger for hele virksomhetene eller IT-området og ned til risikovurderinger av IT-systemer og vurdering av personvernkonsekvenser i for eksempel forskningsprosjekter.

Omfanget av dokumenterte risikovurderinger av informasjonssikkerhet er vanskelig å fastslå nøyaktig fordi virksomhetene mangler oversikt. Innhentede oversikter viser imidlertid et langt mindre omfang av risikovurderinger enn hva kravene i ledelsessystemene tilsier for de fleste av virksomhetene.

For eksempel viser mottatt oversikt fra [redacted] og det ifølge ledelsessystemet skal gjennomføres risikovurderinger av disse minst annethvert år. [redacted] oversendte 24 risikovurderinger av IT-systemer fra perioden 2019–2022 tross omfattende krav i ledelsessystemet. De mener selv at det dokumenteres færre risikovurderinger enn virksomhetens størrelse skulle tilsi.[269]

De fleste store og mellomstore virksomhetene har gjennomført risikovurderinger av vanlige IT-systemer som benyttes av ansatte og studenter, også som en del av forskningsvirksomheten, for eksempel [redacted]. Som nevnt i kapittel 6.5 så vi at det kun unntaksvis var gjennomført risikovurderinger av løsninger for lagring og behandling av forskningsdata som ble forvaltet og driftet ute på fakulteter og institutter.

[redacted] har ingen skriftlige risikovurderinger av informasjonssikkerhet i perioden. [redacted] har søkt å tilpasse gjennomføringen av risikovurderingene til en liten virksomhet ved å gjennomføre én samlet risikoanalyse som omfatter hele IT-infrastrukturen istedenfor å analysere hvert enkelt IT-system mv. Denne analysen har blitt oppdatert flere ganger, senest i 2022.

[redacted] er det gjennomført **risikovurderinger av alle de relevante delene av virksomhetens sentrale IT-infrastruktur**. Ved mange av de andre virksomhetene er det lagt større vekt på å risikovurdere enkeltstående system, mens risiko i eksisterende infrastruktur ikke vurderes.[270] Mange av disse IT-systemene vil være avhengig av sentral IT-infrastruktur, som kan innebære mangler i grunnlaget for risikovurderinger når et IT-system vurderes isolert.

De fleste virksomhetene gjennomfører en **overordnet risikovurdering** som gjelder hele virksomheten og omfatter risiko knyttet til informasjonssikkerhet. Denne vurderingen er flere steder utformet som en scenariobasert risiko- og sårbarhetsanalyse, hvor et scenario kan inkludere dataangrep.

Ingen av de overordnede risikovurderingene sammenstiller informasjon fra mer detaljerte risikovurderinger av IT-systemer mv. Vår analyse av risikovurderingene vi har mottatt, viser at virksomhetenes rutiner og støtteverktøy for risikostyring ikke ser ut til å legge til rette for å samle funn fra mer detaljerte risikovurderinger til de overordnede risikovurderingene for området.

Enkelte virksomheter har grundigere overordnede risikovurderinger av informasjonssikkerhet. For eksempel har [redacted] i flere år gjennomført en overordnet risikovurdering innenfor informasjons-sikkerhet, HMS og beredskap i regi av virksomhetens beredskaps- og sikkerhetsutvalg. [redacted]

[269] [redacted]. (2023). *Årsmelding 2022*.

[270] I [redacted] overordnede risikovurdering ble det anbefalt at det burde gjennomføres en risikovurdering av eksisterende infrastruktur. Dette har imidlertid ikke blitt prioritert fordi det gjøres betydelige investeringer i infrastrukturen. [redacted] påpeker at risikovurderinger som gjøres som del av årlig internkontroll, også inkluderer vurderinger av eksisterende IT-infrastruktur. Universitet har imidlertid ikke gjennomført egne, helhetlige risikovurderinger av eksisterende IT-infrastruktur.

gjennomførte i 2020 en større overordnet risikovurdering [redacted], som pekte på ti risikoområder innenfor informasjonssikkerhet for virksomheten som helhet. Som nevnt i kapittel 7.1 viser ikke den tilsendte dokumentasjonen hvordan [redacted] har fulgt opp risikoene.

Vår analyse av mottatte risikovurderinger viser også **mangler i gjennomførte risikovurderinger**. Mange angir tiltak for å redusere risiko**,** men det er i liten grad angitt hvem som har ansvar for å gjennomføre tiltaket, eller hva som er fristen for å gjennomføre tiltaket. For at en risikovurdering skal ha noen effekt, må risikoreduserende tiltak faktisk gjennomføres.

I flertallet av risikovurderingene vi har mottatt, er det angitt hvor høy sannsynligheten er for at en risiko inntrer, og hva konsekvensen er dersom dette skjer. I en del risikovurderinger er dette imidlertid ikke spesifisert. Dermed er det ikke mulig å se hvor alvorlig en risiko er, og om det bør iverksettes tiltak, ut fra risikovurderingen i disse tilfellene.

7.4.3 Flere virksomheter mangler gode systemer for lagring og oppfølging av risikovurderinger

Mange av virksomhetene mangler gode systemer for å støtte og lagre risikovurderinger, og de lagrer disse ulike steder eller i ulike systemer.[271] Dette gjør det vanskeligere for virksomhetene å holde oversikt over hvilke risikovurderinger som er gjennomført. Manglende oversikt gjør det igjen vanskeligere å sikre at vedtatte risikoreduserende tiltak som følger av vurderingene, blir fulgt opp og gjennomført.

Flere av virksomhetene har ønsket å kjøpe inn et nytt system for å støtte risikoarbeidet, men venter på innkjøp av felles sektorløsning som har vært planlagt gjennom Sikt. Prosessen for å få etablert en fellesløsning har tatt tid, og anskaffelsen ble i 2023 felt i Klagenemda for offentlige anskaffelser (KOFA).

7.4.4 Risikovurdering av felles løsninger gjennomføres av den enkelte virksomhet uten støtte

De fleste universitetene og høyskolene i undersøkelsen bruker en del av de samme IT-systemene, som kontorstøtteverktøy, ofte kjøpt fra Microsoft, læringsplattformer og administrative system. For noen av disse IT-systemene er det inngått felles avtaler for sektoren. Risikovurderinger av disse systemene i de enkelte virksomhetene må omfatte både risiko som er den samme for alle virksomhetene som bruker systemet, og risiko som følger av den lokale implementasjonen av systemet.

Vi har i liten grad sett risikovurderinger som er utført for hele sektoren, som kunne redusere behovet for å vurdere risiko for momenter som vil være felles for alle virksomhetene. Uninett har gjennomført en risiko- og sårbarhetsanalyse av Microsoft Office i 2016 og [redacted] en risikovurdering av videomøtetjenesten Zoom sammen med Uninett i 2019. For øvrig ser det ut til at risikovurderinger er gjennomført av den enkelte virksomhet uten støtte fra sentrale organer eller samarbeid i sektoren.

Risikoen av en løsning kan vurderes forskjellig av ulike virksomheter. Et eksempel på det er at noen virksomheter tillater å lagre forskningsinformasjon [redacted], mens andre ikke tillater det (se punkt 6.2.1). Løsningene fra [redacted] som risikovurderes, er i all hovedsak de samme, selv om det kan være enkelte forskjeller i oppsett av systemene eller rutiner i virksomheten.

[271] For eksempel håndteres risikovurderinger lokalt i de enkelte enhetene eller i prosjekter ved [redacted] uten noen samlet oversikt. Heller ikke [redacted] har en samlet oversikt over risikovurderinger. [redacted] opplyser at risikovurderinger skal sendes inn og registreres i et regneark, etter at en løsning med felles arkiv for risikovurderinger ikke fungerte i praksis.

7.5 Evaluering, kontroll og avvikshåndtering

7.5.1 Få virksomheter stiller krav til og gjennomfører evaluering og kontroll i stor grad

Sikkerhetsrevisjoner og kontroller skal gi virksomheter et grunnlag for å evaluere om ledelsessystemet for informasjonssikkerhet fungerer slik at virksomheten oppnår ønsket sikkerhet. Det varierer mellom virksomhetene i undersøkelsen hvilke krav som stilles til gjennomføring av evaluering og kontroll i ledelsessystemene. Det varierer også i hvilken grad virksomhetene gjennomfører evaluering og kontroll, og om de følger egne rutiner. Tabellen nedenfor gir en overordnet oversikt over hvilke krav som stilles til evaluering og kontroll i virksomhetenes ledelsessystemer, og om det gjennomføres kontroller i praksis.

Tabell 6 Krav til og gjennomføring av evaluering og kontroll i de ti virksomhetene

Virksomhet	Krav til og gjennomføring av evaluering og kontroll
[redacted]	Ledelsessystemet har et eget kapittel som beskriver en rekke kontroller og sikkerhetsrevisjoner som skal gjennomføres. Det gjennomføres også en rekke kontrollaktiviteter i praksis.
[redacted]	Ledelsessystemet beskriver kontroller og sikkerhetsrevisjoner som skal gjennomføres, inkludert stikkprøver av forskningsprosjekter. Det er et eget kapittel i ledelsessystemet som omhandler internkontroll og sikkerhetsrevisjon. Det gjennomføres også en rekke kontrollaktiviteter.
[redacted]	Ledelsessystemet omtaler noen steder kontroller som skal eller kan gjennomføres. Blant annet skal det gjennomføres sikkerhetsrevisjoner, og systemeiere skal gjennomføre en egenvurdering/egenrapportering av IT-sikkerhet i sine systemer. I tillegg kan det tas stikkprøver for å sikre etterlevelse av personopplysningsloven, eller skriftlig eller stedlig gjennomgang. Det er gjennomført egenrapportering fra enhetene, men ellers i praksis få kontroller. I tillegg har internrevisor gjennomført noen revisjoner på området.
[redacted]	Det stilles en rekke krav til kontroller i ledelsessystemet, og det er utarbeidet skriftlige rutiner for kontroll av forskningsprosjekter, inkludert krav om at det skal tas stikkprøver av forskningsprosjekter. Det gjennomføres få kontroller i praksis.
[redacted]	Det stilles en rekke krav til kontroller i ledelsessystemet, inkludert at det skal tas stikkprøver av forskningsprosjekter. Få av disse gjennomføres i praksis.
[redacted]	Ledelsessystemet stiller krav til revisjoner av arbeidet med informasjonssikkerhet på alle nivåer. I praksis er det gjennomført lite revisjon og kontroll, utover et par revisjoner gjennomført av internrevisor.
[redacted]	Det stilles en rekke krav til kontroller i ledelsessystemet. Få av disse gjennomføres i praksis.
[redacted]	Ledelsessystemet er ikke implementert, og utkastet stiller få krav til revisjon og kontroll, utover at det skal gjennomføres en «egenkontroll». Bortsett fra en ad-hoc-sikkerhetstest som ble gjennomført av NSM, er det ikke gjennomført kontroller eller revisjon i praksis.
[redacted]	Det stilles ikke krav til revisjon og kontroll i ledelsessystemet. Revisjon og kontroll gjennomføres heller ikke i praksis.
[redacted]	Det stilles ikke krav til revisjon og kontroll i ledelsessystemet. Revisjon og kontroll gjennomføres heller ikke i praksis.

Tabellen viser at syv av virksomhetene stiller krav til gjennomføring av evaluering og kontroll, men bare noen få virksomheter gjennomfører kontrollaktivitet i noen stor grad. Behovet for evaluering og kontroll vil naturlig nok også variere fra virksomhet til virksomhet, blant annet avhengig av organisasjonens størrelse og kompleksitet.

Noen av virksomhetene som i ledelsessystemene beskriver kontroller og sikkerhetsrevisjoner som skal gjennomføres, for eksempel [redacted], gjennomfører også en rekke kontrollaktiviteter. Enkelte virksomheter, som [redacted] stiller en rekke krav til interne kontroller i

ledelsessystemene som ikke gjennomføres i praksis. [redacted] stiller få krav til kontroll i ledelsessystemene, og revisjon og kontroll er også nærmest fraværende i praksis.

7.5.2 Det er stor variasjon i hvilke kontroller og evalueringer som er gjennomført i perioden

Vi har sett på innholdet i evalueringer og kontroller som er gjennomført i perioden.

Interne kontroller med at forskningsdata behandles i samsvar med rutiner og retningslinjer

Generelt tas det få formelle stikkprøver og gjennomføres få kontroller med at forskningsdata behandles i samsvar med rutiner og retningslinjer, men det finnes et par unntak:

- [redacted] kontrollerer 10 prosent av forskningsprosjektene årlig.
- Ved [redacted] har [redacted] laget sin egen rutine, og gjennomgår årlig et utvalg prosjekter der det er nødvendig, for å se om prosjektet gjennomføres i samsvar med lovverk, internkontrollsystemet, samt krav fra REK og Sikt.

Ingen av de andre virksomhetene tar stikkprøver. Det gjør heller ikke [redacted] som stiller eksplisitte krav om at dette skal gjennomføres i ledelsessystemene.

Enkelte virksomheter gjennomfører en årlig kartlegging ved underliggende enheter. Dette kan bidra til både å kartlegge tilstanden og bevisstgjøre ansatte ved enhetene samt å identifisere nødvendige tiltak. Følgende virksomheter gjennomfører en årlig undersøkelse ved underliggende enheter:

- [redacted]: Ledere ved hver enhet skal svare på et spørreskjema årlig. De viktigste resultatene blir samlet i et notat til ledelsen.
- [redacted]: Alle enhetene rapporterer årlig til en faggruppe for informasjonssikkerhet og personvern om kartlegging av informasjonsverdier og om sårbarheter, tiltak, risikovurderinger, organisering, personvern, og vurdering av status på området.
- [redacted]: En spørreundersøkelse for egenevaluering sendes ut til alle de organisatoriske enhetene, med spørsmål om blant annet bevissthet om systemeieransvaret, hvilke risikovurderinger som er gjennomført, og kjennskap til avvikssystemet.

Det er også noen virksomheter som har gjennomført enkeltstående spørreundersøkelser rettet mot fakulteter, institutter eller andre enheter for å kartlegge bevissthet om informasjonssikkerhet og/eller etterlevelse av regler på området.[272]

[redacted] har gjennomført seks «stedlige kontroller» i undersøkelsesperioden.[273] De kontrollerte blant annet om rutiner for personvern og informasjonssikkerhet etterleves ved enheten [redacted], og gjennomgikk informasjonssikkerheten ved klinikkdriften samt om personvernregelverket etterleves ved [redacted]. I [redacted] ledelsessystem står det også at det *kan* gjennomføres stedlige kontroller, men det er ikke gjennomført noen slike i undersøkelsesperioden.

[redacted]. I

[272] [redacted] gjennomførte en spørreundersøkelse på fakultetsnivå i 2021, hvor ledergruppene svarte på spørsmål om tilstanden og etterlevelse på området. [redacted] gjennomførte en spørreundersøkelse rettet mot ledere i 2020 som en del av arbeidet med overordnet risikoanalyse. Denne ga overordnet informasjon om ledernes oversikt over og bevissthet om informasjonsverdier ved sine enheter, samt hvordan de vurderer digitale sikkerhetsrisikoer og trusler. Ved [redacted] har administrativt personell ved to anledninger svart på spørsmål om bevissthet om systemeierskap, databehandleravtaler, risikovurderinger sikring av personopplysninger og kjennskap til avviksrutiner.

[273] Disse utføres hovedsakelig der det har vært endringer eller større saker som tilsier at kontroll er nødvendig.

tillegg gjennomførte [redacted] en gjennomgang av et utvalg prosjekter registrert hos Sikt i mai 2022, hvor det ble vurdert om informasjonsskriv og samtykkeskjema oppfylte kravene i GDPR.

Inntrengingstester og andre tekniske kontroller

Tekniske kontroller er viktig for å få kunnskap om den faktiske sikkerhetstilstanden og for å kunne identifisere nødvendige tiltak for å tette eventuelle sikkerhetshull og forbedre den tekniske sikkerheten. Følgende virksomheter har gjennomført tekniske sikkerhetsrevisjoner i undersøkelsesperioden:

[redacted]: Inntrengingstester av [redacted]

- [redacted]: Internrevisor gjennomførte en inntrengingstest av to kritiske løsninger og tjenester, herunder [redacted][275] og [redacted] klientnettverk på [redacted] (2020). I tillegg gjennomførte en ekstern konsulent inntrengingstest av nettet til [redacted] og en gjennomgang av Active Directory og klientoppsettet for Microsoft PC-er i 2021. Som del av et prosjekt for å rydde opp i lokalt driftede IT-systemer og utstyr (prosjekt [redacted]) har [redacted] også kontrollert hvordan systemeiere ivaretar krav til sikkerhet i disse systemene.
- [redacted]: Nasjonal sikkerhetsmyndighet (NSM) gjennomførte en inntrengingstest høsten 2021.
- [redacted]: En ekstern konsulent testet teknisk sikkerhet i 2018. I tillegg produserer IRT-teamet halvårlige rapporter som omtaler trusler og status for arbeidet med teknisk informasjonssikkerhet og foreslår tiltak.

Disse testene ser ut til å ha vært viktige kilder til informasjon for de nevnte virksomhetene om svakheter i tekniske sikkerhetstiltak. Ved [redacted] avdekket revisjoner [redacted], og rapportene har vært viktige i forbedringsarbeidet i etterkant sammen med kontrollene som [redacted] selv har gjennomført. Ved [redacted] avdekket NSM flere svakheter. Virksomheten har jobbet med å utbedre disse og har blant annet innført gode passordkrav.

De andre virksomhetene har ikke gjennomført tilsvarende revisjoner i perioden og har dermed begrenset kunnskap om den faktiske tilstanden.

Internrevisjon

[redacted] som inngår i undersøkelsen, har ingen internrevisjonsfunksjon.[276] [redacted] samarbeider med to andre virksomheter om **internrevisjon**, [redacted] har en egen internrevisjonsenhet, mens [redacted] har avtaler med private revisjonsfirmaer om denne funksjonen.

De fire virksomhetene som har innleid internrevisor, har fått gjennomført internrevisjon av personvern og informasjonssikkerhet. Internrevisor ved virksomhetene har gjennomført overordnede gjennomganger av arbeidet med informasjonssikkerhet og personvern for å gi styret og ledelsen en vurdering av status på området, samt utarbeidet en rekke anbefalinger.[277] Revisjonsrapportene om arbeidet med personvern og informasjonssikkerhet trekker fram som hovedanbefalinger at det må arbeides med rolleavklaring og gjennomføringsevne, og opplæring og bevisstgjøring. Ved disse fire er det også gjennomført noen andre internrevisjoner:

- Internrevisor ved [redacted] gjennomførte en gjennomgang av ledelsessystemet i 2020 og avviksoppfølging i 2019.
- Ved [redacted] har internrevisor gjennomført en kartlegging av status GDPR, samt en gjennomgang av lokale IT-systemer ved enkelte institutter i 2019.
- Ved [redacted] har internrevisor gjennomført en revisjon av tilgangsstyring i 2022.

[274] Inntrengingstesten av [redacted] ble gjennomført av eksterne konsulenter.
[275] [redacted]
[276] [redacted]
[277] Alle de fire virksomhetene har brukt PwC som internrevisor i hele eller deler av perioden. PwCs revisjoner på området er inndelt etter fem overordnede tema: Organisering roller og ansvar, styrende nivå, gjennomførende nivå, kontrollerende nivå, samt opplæring og bevisstgjøring.

- Ved [redacted] ble det også, i forbindelse med utarbeidelse av virksomhetens *Strategi for informasjonssikkerhet 2019–2021* (omtalt i kapittel 7.1.2), gjennomført en bred kartlegging av «nåsituasjonen» på informasjonssikkerhetsområdet.[278]

Ved [redacted] er det gjennomført ni revisjoner av informasjonssikkerhet og personvern i undersøkelsesperioden. Disse er mindre omfattende enn revisjonene som gjøres av innleid internrevisor. Eksempler på temaer som er gjennomgått, er tilgangsstyring, oppfølging av GDPR og internkontroll av forskningsdata som ikke omfattes av kvalitetssystem for medisinsk og helsefaglig forskning. Internrevisjonen rapporterer til styret halvårlig, og inkluderer status for implementering av tiltak for hver gjennomgang.

Ved de resterende fem virksomhetene i undersøkelsen er det ikke gjennomført noen internrevisjon av informasjonssikkerhet og personvern.

Andre gjennomganger og rapporteringer

Bortsett fra [redacted][279] har alle virksomhetene et **personvernombud.** Åtte av virksomhetene har et internt ansatt personvernombud, mens [redacted] har leid inn personvernombud.[280] Alle personvernombudene, bortsett fra ved [redacted], leverer en årsrapport. Dette er ikke en evaluering eller revisjon, men gir noe informasjon om hvordan PVO arbeider, og utviklingen på området.

Omfanget av årsrapportene varierer betydelig. Noen gir kort omtale av utvikling det siste året, utfordringer og mangler.[281] Andre rapporter er mer omfattende og inneholder informasjon om både avvikshåndtering, internkontroll, risikoområder, utfordringer og områder hvor ombudet opplever at det er behov for forbedring. De viktige forbedringsområdene som er gjennomgående i rapportene, er opplæring og bevisstgjøring, og kunnskap om hvilke regler som gjelder for avviksrapportering.

HK-dir gjennomfører årlig en kartlegging av arbeidet med informasjonssikkerhet og personvern i virksomhetene. Det gjennomføres ingen testing eller dokumentgjennomgang, og anbefalingene er basert på informasjon virksomhetene selv har oppgitt. Denne gjennomgangen er nærmere omtalt i kapittel 8.2.2.

I tillegg gjennomfører en del av virksomhetene en **ledelsens gjennomgang** årlig. Dette er ingen kontroll, men en gjennomgang av ledelsessystemet. Det er stor variasjon i både innhold, gjennomføring og rapportering fra gjennomgangen. Ledelsens gjennomgang er nærmere omtalt i kapittel 7.6.1.

7.5.3 De fleste har rutiner for melding og håndtering av avvik og hendelser innenfor informasjonssikkerhet, men det er trolig underrapportering, og de fleste har mangelfull oversikt over hendelser

Alle virksomhetene i undersøkelsen har omtale i ledelsessystemet, egne rutiner for å **melde avvik og hendelser**[282] innenfor informasjonssikkerhet/personvern og/eller publisert informasjon på brukerrettede informasjonssider på internett om melding av avvik og hendelser innenfor informasjonssikkerhet og personvern.[283] Virksomhetene har valgt ulike løsninger for melding av avvik:

[278] Denne ble ikke gjennomført av internrevisor, men av konsulent Gartner Consulting i samarbeid med ressurser fra [redacted].
[279] Det er foretatt en juridisk vurdering (av Haavind) som konkluderte med at [redacted] ikke er pålagt å ha et personvernombud.
[280] [redacted]
[281] For eksempel [redacted]
[282] **Avvik** kan defineres som brudd på lover, regler eller føringer i virksomhetenes interne dokumenter. Der virksomheten er dataansvarlig, skal avvik som innebærer brudd på personopplysningssikkerheten, som hovedregel meldes til Datatilsynet. **Informasjonssikkerhetshendelser** kan defineres som uønskede hendelser som kan medføre eller har medført brudd på konfidensialitet, integritet eller tilgjengelighet på virksomhetens informasjon. Kilde: https://www.digdir.no/informasjonssikkerhet/begrepsliste/3230#hendelser_informasjonssikkerhetsbrudd_og_avvik
[283] Syv av virksomhetene har utarbeidet egne retningslinjer/rutiner for hvordan avvik og hendelser skal håndteres, eller angitt dette i et eget kapittel i ledelsessystemet ([redacted] har egne retningslinjer, [redacted] har egne rutiner, mens [redacted] har et eget kapittel om håndtering av hendelser og avvik i ledelsessystemet) Ved to virksomheter angis det i ledelsessystemets oversikt over roller og ansvar hvem som har ansvar for håndteringen ([redacted]). Den siste virksomheten ([redacted]) opplyste å ha utarbeidet en rutine for intern avvikshåndtering med personvernbrudd i utkastet til internkontroll med personvern, men hadde ikke dokumenter som angir hvordan informasjonssikkerhetsavvik skal håndteres.

- Noen har HMS-varslingssystemer som også skal brukes til melding om avvik og hendelser innenfor informasjonssikkerhet og/eller personvern (typisk med skjema tilgjengelig på nettsiden).
- Noen har et eget meldesystem for informasjonssikkerhetsavvik.
- Ved en del virksomheter skal avvik og hendelser innenfor informasjonssikkerhet varsles per e-post.

En av virksomhetene hadde tilrettelagt for avviksmelding i et system som i praksis kun ble brukt av ansatte i administrasjonen med dedikerte roller i ledelsessystemet for informasjonssikkerhet.[284]

De fleste virksomhetene har enten utarbeidet egne rutiner for håndtering av avvik og sikkerhetshendelser eller omtaler i overordnede dokumenter i ledelsessystemet i grove trekk hvem som skal håndtere hendelser, og hvordan.[285] Avvik som gjelder personopplysningssikkerheten, skal som regel behandles av personvernombud, mens andre avvik og hendelser innenfor informasjonssikkerhet gjerne behandles av et hendelseshåndteringsteam (IRT-team) eller av andre ressurser i IT-avdelingen.

Vi har bedt alle de ti virksomhetene om å sende oss en oversikt over henholdsvis avvik og hendelser som er registrert i perioden 2019 til 2022. Videre ba vi om detaljer om hvert enkel avvik/hendelse. De tilsendte oversiktene viser at det er svært stor variasjon mellom virksomhetene i hvor mange avvik og hendelser som meldes og registreres.

Antallet registrerte **informasjonssikkerhetsavvik** følger i noen grad størrelsen på virksomhetene. [redacted] har også flest registrerte avvik (284 over en fireårsperiode), mens [redacted] få (4 ved [redacted]) eller ingen ([redacted]). Tallene er imidlertid ikke helt sammenlignbare mellom alle de ti virksomhetene. Noen har også inkludert avvik i forskningsprosjekter som er meldt inn gjennom Sikts personverntjeneste, i tillegg til avvik som ansatte og studenter melder inn.[286] Videre er det en del virksomheter som ikke skiller eksplisitt mellom avvik og hendelser i oversiktene sine.

Intervjuer og dokumentanalyse indikerer at det samlet sett trolig er en underrapportering. Denne risikoen er beskrevet av personvernombudene i flere av virksomhetene.[287] Personvernombudet ved [redacted] uttrykker for eksempel i sin årsrapport for 2021 bekymring for at det meldes inn færre avvik enn institusjonens størrelse og kompleksitet skulle tilsi. Ombudet mener det er behov for mer opplæring og informasjon til ansatte og studenter om hva som skal meldes inn, hvorfor det er viktig å melde inn, og hvordan man melder inn.[288]

Det er svært store forskjeller i hvor god oversikt virksomhetene har over **informasjonssikkerhetshendelser**. [redacted] skiller seg ut ved at de har god oversikt over hendelser, mens de øvrige virksomhetene ikke har det.

- Tilsendte oversikter fra [redacted] viser at disse har registrert flere tusen hendelser i perioden 2019–2022.[289]
- Ved [redacted] ligger antallet avvik og sikkerhetshendelser totalt sett i området 30–70 tilfeller. Ved [redacted] er antallet registrerte avvik og hendelser noe høyere, og vi ser et oppsving i antall registrerte hendelser i løpet av perioden.[290]

[284] [redacted].
[285] [redacted] hadde ikke en godkjent skriftlig rutine på undersøkelsestidspunktet, men hadde laget et utkast basert på innarbeidet praksis. [redacted] opplyste at de hadde utarbeidet et utkast.
[286] Dette gjelder [redacted]
[287] [redacted]
[288] [redacted]
[289] [redacted] bruker forskjellige systemer for oppfølging av sikkerhetshendelser og klassifiserer hendelsene på ulike måter. Tallene er derfor ikke sammenlignbare. [redacted]
[290] Den tilsendte oversikten viser at det i 2022 ble mottatt totalt 204 meldinger om avvik og sikkerhetshendelser. Dette er høyere enn de foregående årene. Mange av hendelsene er registrert av IT-avdelingen, og økningen kan knyttes til forbedringer i kapasitet til overvåking og oppfølging.

- [redacted] har ikke oversikter over sikkerhetshendelser i perioden.

Hvor god oversikt virksomhetene har, henger sammen med virksomhetenes kapasitet til å oppdage og håndtere hendelser (jf. kapittel 7.2.3). Hendelsene som er registrert, er en blanding av saker meldt inn av brukere, og hendelser som virksomhetene har fanget opp i sin sikkerhetsovervåking. Blant de vanligste hendelsene er ulike former for phishing og kompromittering av brukerkontoer.

Oversiktene til [redacted] gjør det mulig å se på ulike trender, både i antall og type sikkerhetshendelser, hvilke enheter som rammes, alvorlighetsnivå og konsekvens. Dette gir informasjon som er egnet til å vurdere endringer i trusselbilde, og effektiviteten i tekniske sikkerhetstiltak. For eksempel så [redacted] en nedgang i hendelser relatert til phishing etter å ha forbedret filtreringen av e-post. Hendelsesstatistikk fra sikkerhetsmiljøene ved [redacted] er trukket inn i HK-dirs årlige risiko- og tilstandsvurderinger av informasjonssikkerhet og personvern i sektoren.

7.6 Styrets og ledelsens oppfølging

7.6.1 Rundt halvparten av virksomhetene gjennomfører årlige gjennomganger av informasjonssikkerhet og personvern, men det er stor variasjon i hva disse inneholder, og hvor mye informasjon ledelsen får

Det er god praksis at toppledelsen gjennomgår ledelsessystemet for informasjonssikkerhet med planlagte mellomrom. **Ledelsens gjennomgang** er ment å holde ledelsen oppdatert og sikre at ledelsessystemet fungerer, og å danne grunnlag for å kunne sette inn tiltak der det er nødvendig.

Ledelsessystemene i åtte av de ti virksomhetene som inngår i undersøkelsen, sier noe om at det skal gjennomføres en ledelsens gjennomgang eller utarbeides en årlig rapport årlig om statusen for arbeidet med informasjonssikkerhet og personvern.[291] Disse virksomhetene har også rutiner for ledelsens gjennomgang, men innholdet i rutinene varierer betydelig.

Vi har undersøkt om virksomhetene har gjennomført en ledelsens gjennomgang innenfor informasjonssikkerhet i perioden 2019–2022, og om gjennomgangene inneholder sentrale momenter som status for tiltak fra tidligere gjennomganger, informasjon om informasjonssikkerhetsprestasjon, avvik og tiltak, resultater fra revisjoner og resultater fra risikovurderinger.

Syv av virksomhetene har gjennomført en form for ledelsens gjennomgang ett eller flere av årene i undersøkelsesperioden[292]. [redacted] har gjennomført dette alle årene. [redacted] gjennomførte ledelsens gjennomgang i 2019 og 2020, men ikke de to påfølgende årene. [redacted] kom i gang med dette i 2021, men fikk først i 2022 på plass en formell gjennomgang.

De øvrige tre – [redacted] – hadde ikke gjennomført en ledelsens gjennomgang i undersøkelsesperioden. Som nevnt i kapittel 7.5.3 har den sentrale sikkerhetsorganisasjonen ved [redacted] i utgangspunktet mye informasjon om avvik og sikkerhetshendelser. Data fra [redacted] om sikkerhetstruende aktivitet på internettet er en viktig kilde til informasjon i HK-dirs vurderinger av trusselbildet i sektoren som sådan. På undersøkelsestidspunktet hadde denne typen informasjon i liten grad blitt formidlet til virksomhetens øverste ledelse.

Blant dem som har gjennomført ledelsens gjennomgang, varierer *innholdet* i gjennomgangene betydelig:

[291] [redacted] hadde ikke dette kravet på undersøkelsestidspunktet, men vi er gjort oppmerksom på at [redacted] har laget en rutine for dette i etterkant.
[292] [redacted].

- Gjennomgangene ved [redacted] er relativt omfattende og inkluderer blant annet endringer i forhold som er relevante for ledelsessystemet for informasjonssikkerhet, status for arbeidet med informasjonssikkerhet, utfordringer, og informasjon om avvik og korrigerende tiltak. Som omtalt i kapittel 7.5 innhenter disse virksomhetene informasjon om tilstanden i underliggende enheter og gjennomfører internrevisjoner, og dermed har de et bedre grunnlag for å vurdere statusen for informasjonssikkerheten enn en del andre virksomheter. [redacted], rapporterer blant annet detaljerte data om sikkerhetshendelser i IT-infrastrukturen. Også ved [redacted] oppsummeres de registrerte sikkerhetshendelsene i løpet av året, og de mest alvorlige avvikene kommenteres.
- [redacted] gjennomgang følger en sjekkliste og en tiltaksplan som viser status for tiltak for foregående år.
- [redacted] gjennomgang er begrenset til en oppdatering og gjennomgang av to av dokumentene i ledelsessystemet. Det ene dokumentet er en overordnet risikovurdering som oppdateres årlig, mens det andre beskriver virksomhetens rutiner for personvern. Ledelsens gjennomgang er dermed ikke en gjennomgang av status for informasjonssikkerhetsarbeidet.

Det er noen områder som i liten grad gjennomgås i virksomhetenes gjennomganger. Særlig er det lite gjennomgang av resultater fra risikovurderinger og status for risikoreduserende tiltak. Dette kan henge sammen med at flere av virksomhetene bare i noen grad har gjennomført og dokumentert risikovurderinger, jf. omtale i kapittel 7.4. I tillegg inneholder de fleste gjennomgangene lite informasjon om resultater fra evalueringer, kontroller og revisjoner og hvordan disse er fulgt opp.

Som vist i tabell 6 i kapittel 7.1.2 varierer det også om virksomhetene har opprettet handlingsplaner/tiltaksplaner for informasjonssikkerhet, og hvordan disse er fulgt opp. Status for gjennomføring av planer for informasjonssikkerhetsarbeidet er i liten grad tatt inn i ledelsens gjennomgang, men det er et par unntak. [redacted] legger ved en statusoversikt for arbeidet med informasjonssikkerhet, som inkluderer utvikling over tid, status på eksisterende tiltak og behov for tiltak videre. [redacted] legger ved status for implementering av tiltak.

Informasjonssikkerhet og personvern tas også opp i ledermøter utenom de årlige gjennomgangene. Alle virksomhetene opplyser[293] at informasjonssikkerhet og personvern er tema i forskjellige typer ledermøter. Blant dem som skriver referat fra møtene, er det stor variasjon når det gjelder i hvilken grad informasjonssikkerhet og personvern tas opp i ledermøter og i andre fora. Syv av ti virksomheter[294] har sendt referater fra møter i rektoratet/toppledergruppen i undersøkelsesperioden. Få ser ut til å ta opp temaer relatert til informasjonssikkerhet og personvern regelmessig, og noen har kun tatt opp slike saker i et par møter i perioden. Fire virksomheter[295] har sendt møtereferater fra dekanmøte eller lignende, og også her varierer det hvor ofte temaet har vært på agendaen.

Eksempler på temaer som er tatt opp, er status for innføring av ledelsessystem for informasjonssikkerhet, informasjon om trusselbildet nasjonalt eller mer spesifikke saker som informasjon om aktiviteter i sikkerhetsmåneden eller innføring av to-faktorautentisering. Enkelte har også gått gjennom overordnede ROS-analyser.

[redacted] skiller seg ut fra de andre ved at toppledelsen har pålagt fakultetsstyrene å behandle universitetets egen årsrapport om informasjonssikkerhet og personvern. Ledelsen ved enhetene skal utarbeide og legge fram saken for fakultetsstyret, og denne skal også inkludere særskilte problemstillinger og forbedringsområder for egen enhet. Ved [redacted] har også informasjonssikkerhet og personvern vært på agendaen i en rekke møter i forskjellige ledergrupper, både dekanmøter, rektors ledermøte og administrative ledermøter.

[293] I møte, intervju eller skriftlig tilbakemelding.
[294] [redacted]
[295]

Også toppledelsen ved [redacted] involverer ledelsen ved fakultetene og andre underliggende enheter ved at de må rapportere om arbeidet med informasjonssikkerhet og personvern årlig. Dette omtalte vi i kapittel 7.5.1 *Evaluering og kontroll*.

7.6.2 Det er stor variasjon i hvor mye informasjon styrene får om arbeidet med informasjonssikkerhet og personvern

For at styret skal kunne ivareta sitt ansvar for å føre kontroll med informasjonssikkerheten og sette virksomheten i stand til å håndtere risikoen knyttet til virksomhetens informasjonsverdier, bør styret ha god nok informasjon om både status for arbeidet med informasjonssikkerhet, utfordringer, risikoarbeidet, resultater fra evalueringer, kontroller og internrevisjoner og status for tiltak.

Ved bortimot alle virksomhetene som inngår i undersøkelsen, har styrene mottatt noe informasjon om informasjonssikkerhet og personvern gjennom virksomhetenes årsrapporter, som styrene vedtar.[296] Informasjonen i årsrapportene er som regel overordnet. De fleste nevner kun kort ledelsessystemet for informasjonssikkerhet. Årsrapportene til de fire store inkluderer i tillegg i varierende grad informasjon om utfordringer, avvik og hendelser, implementerte tiltak det siste året, og/eller informasjon om gjennomførte internrevisjoner på området.

Utover dette er det stor variasjon mellom virksomhetene i hvor mye styrene får vite om informasjonssikkerhet og personvern. Seks av virksomhetene har en formulering i ledelsessystemet om at styret skal informeres årlig om arbeidet med informasjonssikkerhet og personvern.[297] Ved de resterende virksomhetene sier ledelsessystemet lite om hva styret skal informeres om.

En gjennomgang av virksomhetenes styresaker viser at de fleste styrene har fått vite status for arbeidet med informasjonssikkerhet og personvern en eller flere ganger i løpet av undersøkelsesperioden:

- Tre av styrene (ved [redacted]) har årlig mottatt en rapport fra ledelsens gjennomgang av arbeidet med informasjonssikkerhet og personvern eller andre statusoppdateringer. Styret ved [redacted] har årlig blitt informert om at det er gjennomført en sikkerhetsgjennomgang.[298]
- Styrene ved [redacted] har kun behandlet en statusgjennomgang, mens styret ved [redacted] behandlet en gjennomgang de to første årene i undersøkelsesperioden.
- Styrene ved [redacted] har ikke behandlet ledelsens gjennomgang eller andre statusrapporteringer om arbeidet med informasjonssikkerhet og personvern.

Det er stor variasjon i innholdet i statusrapporteringene. Gjennom rapporteringen fra ledelsens gjennomgang får styrene ved [redacted] vite blant annet status for arbeidet, rapporteringen fra underliggende enheter, utfordringer, avvik og korrigerende tiltak, mens styret ved [redacted] kun får en oppdatert overordnet risikovurdering og oppdatert rutinebeskrivelse på personvernområdet (jf. kapittel 7.6.1 om ledelsens gjennomgang).

I tillegg har noen virksomheter hatt andre styresaker om informasjonssikkerhet og personvern:

- Ved virksomheter hvor det er gjennomført internrevisjoner, har disse vært framlagt for styret (jf. kapittel 7.5.2).
- Styrene ved alle virksomhetene bortsett fra [redacted] har fått framlagt personvernombudets årsrapporter, enten som orienteringssaker sammen med andre typer årsrapporter, eller som

[296] Unntaket er [redacted], som først tok inn et avsnitt i 2021 etter at styret spesifikt ba om dette.
[297] [redacted]
[298] Styret får ingen skriftlig statusoppdatering, men oppdatert ROS-analyse, og deler av ledelsessystemet er vedlagt styresaken.

vedlegg til statusoppdateringer på informasjonssikkerhet og personvern. Innholdet i disse rapportene varierer betydelig (jf. kapittel 7.5.2).[299]
- Noen styrer har i tillegg hatt oppe enkelte enkeltsaker på området.[300]

Styrene ved virksomheter som har gjennomført internrevisjoner, kontroller og evalueringer (jf. kapittel 7.5.2), kartlagt status på underliggende enheter og gjennomført ledelsens gjennomgang (jf. kapittel 7.6.1), har gjennomgående fått mer informasjon om status for informasjonssikkerhetsarbeidet enn styrene ved virksomheter hvor dette ikke gjøres. Styrene ved [redacted] og [redacted] ser ut til å være best informert om informasjonssikkerhet og personvern i sine virksomheter. Disse mottar de mest omfattende statusoppdateringene/gjennomgangene, og disse inkluderer også informasjon fra kartlegginger på fakultetsnivå. I tillegg får disse styrene framlagt personvernombudenes årsrapporter og internrevisjonsrapporter.

De styrene som får minst informasjon, er de i virksomhetene hvor også ledelsen har lite informasjon fordi det ikke gjennomføres internrevisjoner, annen internkontroll eller en ledelsens gjennomgang. Ved [redacted] har styrene fått lite informasjon. Ingen av disse har gjennomført internrevisjoner på området, og der styrene har fått presentert en sak om status, inneholder presentasjonen lite informasjon om tilstanden, arbeidet med informasjonssikkerhet og utfordringer. Generelt får styrene lite informasjon om risikoarbeidet, identifisert risiko og hvordan det jobbes for å redusere risiko på området.

Det er også stor variasjon i hvor aktive styrene er. De fleste styrer tar de fleste saker kun til orientering, mens enkelte andre styrer har fattet aktive vedtak i flere saker. For eksempel har styrene ved [redacted] ved noen tilfeller gått aktivt til verks:

- [redacted]: Ved behandlingen av personvernombudets årsrapport for 2021 vedtok styret at foreslåtte tiltak skal følges opp gjennom det pågående arbeidet med å revidere [redacted] ledelsessystem for informasjonssikkerhet og personvern. Ved behandling av virksomhetens årsrapport om informasjonssikkerhet og personvern for 2021 ba styret blant annet om at [redacted] styrker arbeidet med informasjonssikkerhet ytterligere og planlegger og iverksetter sikkerhetsforbedringer, og at informasjonssikkerhet og personvern tas inn i relevant omfang som en del av internopplæring. Styret ba også om å få jevnlige orienteringer om sikkerhetsarbeid og problemstillinger som gjelder informasjonssikkerhet og personvern.
- [redacted]: Ved behandlingen av statusoppdatering for 2021 ba styret ledelsen om å arbeide med prosessen for oppfølging av de foreslåtte tiltakene. Styret har også i 2023 bedt ledelsen om å legge fram en sak som konkretiserer risikoreduserende tiltak som skal gjennomføres i 2023. Styret sluttet seg i neste styremøte til planen som ble lagt fram av administrasjonen. Planen innebar en betydelig økning i ressurser til operativ IT-sikkerhet og tekniske sikkerhetstiltak og til mer sentralisert drift og forvaltning av IT-systemer og -utstyr for forskningsmiljøer. Styret ba også om halvårlig rapportering av status for arbeidet med å styrke informasjonssikkerheten ved [redacted].

[299] [redacted] har ikke personvernombud, og ved [redacted] lager ikke ombudet en årsrapport.
[300] F.eks. saker hvor styret vedtar nytt eller endringer i ledelsessystemet for informasjonssikkerhet og personvern. Andre eksempler er [redacted], hvor styret har fått en orienteringssak om pågående og planlagte aktiviteter innen personvernområdet, og [redacted]

8 Kunnskapsdepartementets oppfølging og virkemiddelbruk

Oppsummering

- Departementet igangsatte i 2019 en fireårssatsing for å styrke informasjonssikkerheten i sektoren. Det er etablert en styringsmodell som omfatter alle departementets underliggende virksomheter innen høyere utdanning og forskning. Virksomhetene er fulgt opp gjennom etats- og eierstyringen.
- Det er også etablert et Cybersikkerhetssenter for forskning og utdanning (eduCSC) for å understøtte informasjonssikkerhetsarbeidet i virksomhetene.
- Ikke alle tiltakene departementet la opp til i informasjonssikkerhetsprogrammet, er gjennomført. Blant annet har ikke tilbudet om rådgivning og kompetanseheving blitt som planlagt, og Sikt vurderer at eduCSCs evne til å oppdage dataangrep ikke har blitt bedre i perioden.
- Heller ikke alle tiltakene i de årlige risikohåndteringsplanene på sektornivå blir gjennomført. En del av tiltakene forutsetter at Sikt/eduCSC etablerer tjenester de ikke tilbyr i dag, og at virksomhetene betaler for gjennomføringen.
- Flere virksomheter opplever at tjenestetilbudet er uklart og/eller ikke dekker deres behov, og de fire største universitetene har gått sammen om et eget sikkerhetssamarbeid.
- Departementet får informasjon om status for arbeidet i sektoren, men får lite informasjon om det faktiske sikkerhetsnivået i virksomhetene. NOKUT har fått ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren, men har ikke hatt kapasitet til å følge opp.

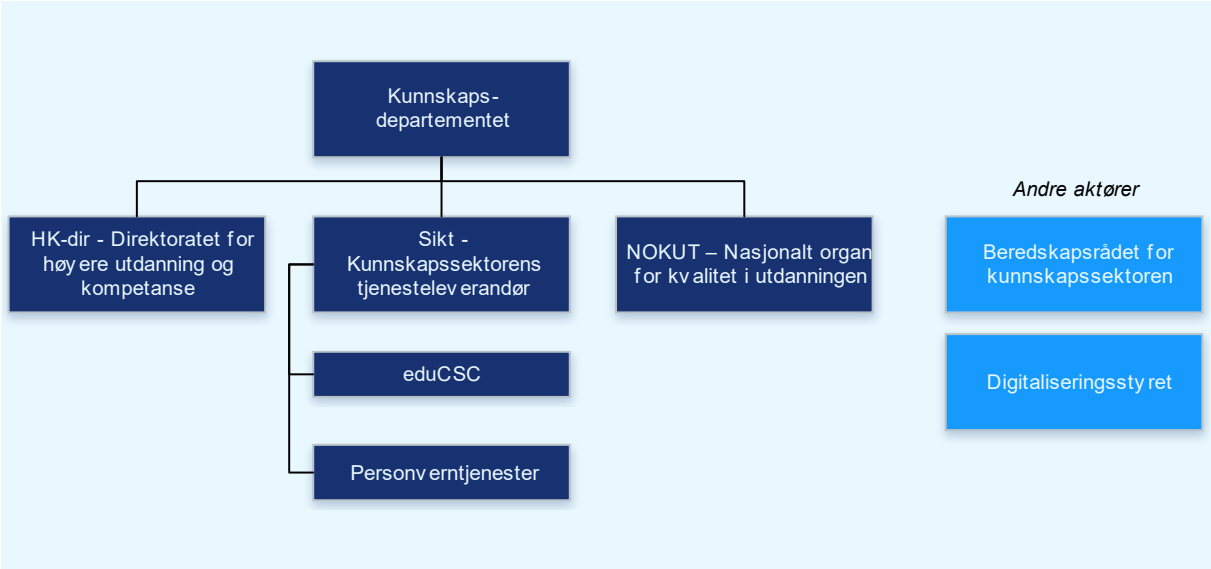
8.1 Departementets sektoransvar og virkemidler overfor virksomhetene

8.1.1 Sentrale aktører i informasjonssikkerhetsarbeidet i forskning og høyere utdanning

Kunnskapsdepartementet har det overordnede ansvaret for informasjonssikkerheten i høyere utdanning og forskningssektoren, mens den enkelte virksomhet er ansvarlig for sin egen informasjonssikkerhet.

Departementet har gitt ansvar for enkelte områder innenfor tjenesteleveranser, tilrettelegging og oppfølging av virksomhetene i sektoren til direktorater/forvaltningsorgan. I 2021/2022 ble det gjennomført en større omorganisering av sektoren. Figur 6 gir oversikt over sentrale aktører i arbeidet med informasjonssikkerhet innenfor forskning og høyere utdanning etter omorganiseringen:

Figur 6 Oversikt over sentrale aktører i informasjonssikkerhetsarbeidet



HK-dir har ansvar for den løpende styringen av informasjonssikkerhet og personvern innenfor høyere utdanning og forskning og utarbeider blant annet årlige risiko- og tilstandsvurderinger av dette. HK-dir ble opprettet 1. juli 2021. Delen av HK-dir som har ansvar for den løpende sektorstyringen av informasjonssikkerhet og personvern, lå fram til dette i det nå avviklede Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning.

Sikt er kunnskapssektorens tjenesteleverandør som utvikler, kjøper inn og leverer produkter og tjenester til utdanning og forskning. Sikt ble opprettet 1. januar 2022 gjennom en sammenslåing av NSD (Norsk senter for forskingsdata AS), Uninett AS og deler av Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning. Sikt leverer blant annet:

- **Cybersikkerhetssenter for forskning og utdanning (eduCSC)**, som er ansvarlig for å utøve rollen som sektorvist responsmiljø (SRM) for høyere utdanning og forskning, i tillegg til å være en leverandør av sikkerhetstjenester til sektoren
- **personverntjenester for forskning** (tidligere NSD – Norsk senter for forskningsdata)
- det nasjonale **forskningsnettet**, som brukes av over 150 virksomheter
- ulike tjenester som bl.a. **Feide**, den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning, og **IAM**, fellessystemet for tilgangsstyring i sektoren

Sikt eier også **Sigma2 AS**, som administrerer innkjøp og drift av nasjonalt utstyr for avanserte vitenskapelige beregninger.

NOKUT fører tilsyn med kvaliteten i norsk høyere utdanning og høyere yrkesfaglig utdanning. I tildelingsbrevet for 2021 fikk NOKUT ansvar for å føre uavhengig kontroll med om kravene til informasjonssikkerhet og personvern etterleves.

I tillegg til de tre virksomhetene som er underlagt departementet, finnes det to samarbeidsorganer for virksomheter i sektoren som er gitt ansvar som har betydning for sektorens arbeid med informasjonssikkerhet:

Digitaliseringsstyret er det øverste nivået i universitets- og høyskolesektorens **samstyringsmodell for digitalisering**. Samstyringsmodellen skal sikre styring, innflytelse og brukerinvolvering fra institusjonene, og bidra til realisering av strategi og handlingsplan for sektorens digitale omstilling samt måloppnåelse for sektormål. Under digitaliseringsstyret er det etablert tre porteføljestyrer, med ansvar

for å følge opp hver sin portefølje med underliggende produktområder.[301] Samstyringsmodellen ble etablert i 2018 og revidert i 2022. Dagens modell trådte i kraft 1. januar 2023.

Av de 21 universitetene og høyskolene er 11 representert i digitaliseringsstyret. Alle de 21 er imidlertid representert i UH-IT, som er et samarbeidsforum for IT-ledere ved universiteter. Forumet skal blant annet arbeide for at universitetene og høyskolene har en felles IT-infrastruktur og digitalt tjenestetilbud, og ha en rådgiverrolle i samstyringsmodellen for digitalisering.

Beredskapsrådet for kunnskapssektoren er etablert for å styrke arbeidet med samfunnssikkerhet og beredskap i statlige og private institusjoner. Beredskapsrådet har blant annet utarbeidet et notat om kontroll med kunnskapsoverføring (eksportkontroll) i kunnskapssektoren. Beredskapsrådets sekretariat er lokalisert ved UiS, og det er Kunnskapsdepartementet som oppnevner medlemmer til beredskapsrådet.

8.1.2 Departementets sektoransvar

Kunnskapsdepartementet har definert sitt sektoransvar innenfor **sikkerhet og beredskap** i et eget styringsdokument for sektoren.[302] Styringsdokumentet slår fast at alle departementets underliggende virksomheter og statsaksjeselskaper, samt private høyskoler, faller innenfor departementets sektoransvar.[303]

Selskaper som eies av departementets underliggende virksomheter,[304] vil ifølge styringsdokumentet også kunne regnes som en del av sektoransvaret. I styringsdokumentet står det at nivået på oppfølgingen fra departementet av slike selskaper skal vurderes i det enkelte tilfellet, blant annet basert på risiko, vesentlighet, statens andel av eierskapet, hvor mye offentlig tilskudd selskapene får, i hvilken grad de utøver oppgaver på vegne av staten, og om virksomheten deres omfatter ansvar for studenter og ansatte ved statlige institusjoner.

Departementet opplyste i intervju at det ikke er gjort noen konkrete vurderinger av departementets sektoransvar for informasjonssikkerhet for aksjeselskaper som er hel- eller deleid av departementets underliggende virksomheter. Dette dreier seg blant annet om selskapene NTNU Technology Transfer AS[305], NTNU Samfunnsforskning AS[306], Inven2 AS[307] og NORCE Norwegian Research Centre AS[308].

Forskningsinstitutter som mottar basisfinansiering over Kunnskapsdepartementets eller andre departementers budsjetter, ble definert utenfor departementets sektoransvar i departementets *Risiko- og sårbarhetsanalyse av Kunnskapsdepartementets sektor 2020*. Departementet opplyser imidlertid at spørsmålet om departementets sektoransvar er under utvikling ettersom den sikkerhetspolitiske situasjonen har endret seg. Departementet har et ansvar for forskningspolitikk som også omfatter disse instituttene, og sikkerhet inngår i økende grad i dette arbeidet. Departementet påpeker at det er viktig å se hen til hvordan situasjonen er for instituttsektoren ved vurderinger av trusselbildet og sikkerhetssituasjonen i sektoren.

Departementet har også et ansvar for **forebyggende sikkerhetsarbeid** innenfor sitt ansvarsområde, jf. sikkerhetsloven. Dette ansvaret innebærer blant annet å identifisere og holde oversikt over

[301] De tre underliggende «produktområdene» er: Utdanning og administrasjon, Forskning og kunnskapsressurser, og Data og infrastruktur.
[302] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor.
[303] I tillegg er hele barnehage- og opplæringssektoren uavhengig av eierskap, de private fagskolene og studentsamskipnadene definert innenfor departementets sektoransvar. Disse virksomhetene er ikke relevante for denne undersøkelsen.
[304] Slik som teknologioverføringsselskaper eller forskningsinstitusjoner eid av universitetene
[305] Heleid av staten med NTNU som største eier.
[306] Heleid av NTNU.
[307] Heleid av staten med UiO og Oslo universitetssykehus som like store eiere.
[308] UiB er største eier (51,8 prosent), UiT er en mindre aksjonær (3,2 prosent), og to andre universiteter er inne på eiersiden men via holdingselskaper (UiS gjennom Stavanger Research Holding AS og Universitetet i Agder gjennom Agder Research Holding). Det er også noen små private eiere (4,2 prosent).

grunnleggende nasjonale funksjoner (GNF)[309] innenfor sine ansvarsområder samt over virksomheter som har vesentlig betydning for slike funksjoner eller for nasjonale sikkerhetsinteresser.[310]

På NSMs oversikt over innmeldte grunnleggende nasjonale funksjoner er det kun «Kunnskapsdepartementets virksomhet, handlefrihet og beslutningsdyktighet» som er ført opp. Departementet opplyser at det pågår en prosess med å avgjøre om det skal utpekes andre grunnleggende nasjonale funksjoner (GNF) innenfor departementets ansvarsområde. Videre opplyser departementet at det foregår en kartlegging av virksomheter som har betydning for en eventuell ny GNF eller som har vesentlig betydning for nasjonal sikkerhet.

8.2 Departementets styring og oppfølging av informasjonssikkerheten i sektoren

8.2.1 Departementet igangsatte i 2019 en fireårig satsing for å styrke informasjonssikkerheten i sektoren

Kunnskapsdepartementet igangsatte i 2019 et fireårig informasjonssikkerhetsprogram i universitets- og høyskolesektoren. Målet med programmet var å styrke informasjonssikkerheten i sektoren og forbedre evnen til å forebygge og håndtere trusler mot forskningsnettet.[311] Stortinget har bevilget totalt 70 millioner kroner til programmet fordelt over tre år.[312] Programmet inneholdt tre prosjekter:

1. **Styringsmodell for informasjonssikkerhet og personvern:** Unit (senere HK-dir) fikk ansvar for den løpende sektorstyringen av informasjonssikkerhet og personvern i departementets underliggende virksomheter. De ble bedt om å implementere en ny styringsmodell for informasjonssikkerhet og personvern, forvalte styringsmodellen og rapportere til departementet.
2. **Analysesenter og responsmiljø:** Uninett AS (senere Sikt) fikk i oppdrag å forbedre deteksjons- og analysekapasiteten i sektoren, ta rollen som sektorens responsmiljø og forbedre sektorens evne til å håndtere trusler.
3. **Rådgivningstjenester og kompetanseheving:** I tillegg fikk Uninett AS (senere Sikt) ansvar for å etablere rådgivningstjenester for implementering og helhetlig praktisering av ledelsessystemer for informasjonssikkerhet, samt å etablere et program for kompetanseheving innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte.

Prosjekt 2 og 3 er rettet mot å understøtte arbeidet med informasjonssikkerhet i virksomhetene.

Styringsdokumentet for programmet ble vedtatt av Digitaliseringsstyret for høyere utdanning og forskning i april 2019.[313]

[309] GNF defineres i § 1-5 i loven som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.»
[310] Sikkerhetsloven § 2-1.
[311] Prop. 1 S (2018–2019).
[312] I tildelingsbrevene fra Unit til Uninett AS for 2019, 2020 og 2021 tildelte Unit årlig 12,5 millioner kroner videre til Uninett for gjennomføring av de to prosjektene de fikk ansvar for. For 2022 tildelte Kunnskapsdepartementet de siste 12,5 millioner kronene for disse to prosjektene til Sikt. 5 millioner kroner årlig ble brukt på styringsmodellprosjektet. For 2023 bevilget Kunnskapsdepartementet 3,8 millioner kroner til arbeidet med styringsmodell for informasjonssikkerhet.
[313] Sak 21/19.

8.2.2 Departementet har etablert en styringsmodell for informasjonssikkerhet

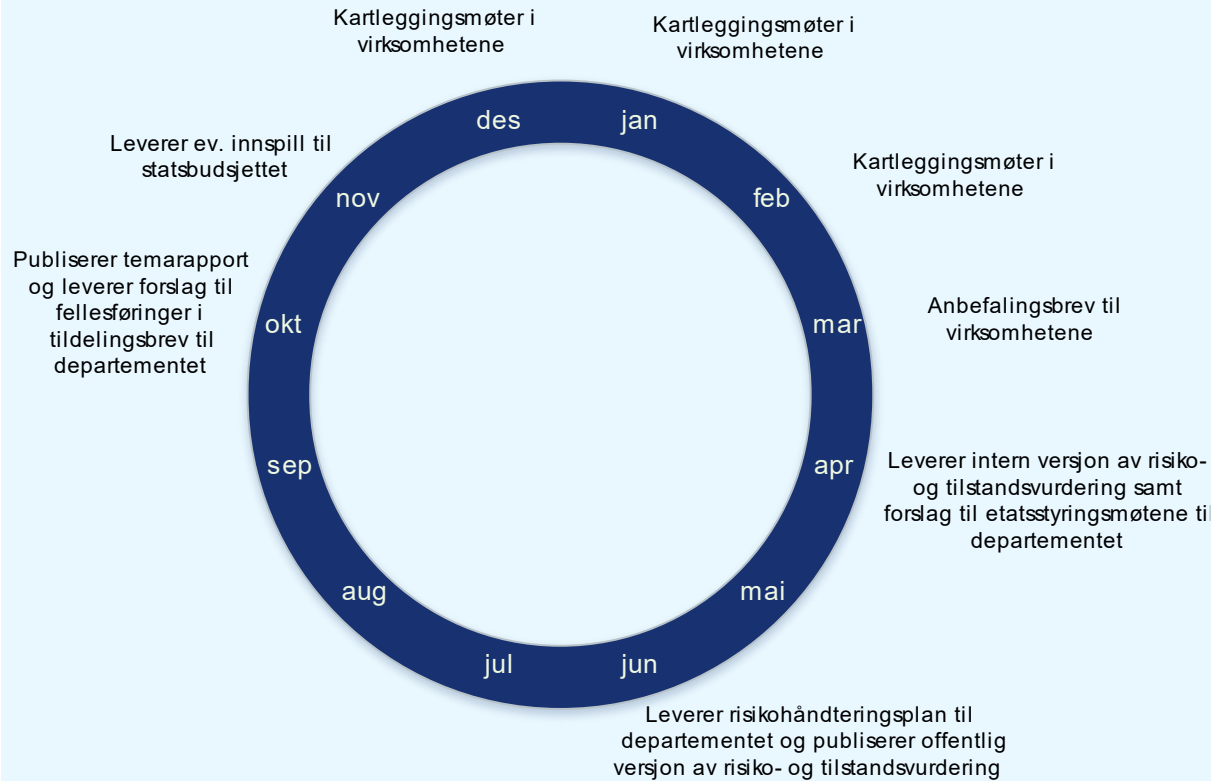
Rammene for styringsmodellen er beskrevet i *Oversikt over Kunnskapsdepartementets styringsmodell for informasjonssikkerhet*.[314] Dokumentet definerer Kunnskapsdepartementets og HK-dirs roller og slår fast seks prinsipper som skal legges til grunn for styringen:[315]

- etablere informasjonssikkerhet som omfatter hele sektoren
- anta en risikobasert tilnærming (at beslutninger om styring av informasjonssikkerhet skal bygge på risikovurderinger, og at sikkerhetsnivået skal bestemmes ut fra en organisasjons risikoaksept)
- gi retning til investeringsbeslutninger
- sikre etterlevelse av interne og eksterne krav
- skape et miljø som er positivt til sikkerhet
- vurdere gjennomføringsevnen opp mot mål

Det er utarbeidet et årshjul i styringsmodellen med faste årlige aktiviteter. HK-dir har flere leveranser gjennom året, både til departementet og virksomhetene (se illustrasjon nedenfor). Den største leveransen fra HK-dir er den årlige risiko- og tilstandsvurderingen av informasjonssikkerhet og personvern i sektoren. Den første risiko- og tilstandsvurderingen ble publisert i 2019.[316] HK-dir utarbeider også forslag til risikohåndteringsplan på sektornivå samt temarapporter som utdyper tilstanden i sektoren innenfor utvalgte områder.[317]

[314] https://cdn.sanity.io/files/dc7vgrwe/production/c804d08e83024848b4a5f6c1be3ce0175999e560.pdf?dl
[315] Styringsmodellen er basert på ISO/IEC 27014:2013.
[316] Den første risiko- og tilstandsvurderingen omfattet 21 universiteter og høyskoler. Fra og med 2020 har risiko- og tilstandsvurderingene også inkludert de øvrige virksomhetene som er omfattet av styringsmodellen.
[317] Hittil er fem temarapporter publisert: *Temarapport 2020: Tjenesteutsetting av digitale systemer og tjenester*; *Temarapport 2020: Kontinuitet, beredskap og øvelser*; *Temarapport 2021: Pandemihåndteringen og betydningen for arbeidet med informasjonssikkerhet og personvern i UH-sektoren*; *Temarapport 2021: Ledelsens styring og kontroll av arbeidet med informasjonssikkerhet*; og *Temarapport 2022: Praktisering av krav til informasjonssikkerhet og personvern*.

Figur 7 Årshjul i styringsmodell for informasjonssikkerhet – HK dirs aktiviteter og leveranser



Kilde: Årshjul for Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.

Styringsmodellen innebærer at HK-dir har fått et ansvar for sektorstyringen innenfor informasjonssikkerhet og personvern og skal blant annet følge opp til sammen 28 virksomheter:

- de 21 statlige universitetene og høyskolene
- Norges forskningsråd (NFR)
- de nasjonale forskningsetiske komiteene (FEK)
- NOKUT – Nasjonalt organ for kvalitet i utdanninga
- NUPI – Norsk utenrikspolitisk institutt
- Simula Research Laboratory AS
- UNIS
- Sikt – Kunnskapssektorens tjenesteleverandør

Alle disse virksomhetene er direkte underlagt Kunnskapsdepartementet. HK-dir omfattes også av sektorstyringen. Det er KD som følger opp direktoratets eget arbeid med informasjonssikkerhet og personvern.[318]

Sentralt i styringsmodellen er dokumentet *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*. Policyen sammenfatter de overordnede kravene til virksomhetene på området med utgangspunkt i lovpålagte krav og nasjonale føringer gitt av regjeringen (se faktaboks).

[318] I 2022 ble det gjennomført en ekstern modenhetsvurdering av HK-dirs arbeid med informasjonssikkerhet og personvern. Kilde: Intervju med Kunnskapsdepartementet.

Faktaboks 16 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning

Policyen for informasjonssikkerhet og personvern i høyere utdanning og forskning ble utarbeidet av Unit (senere HK-dir) og fastsatt av departementet i rundskriv F-04-20 1. oktober 2020.

Policyen sammenfatter de overordnede kravene til virksomhetene på området, og tar utgangspunkt i lovpålagte krav og nasjonale føringer gitt av regjeringen. Ifølge policyen skal virksomhetene

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

Kilde: *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*, fastsatt av Kunnskapsdepartementet i rundskriv F-04-20 1. oktober 2020.

Et prinsipp i styringsmodellen er at det også skal etableres informasjonssikkerhet som omfatter hele sektoren.[319] I dette ligger det at også private høyskoler kan følges opp gjennom tilskuddsforvaltning og dialog med departementet, i tråd med departementets vurdering av sektoransvaret overfor disse virksomhetene under samfunnssikkerhetsinstruksen.

HK-dirs kartlegginger i virksomhetene

Som ledd i sektorstyringen gjennomfører HK-dir årlige kartlegginger av hvordan de 28 virksomhetene arbeider med informasjonssikkerhet og personvern. I forkant av kartleggingsmøtene sender HK-dir brev til virksomhetene med spørsmål om arbeidet med informasjonssikkerhet og personvern. Deretter avholder direktoratet møter med den enkelte virksomhet. I møtene redegjør virksomhetene for sin egen oppfatning av status på informasjonssikkerhetsområdet med utgangspunkt i spørsmålene og kravene i policyen. Se faktaboks for en oversikt over hvilke temaer som ble kartlagt i 2023.

På bakgrunn av virksomhetenes svar i kartleggingsmøtene vurderer HK-dir etterlevelsen av kravene i policyen og sender anbefalingsbrev til hver virksomhet.[320] Første runde med kartleggingsmøter i virksomhetene ble gjennomført i 2019.

Videre utarbeider HK-dir forslag til konkrete tilbakemeldinger som departementet kan bruke i styringen av virksomhetene. HK-dir leverer også forslag til fellesføringer som departementet kan bruke i sine tildelingsbrev til virksomhetene påfølgende år.

[319] Sikt. (u.å.). *Oversikt over Kunnskapsdepartementets styringsmodell for informasjonssikkerhet. https://cdn.sanity.io/files/dc7vqrwe/production/c804d08e83024848b4a5f6c1be3ce0175999e560.pdf*

[320] I brevet oppsummerer HK-dir sin vurdering av virksomhetens arbeid med informasjonssikkerhet og personvern i foregående år og kommer med anbefalinger til det videre arbeidet. Anbefalingene er relativt overordnede, som å styrke risikostyringen og å ta i bruk, ferdigstille eller innføre ledelsessystemet. De fleste virksomhetene har også fått anbefalinger som omhandler opplæring og kompetanseheving.

Faktaboks 17 Temaer i kartleggingsmøte mellom HK-dir og virksomhetene i 2023

I kartleggingsmøtene mellom HK-dir og de 28 virksomhetene i 2023 ble følgende temaer kartlagt:

- ressurser øremerket til arbeidet med informasjonssikkerhet og personvern
- oversikt over informasjonsverdier
- brudd og avvik på informasjonssikkerhet og personvern
- sårbarheter
- status for etterlevelse av personopplysningsloven og nye tiltak
- status for innføring og praktisering av ledelsessystemet for informasjonssikkerhet,
- risikostyring og risikovurderinger og innføring av sikringstiltak
- tiltak for å oppdage og håndtere uønskede informasjonssikkerhets- og personvernhendelser
- virksomhetens kontinuitet -og beredskapsplan
- hvilke temaer som blir behandlet i virksomhetens ledelsens gjennomgang

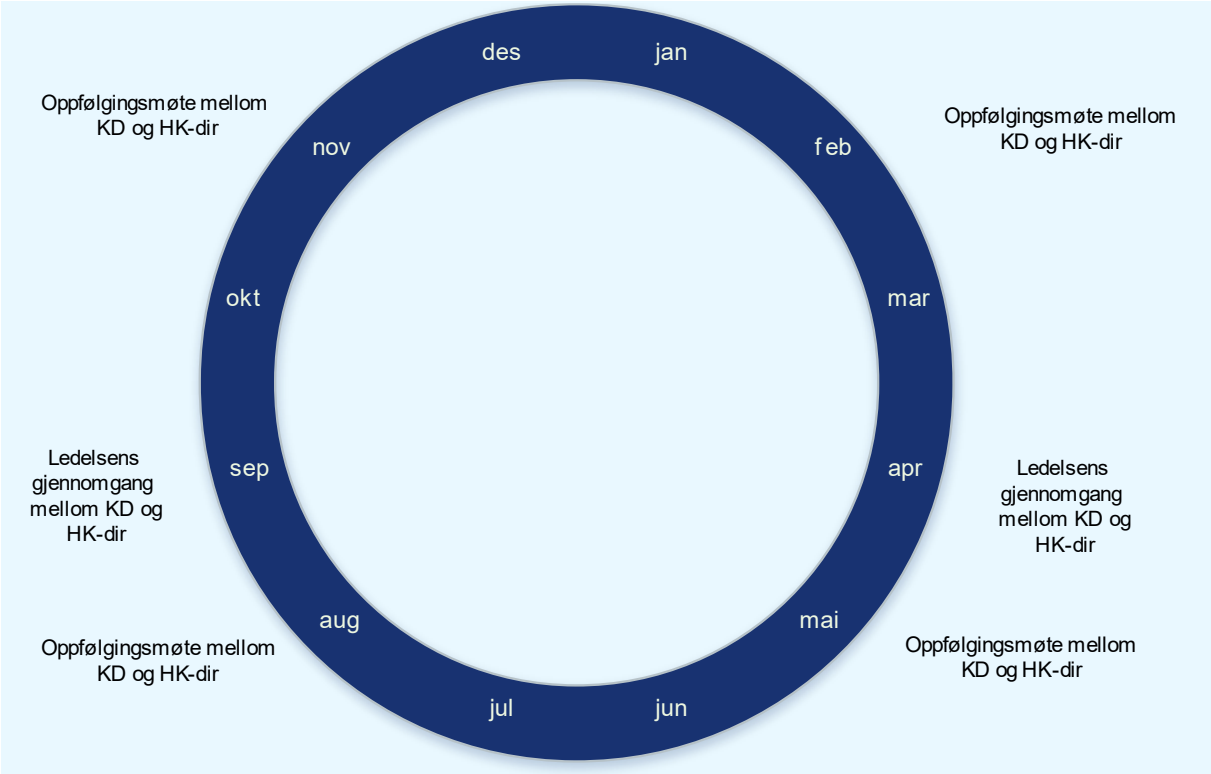
Kilde: Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2023.

En del av virksomhetene som er undersøkt, oppgir i intervju at de har hatt nytte av HK-dirs kartlegging, og at den har bidratt til å rette virksomhetenes oppmerksomhet mot informasjonssikkerhet og stake ut en kurs for deres videre arbeid. Dette er særlig tilfellet for de minste virksomhetene. Andre opplever at kartleggingen er mindre nyttig, og påpeker at siden den i hovedsak er basert på virksomhetenes egenrapportering, sier den ikke nødvendigvis så mye om hva som faktisk er status for arbeidet med informasjonssikkerhet og personvern. Videre påpeker flere virksomheter at gjennomgangene er for generelle, og at rådene er vanskelige å følge opp, og etterlyser mer praktiske og konkrete råd og veiledninger.

Møtepunkter mellom HK-dir og Kunnskapsdepartementet

Ifølge årshjulet skal det avholdes kvartalsvise oppfølgingsmøter mellom HK-dir og departementet på operativt nivå samt halvårlige møter med en «ledelsens gjennomgang» av styringsmodellen på ledernivå (se illustrasjon nedenfor).

Figur 8 Møtepunkter mellom HK-dir og Kunnskapsdepartementet



Kilde: Årshjul for Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.

Den første «ledelsens gjennomgang» ble gjennomført i september 2019. I ledelsens gjennomgang gjennomgås blant annet årets risiko- og tilstandsvurdering samt oppnådde resultater. Gjennomgangene omfatter også oppfølging av risikostyringen og risikohåndteringsplanene som HK-dir årlig utarbeider for sektoren, samt budsjettinnspill.

Departementet opplyser at ledelsens gjennomgang er en viktig arena for å sikre at toppledelsen i HK-dir og ledelsen i Kunnskapsdepartementets avdeling for eierskap i høyere utdanning og forskning får lik situasjonsforståelse og samme faktagrunnlag og kan diskutere status og vurderinger for det videre arbeidet. Videre mener departementet at faste møtepunkter bidrar til å forbedre strukturen og prosessen, til å bevisstgjøre om forhold oppover i systemet i både departementet og HK-dir og til å forankre arbeidet.

Både intervjuet med HK-dir og intervjuet med Sikt tyder på at det gjenstår noen utfordringer i samarbeidet mellom Kunnskapsdepartementet, HK-dir og Sikt. Sikt har fram til september 2023 ikke deltatt i ledelsens gjennomgang,[321] og departementet har ikke hatt noen andre direkte møtepunkter med Sikt hvor informasjonssikkerheten i sektoren tas opp, selv om Sikt nå er direkte underlagt Kunnskapsdepartementet på samme måte som HK-dir.[322] Da informasjonssikkerhetsprogrammet ble igangsatt, eide Unit (nå HK-dir) Uninett AS, som i dag er videreført i Sikt.

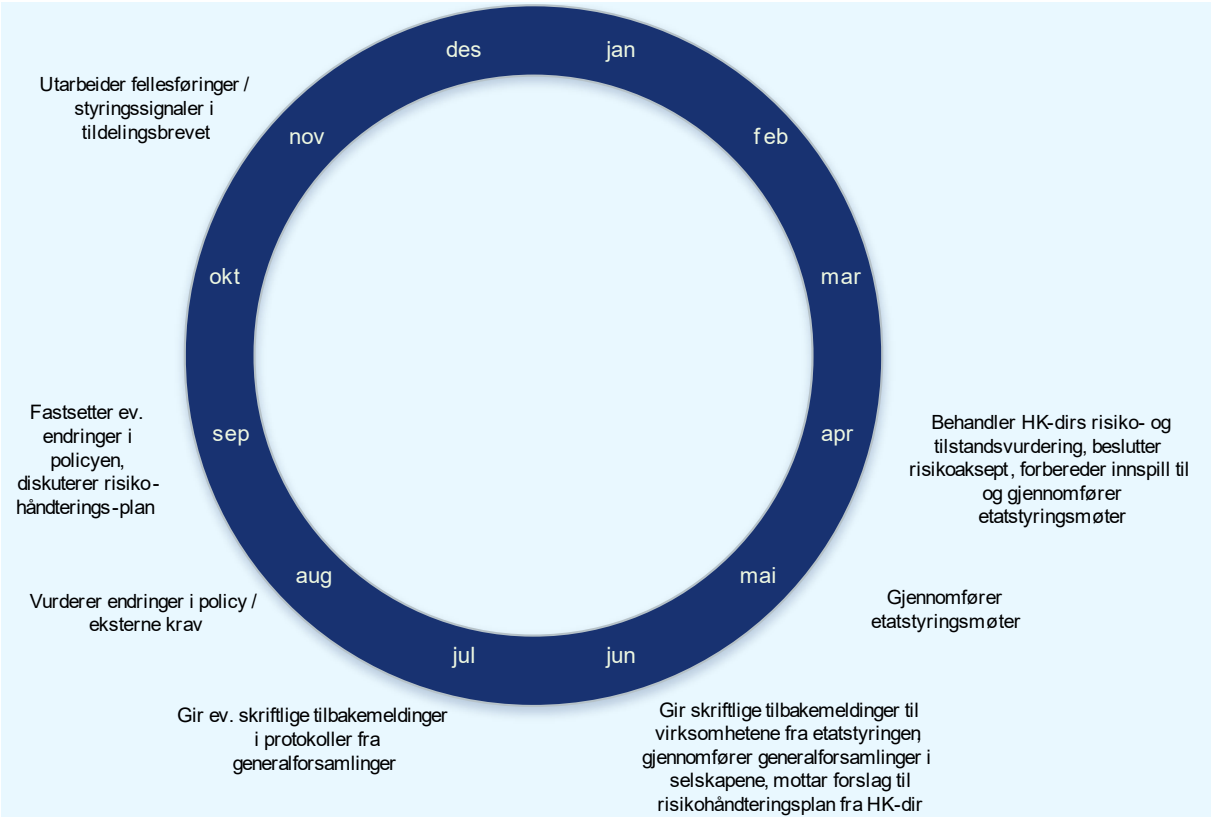
Selv om Sikt er likestilt med HK-dir etter omorganiseringen, er det fortsatt et hierarki i styringsmodellen, og Kunnskapsdepartementet har ikke forholdt seg direkte til Sikt på dette området.[323] Sikt mener det er positivt at omorganiseringen i sektoren har gjort virksomheten til en ren tjenesteleverandør, og at denne rollen er skilt fra direktorats-/myndighetsrollen. Departementet påpeker at dagens struktur i sektoren fortsatt er relativt ny, og at det er naturlig at man justerer styringsmodellen underveis.

[321] Kunnskapsdepartementet opplyser at Sikt deltok som observatør med talerett på ledelsens gjennomgang for første gang 29. september 2023.
[322] Intervju med Kunnskapsdepartementet.
[323] Intervju med HK-dir.

Departementet følger opp underliggende virksomheter gjennom etats- og eierstyringen

Departementet har etablert interne prosesser for å innarbeide fellesføringer i tildelingsbrev til virksomhetene, samt for å stille krav til den enkelte virksomhet i de årlige etatsstyringsmøtene og/eller i tilbakemeldingsbrev, samt føringer i generalforsamlinger i selskapene (se illustrasjon nedenfor).

Figur 9 Departementets prosesser med å forberede krav til virksomhetene om informasjonssikkerhet og personvern



Kilde: Årshjul for Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.

Fra 2020 har departementet gitt muntlige og skriftlige tilbakemeldinger til virksomhetene i forbindelse med etatsstyringsmøtene, basert på HK-dirs rapportering.

Departementet opplyser at denne praksisen ble justert i 2023. Fra da av har departementet valgt hvilke temaer som skal følges opp i etatsstyringsmøtet med den den enkelte virksomhet, basert på risiko og vesentlighet. Dette innebærer at departementet har definert et sett med kriterier for når virksomhetene skal motta føringer om informasjonssikkerhet og personvern i etatsstyringsmøtet.[324] Departementet opplyste at alle unntatt fem virksomheter mottok skriftlige og/eller muntlige tilbakemeldinger om temaet i årets etatsstyringsmøter.

Departementet har gitt føringer til sine underliggende selskaper, men ikke uttrykt forventninger om hvordan universiteter og høyskoler skal følge opp informasjonssikkerheten i selskapene de eier

De heleide selskapene, som er direkte eid av departementet, Universitetssenteret på Svalbard AS (UNIS) og Simula Research Laboratory AS (Simula) har ikke mottatt krav til informasjonssikkerhet og

[324] Blant annet om HK-dir vurderer det som «ikke sannsynlig» at virksomheten etterlever kravene i policyen, om etterlevelsen ikke er forbedret siden forrige gjennomføring, og om virksomhetens kontinuitet og beredskap er mangelfull.

personvern i sine tilskuddsbrev. Til gjengjeld har de mottatt informasjon om departementets forventninger i generalforsamling i 2020.[325]

I forbindelse med Units årlige risikovurdering av informasjonssikkerheten og personvernet ble det avdekket et behov for å kommunisere departementets forventninger tydeligere overfor selskapene. Dette kom fram i et internt notat som departementet utarbeidet før gjennomføringen av generalforsamlingene med de heleide selskapene i 2020. Ifølge notatet hadde ikke Unit lyktes med å få i stand en dialog med UNIS. Som følge av dette tok departementet inn en egen sak om informasjonssikkerhet og personvern i generalforsamling med UNIS avholdt i juli 2020. Overfor Simula presiserte departementet sine forventninger under sak om godkjenning av årsregnskap og årsberetning.[326]

Departementet gjennomfører også kontaktmøter med selskapene, som avholdes i tilknytning til generalforsamlingene. Kontaktmøtene er ikke et styringsvirkemiddel. Departementet opplyser at informasjonssikkerhet og personvern ikke har vært tema i departementets kontaktmøter med selskapene med unntak av i kontaktmøtet med UNIS i 2022.

Til sammenligning har ikke departementet uttrykt eksplisitte forventninger til hvordan eierinstitusjonene skal følge opp selskaper de eier, på informasjonssikkerhetsområdet. Departementet opplyser at de generelt har valgt å ikke styre gjennom å uttrykke særskilte forventninger til de underliggende virksomhetene om hvordan de skal følge opp interne regler i selskaper de har eierskap i. Departementet forventer imidlertid på generelt grunnlag at eierinstitusjonene utøver sitt eierskap på en god måte, og at de etterlever gjeldende lover og krav. Departementet viser i den forbindelse til *Reglement for økonomistyring i staten* §10[327], og prinsippene som skisseres i Meld. St. 19 (2020-2021) *Styring av statlige universiteter og høyskoler* som blant annet sier at Kunnskapsdepartementet skal «styre i det store og ikke i det små» og at styringen skal være strategisk og overordnet.

Vi har bedt tre universiteter redegjøre for eventuelle føringer eller forventninger de har gitt til selskaper de eier. Verken NTNU, som blant annet eier NTNU Technology Transfer AS, UiO, som eier 50 prosent av Inven2 AS, eller UiB, som eier over 50 prosent av NORCE Norwegian Research Centre AS, har stilt krav eller uttrykt forventninger til informasjonssikkerhetsarbeidet i eierdialogen sin med virksomhetene.[328] UiB viser i skriftlig svar om universitetets eierstyring av NORCE at temaet er viktig, og at de vil ta dette med seg i innretning av eierdialog framover.

Departementet gir anbefalinger til private høyskoler gjennom tilskuddsbrev

Departementet har også gitt anbefalinger til private høyskoler gjennom tilskuddsbrevene.[329] Dette er i tråd med prinsippet om at det skal etableres informasjonssikkerhet i hele sektoren, samt føringer som gis i departementets styringsdokument for arbeidet med sikkerhet og beredskap.[330]

En gjennomgang av tilskuddsbrevet til de private høyskolene for perioden 2019–2022 viser at departementet har gitt anbefalinger på de samme områdene som de har stilt krav til universitetene og høyskolene. Eksempelvis stilte departementet i tildelingsbrev til de statlige universiteter og høyskoler for 2022 krav om at *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning* skal ligge til grunn for virksomhetens arbeid med informasjonssikkerhet og personvern.

[325] Selskapene mottok også, i likhet med de øvrige virksomhetene, brev fra statsråden datert 07.01.2019 om innføringen av styringsmodellen og at de er omfattet av den, samt rundskriv F-04-20 med policyen for informasjonssikkerhet og personvern, hvor det framgikk at policyen også gjelder for dem.
[326] Generalforsamling avholdt juli 2020.
[327] Det heter blant annet at «utøvelsen (…) av eierskapet skal understøtte en klar fordeling av myndighet og ansvar mellom eier og styret».
[328] NTNU Technology Transfer og Inven2 bruker henholdsvis NTNU og UiO (eierne) som nettverksleverandør og har i den forbindelse direkte avtaler med disse som gir noen føringer.
[329] I 2023 fikk følgende private høyskoler tilskudd fra Kunnskapsdepartementet: Ansgar høyskole; Barratt Due musikkinstitutt; Bergen Arkitekthøgskole; Dronning Mauds Minne Høgskole for barnehagelærerutdanning; Fjellhaug Internasjonale Høgskole; Handelshøyskolen BI; Høgskulen for grøn utvikling; Høyskolen for dansekunst; Høyskolen for ledelse og teologi; Høyskolen Kristiania; Lovisenberg diakonale høgskole; MF vitenskapelig høyskole; NLA Høgskolen; Steinerhøyskolen; og VID vitenskapelig høgskole
[330] Styringsdokumentet slår fast at virksomheter som er omfattet av departementets sektoransvar innenfor sikkerhet og beredskap, men som faller utenfor styringsmodellen (slik som private høyskoler), skal oppfordres til å oppfylle de overordnede kravene beskrevet i policyen.

Tilskuddsbrevet til de private høyskolene inneholdt samme formulering bortsett fra at «skal» var erstattet med «bør».

Departementet opplyste at det gjennomføres årlige kontaktmøter med utvalgte private høyskoler på bakgrunn av risiko og vesentlighet, men at informasjonssikkerhet og personvern ikke har vært tema i slike møter.

8.2.3 Det utarbeides årlige risikohåndteringsplaner med tiltak som bare i noen grad gjennomføres

En sentral leveranse fra HK-dir gjennom styringsmodellen er risikohåndteringsplaner med forslag til tiltak for å håndtere risikoen på sektornivå. Risikohåndteringsplanene vedtas av Kunnskapsdepartementet.[331]

Den første risikohåndteringsplanen fra HK-dir ble levert i 2020, og deretter er det utarbeidet planer for 2021–2022 og 2022–2023.[332] Forslag til risikohåndteringsplan for 2023–2024 ble bestilt med leveranse 30. juni 2023.

Vi har gjennomgått forslag til risikohåndteringsplan for 2021–2022 og 2022–2023. Gjennomgangen viser at det i all hovedsak er HK-dir og Sikt som står oppført som ansvarlig for å følge opp tiltakene i risikohåndteringsplanene. Sikt har ansvar for flertallet av tiltakene:

- Risikohåndteringsplanen for 2021–2022 inneholdt til sammen 21 etablerte og foreslåtte tiltak, hvorav Sikt stod oppført som ansvarlig for 11 alene og 3 i samarbeid med andre.
- Risikohåndteringsplanen for 2022–2023 inneholdt til sammen 14 tiltak, hvorav Sikt stod oppført som ansvarlig for 10 alene, og 2 i samarbeid med andre. I tillegg er ytterligere 3 tiltak beskrevet, hvorav 2 av dem berører Sikt.

Eksempler på foreslåtte tiltak som risikohåndteringsplanen for 2022–2023 gir Sikt ansvar for, er å gjennomføre sårbarhets- og inntrengingstesting, å tilby rådgivning og veiledning tilpasset den enkelte institusjon eller virksomhet og å gjennomføre revisjoner av arbeidet med informasjonssikkerhet og personvern hos den enkelte virksomhet.

Både disse og flere av de andre tiltakene i risikohåndteringsplanen forutsetter i imidlertid i praksis at Sikt/eduCSC etablerer tjenester de ikke tilbyr i dag, og at virksomhetene betaler for gjennomføringen. Dette gjør at mange av tiltakene som HK-dir mener ville hevet sikkerhetsnivået i sektoren, ikke gjennomføres. HK-dir poengterte i intervju at flere av tiltakene som er lagt til Sikt/eduCSC, ble utarbeidet i programperioden mens tjenestene og eduCSC var under etablering og hadde finansiering gjennom fireårssatsingen.

Sikt opplyser at eduCSC utfører tiltakene i risikohåndteringsplanene etter beste evne, men at noen av tiltakene ikke blir utført i ønsket grad som følge av at eduCSC mangler kapasitet eller kompetanse, eller som følge av manglende betalingsvilje hos eduCSCs kunder.[333] Blant tiltakene som ikke har blitt prioritert, er rådgivning og inntrengingstesting. Dette utdypes nærmere nedenfor og i kapittel 8.3.

eduCSC får ikke innsyn i tilstandsvurderingen for den enkelte virksomhet, og Sikt er ikke involvert i arbeidet med å definere sektortiltak. Sikt påpeker i intervju at det kun er gjennom risikohåndteringsplanene at eduCSC har fått vite hvilke anbefalinger HK-dir vil gi, og hvilke tiltak direktoratet har foreslått at Sikt skal ha ansvar for. Sikt mener at dersom de hadde vært mer involvert i utarbeidelsen av sektortiltak, kunne det kanskje resultert i andre tiltak. Sikt mener det er ryddig at

[331] Forslag til risikohåndteringsplan leveres i henhold til årshjulet til departementet i juni. Deretter diskuteres planen i ledelsens gjennomgang i september. Etter dette behandler departementet planen i avdeling for eierskap i høyere utdanning og forskning, og sender brev tilbake til HK-dir med resultatet av behandlingen og departementets eventuelle innspill.
[332] Intervju med departementet.
[333] Svar på skriftlige spørsmål fra Sikt datert 10. mars 2023.

eduCSC ikke definerer tiltakene, men at Sikt i større grad enn i dag bør ta del i dialogen om hvilke tiltak som er viktigst, og hvilke som er realistiske.

Departementet opplyser at det kan være aktuelt å trekke Sikt mer inn i arbeidet med å utarbeide risikohåndteringsplaner enn før. Departementet erkjenner at det kan være uheldig at en virksomhet (HK-dir) peker på en rekke tiltak en annen virksomhet (Sikt) skal gjennomføre, uten å ha noen myndighet til å bestemme.

8.2.4 Departementet har sørget for et rammeverk for håndtering av IT-sikkerhetshendelser i UH-sektoren

NSM har etablert et rammeverk for håndtering av IT-sikkerhetshendelser, og Kunnskapsdepartementet har gitt HK-dir ansvar for å gjennomføre rammeverket i sektoren.

HK-dir (den gang Unit) har utarbeidet en sektortilpasning av NSMs rammeverk og pekt på sektorspesifikke myndigheter, etater og organer og deres rolle i hendelseshåndtering i tråd med NSMs rammeverk.[334] Rammeverket gjelder for alle departementets underliggende virksomheter i høyere utdanning og forskning, og fra 2022 også for Statsped og Utdanningsdirektoratet.[335] I tråd med føringer gitt blant annet i NSMs rammeverk[336] har HK-dir (den gang Unit) utpekt eduCSC (den gang Uninett CERT) som sektorvist responsmiljø for virksomhetene som er omfattet av rammeverket. Som sektorvist responsmiljø skal eduCSC forebygge, oppdage og håndtere sikkerhetshendelser for å beskytte sektorens informasjonsverdier, produksjons- og kommunikasjonsevne, materielle verdier og omdømme.[337]

8.3 Det er etablert et cybersikkerhetssenter for høyere utdanning og forskning (eduCSC) som skal understøtte informasjonssikkerhetsarbeidet i virksomhetene

Resultatet av informasjonssikkerhetsprogrammets to prosjekter «analysesenter og responsmiljø» og «rådgivningstjenester og kompetanseheving» var at det ble etablert et cybersikkerhetssenter for høyere utdanning og forskning (eduCSC).

Kunnskapsdepartementet har i liten grad involvert seg i å bestemme hvordan senteret bør innrettes. Departementet opplyser at de forutsetter at virksomhetene kommer til enighet om hvilke tjenester senteret bør tilby.[338] Departementet er imidlertid observatør i Digitaliseringsstyret og har kunnet følge utviklingen der.

8.3.1 Cybersikkerhetssenterets tjenester og betalingsmodell

Senteret ble offisielt «åpnet» av forsknings- og høyere utdanningsministeren 25. mars 2021,[339] men på dette tidspunktet var ikke organiseringen eller tjenestene senteret skulle tilby, endelig bestemt.

I etterkant av åpningen fikk Digitaliseringsstyret et første forslag til innretning/finansiering etter programperioden. Institusjonene uttrykte her at de hadde behov for en mye mer detaljert beskrivelse

[334] Unit (2020) Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren. Vedlegg til NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser. Versjon 1.
[335] HK-dir (2023) Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren. Vedlegg til NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser. Versjon 2.1
[336] Samt i Meld. St. 29 (2011-2012) Samfunnssikkerhet, pkt. 4.4., og gjentatt i Nasjonal strategi for informasjonssikkerhet (2012), pkt. 4.4, med tilhørende handlingsplan, tiltak 4.2.
[337] Unit (2020) Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren. Vedlegg til NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser. Versjon 1.
[338] Intervju med Kunnskapsdepartementet.
[339] Uninett. (2021, 23. mars). Statsråd Asheim åpner Cybersikkerhetssenter for forskning og utdanning. *NTB kommunikasjon*. https://kommunikasjon.ntb.no/pressemelding/statsrad-asheim-apner-cybersikkerhetssenter-for-forskning-og-utdanning?publisherId=17847210&releaseId=17903969

av tjenestene (konkrete leveranser) og kostnader.[340] Saken ble deretter diskutert i flere møter, før Digitaliseringsstyret 10. februar 2022 vedtok at eduCSC skulle være en fellestjeneste i universitets- og høyskolesektoren. I påfølgende møte 1. april 2022 fastsatte styret endelig tjenestekatalog og betalingsmodell gjeldende fra 1. januar 2023.

Tjenestene til eduCSC

Det er etablert tre ulike abonnementer, eller «pakker», som kunder av senteret kan velge imellom (se faktaboks nedenfor). Senteret leverer også flere tilleggstjenester. Digitaliseringsstyret besluttet at «basispakken» skulle være obligatorisk for alle universiteter og høyskoler.

Faktaboks 18 Leveransene til eduCSC

Basispakken er gjort obligatorisk for UH21, og gir virksomhetene

- tilknytning til eduCSCs sektorvise responsmiljø
- en skjermet og sikker kommunikasjonskanal for trusler og sikkerhetshendelser
- oppdatert trusselinformasjon
- oversikt over kjente sårbarheter[341]
- tidlig varsling ved hendelser i sektoren
- bistand ved alvorlige eller kritiske hendelser
- et ubegrenset antall sikkerhetssertifikater
- deltakelse i sektorens fagfellesskap, CISO-forum og IRT Community
- gratis tilgang til senterets webinarer

Plusspakken inneholder i tillegg følgende tjenester:

- nettverkssensorer som avdekker trusler og varsler om hendelser
- tilgang til nasjonal delings- og beskyttelsesplattform (under utvikling)[342]
- automatisk blokkering av kjente trusler («DNS brannmur»)
- tilgang til historiske data for etterforskningsformål
- tilgang til nye tjenester først

Totalpakken inneholder alle tjenestene i basis- og plusspakken samt drift og sikring av lokalnett.

Tilleggstjenester omfatter blant annet ekstern sårbarhetsskanning, tilgang til logganalyseverktøy og ulike rådgivningstjenester. Dette er tjenester som virksomhetene selv kan velge. For UH21 er sårbarhetsskanning obligatorisk.

Kilde: Sikts/eduCSCs beskrivelse av abonnementer på senterets nettsider.

Sikt har valgt å organisere senteret som et «produktområde» i divisjon for data og infrastruktur.[343] I starten av 2023 bestod eduCSC av 14 personer som til sammen leverte ca. 11 årsverk.[344] Senteret bygger på og erstatter Uninett CERT, som tidligere overvåket Forskningsnettet og var sektorens responsmiljø. Senteret skal også ivareta tjenester/oppgaver som tidligere ble gjort av sekretariatet for informasjonssikkerhet i Uninett. Sekretariatet ble etablert av departementet i 2013, men overdratt til

[340] Sak 27/21 i Digitaliseringsstyret, 09.06.2021.
[341] Bl.a. Nasjonalt cybersikkerhetssenter sender ut varsler om alvorlige sårbarheter i programvare, eduCSC «siler» disse varslene og videreformidler de som vurderes å være relevante for sektoren, i praksis 1-4 varsler per uke. De videreformidler også varsler fra enkeltleverandører som de vurderer som spesielt sektorrelevante. Senteret kan også oppdage nettaktivitet hos virksomheter tilknyttet forskningsnettet som indikerer at sårbarheter utnyttes. Er sårbarhetene alvorlige nok kan eduCSC følge opp kundene for å forsikre seg om at sårbarheter lukkes.
[342] Felles nasjonal delings- og beskyttelsesplattform for søk og registrering av kjente trusler er under utarbeidelse og kommer fra 3-4 kvartal 2023. Av produktstrategien framgår det at dette vil videreutvikles i 2024.
[343] Sikt har en todelt ledelsesmodell. De ansatte har sin organisatoriske tilhørighet i seksjoner; produktområdene (som eduCSC) leier ressurser fra seksjonene etter behov.
[344] Oversendelsesnotat fra Sikt datert 10.3.2023.

Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning i 2018 som del av omorganisering i sektoren.[345]

Sikt mener det i all hovedsak er positivt at eduCSC nå er etablert som en egen leveranse framfor at sikkerhetstjenestene er en delmengde av en annen leveranse (nettilknytningen). De peker blant annet på at arbeidet dermed synliggjøres i større grad, og mener dette gjør diskusjoner rundt finansiering og innhold i tjenestene enklere.[346]

Foreløpig er det krevende å finansiere senteret. I etableringsfasen 2019–2022 mottok Uninett/Sikt prosjektmidler hovedsakelig til å etablere eduCSC (12,5 millioner kroner årlig). Ifølge Sikt går senteret trolig ca. 10 millioner kroner i underskudd det første året med ny prismodell, blant annet fordi de fleste av kundene (36 av 53) har valgt basispakken nevnt ovenfor. Om senteret ikke skal nedskalere aktiviteten, må Sikt i tiden framover enten bruke mer risikokapital, finne måter å øke inntektene på eller motta mer midler fra departementet.[347]

eduCSC dekker også virksomheter i sektoren som ikke ligger under departementet, men rene nettkunder mottar færre sikkerhetstjenester enn før

Cybersikkerhetssenteret dekker også virksomheter i sektoren som ikke er underlagt Kunnskapsdepartementet. Våren 2023 var det totalt 57 kunder av senteret, hvorav totalt 26 virksomheter ikke ligger under departementet. Dette inkluderer flere private høyskoler[348] og forskningsinstitutter[349].

Selv om eduCSC ikke er *sektorvist responsmiljø* for disse 26 virksomhetene ifølge departementets rammeverk, vil virksomhetene motta de samme tjenestene fra eduCSC ved en eventuell sikkerhetshendelse. Forskjellen er at håndtering av slike hendelser ikke vil eskaleres i tråd med rammeverket – departementet vil ikke kobles inn ved for eksempel et dataangrep på en privat høyskole.

Det er i tillegg ca. 100 virksomheter som er tilknyttet forskningsnettet, men som ikke er kunder av eduCSC. Før sikkerhetssatsingen og omorganiseringen i sektoren var sikkerhetstjenester fra Uninett CERT en implisitt leveranse for *alle* virksomheter som var tilknyttet nettleveransen fra Uninett. Alle kunder av forskningsnettet var også kunder av Uninett CERT.[350] Disse virksomhetene mottar altså færre sikkerhetstjenester enn de gjorde tidligere.

Alle som er tilknyttet Forskningsnettet, får imidlertid noen grunnleggende sikkerhetstjenester. Dette gjelder beskyttelse for tjenestenektangrep[351], at eduCSC følger opp tilfeller der det oppdages «uønsket» nettverkstrafikk eller aktivitet[352], samt åpen sikkerhetsinformasjon som senteret sender ut på e-post. En liten andel av nettilknytningsavgiften (drøyt to millioner kroner totalt) går til eduCSC for å håndtere sikkerhetsarbeid i Forskningsnettet.

Blant virksomheter som bare er kunder av forskningsnettet, finner vi noen selskaper som er hel- eller deleid av universiteter og høyskoler. Dette inkluderer forskningsselskapene NORCE Norwegian Research Centre AS og NTNU Samfunnsforskning AS.

[345] Intervju med HK-dir, Intervju med Sikt, Sluttrapport UH – Sikkerhetssatsing 2019–2022.
[346] Referat fra intervju med Sikt 13. juni 2023, Oversendelsesnotat fra Sikt.
[347] Referat fra intervju med Sikt 13.juni 2023.
[348] Handelshøyskolen BI, VID vitenskapelige høgskole, MF vitenskapelig høyskole for teologi, religion og samfunn, Høyskolen i Kristiania, Dronning Mauds Minne Høgskole, NLA Høgskolen
[349] Andøya Space, CICERO, Framsenteret, Norsk institutt for bioøkonomi, Havforskningsinstituttet, Chr. Michelsens Institutt, Norsk institutt for luftforskning, Norsk institutt for naturforskning.
[350] Intervju med Sikt.
[351] I et tjenestenektangrep (DDOS-angrep) forsøkes det å hindre tilgang til en ressurs i et nett ved å overbelaste denne med nettrafikk, ofte fra flere forskjellige kilder. Forsvar mot dette kan være en kombinasjon av evne til å oppdage angrep, klassifisere trafikk og blokkere uønsket trafikk, samt planlegging av kapasitet til å håndtere trafikkmengder.
[352] Dette kan være basert på eduCSCs egen overvåking av trafikken i nettverket eller på varsler fra andre om at ressurser i en virksomhet brukes til uønsket virksomhet. Et eksempel på det siste kan være en server som er overtatt og brukes til å sende ut spam.

Det jobbes foreløpig ikke aktivt med å promotere eduCSCs abonnementspakker overfor rene kunder av forskningsnettet.

8.3.2 Flere virksomheter opplever at tjenestetilbudet er uklart og/eller ikke dekker deres behov, og BOTT har gått sammen om et eget sikkerhetssamarbeid

Mange av virksomhetene som er omfattet av vår undersøkelse, har lagt vekt på at leveransene fra eduCSC og innholdet i pakkene ikke har framstått som tydelig nok.

I en samlet tilbakemelding i 2022 uttrykte UiB, UiO, UiT og NTNU (BOTT) at de mente det burde være færrest mulig obligatoriske tjenester i eduCSC.[353] Bakgrunnen for dette var at de mente det opprinnelige forslaget til dels var uklart på hva de enkelte tjenestene innebar, til dels bestod av tjenester som virksomhetene mente de allerede betalte Sikt for gjennom andre leveranser, og til dels bestod av tjenester som de fire universitetene allerede hadde selv. I tillegg var enkelte av tjenestene basert på UiOs og NTNUs leveranser til Sikt.[354]

Disse fire universitetene har gått sammen om et eget sikkerhetssamarbeid, **BOTT Digital Sikkerhet**, og har informert alle IT-lederne i UH-21 om at de har til hensikt å etablere et alternativt og supplerende felles tjenestetilbud som kan tilbys alle.[355] Et av områdene som det er klart at virksomhetene vil samarbeide om, er sikkerhetsovervåking og felles logganalyse, der BOTT-universitetene har valgt et annet logganalyseverktøy enn Sikt og eduCSC.

Sikt trekker fram samstyringsmodellen som et viktig forum hvor deltakerne kan gi innspill til hva som bør prioriteres i den videre utviklingen av senteret. eduCSC har våren 2023 laget en produktstrategi som skal presenteres for sektoren i porteføljestyre for data og infrastruktur, UH-IT og CISO-forum. I intervju forteller Sikt at «eduCSC kan ikke fortsette å gjøre litt av alt, og ønsker å vite hva sektoren vil at de prioriterer».

Pilotering og kartlegging av brukerbehov og betalingsvilje for tjenestene

I prosjektperioden gjennomførte eduCSC noe kartlegging av brukerbehov og pilotering av leveranser ved utvalgte virksomheter. Det er begrenset med skriftlig dokumentasjon fra piloteringen, og det ble ikke gjennomført systematiske kartlegginger av brukerbehov mot et bredere lag av virksomheter i sektoren før mot slutten av 2021[356].

Behovskartleggingen og piloteringen som ble gjennomført, bestod av

- innsiktsarbeid som kartla brukerbehov hos to virksomheter basert på tjenestedesign[357]
- pilotering av rådgivning og analyse, registrering og rapportering ved mottak av phishing-e-post og hjelp til å forbedre deteksjonsevne i Microsoft Defender mot to virksomheter[358]
- pilotering av logganalyse mot syv virksomheter[359]
- pilotering av sårbarhetsskanning før dette ble gjennomført som et engangstiltak mot hele sektoren

Sikt opplyste i intervju at kapasitetsbegrensninger hos de syv pilotene medførte at arbeidet ikke ble som Sikt opprinnelig hadde planlagt.[360]

[353] Referat fra digitaliseringsstyret 1. april 2022.
[354] Et eksempel på dette er sperrelister.
[355] Dokumentet fra IT-BOTT ble sendt i kopi til alle IT-lederne i UH21.
[356] Av Sak 8/22 i Digitaliseringsstyret framgår det at det ble gjennomført en workshop med BOTT og en behovskartlegging blant 24 respondenter UH-sektoren i november/desember 2021, med mål om å få ytterligere innsikt i behov og ønsker innenfor arbeidet med informasjonssikkerhet og personvern.
[357] UiB og Arkitektur- og designhøgskolen i Oslo (AHO).
[358] BI og UiA.
[359] UiO, UiS, HiØ, NGU, OsloMet, Uninett AS (nå Sikt) og Unit (nå Sikt).
[360] Særlig de mindre virksomhetene hadde utfordringer med å avsette tilstrekkelig ressurser til å tilrettelegge data og gjennomføre logganalyse. Virksomhetene hadde også begrenset kapasitet til å delta i de jevnlige møtene som var planlagt for å framskaffe nødvendig innsikt.

Sikt har ikke opplevd at kundene har vilje til å betale for rådgivning og kompetanseheving. Betalingsviljen for slike tjenester ble ikke undersøkt i kartleggingen av brukerbehov som ble gjennomført gjennom fireårssatsingen.

Sikt har videre opplevd lite eller ingen etterspørsel etter tjenester som inntrengingstester og revisjoner av virksomhetenes arbeid med informasjonssikkerhet og personvern. Flere av virksomhetene i dybdeundersøkelsen har imidlertid kjøpt slike tjenester fra private konsulentselskaper/revisjonsfirmaer, noe som indikerer at det finnes etterspørsel etter denne typen tjenester i sektoren. Sikt har imidlertid ikke hatt kapasitet til å tilby slike tjenester så langt.

Ifølge eduCSCs produktstrategi fram mot 2025 skal senteret utforske om det skal tilby inntrengingstester framover, og hvilken type tester det er etterspørsel etter. Sikt opplyste i intervju at et slikt tilbud enten kan gis ved hjelp av egen kompetanse, som i så fall må bygges opp, eller gjennom innkjøp av tjenester fra en underleverandør. eduCSC vil blant annet undersøke etterspørselen og betalingsviljen gjennom CISO-forum og/eller IRT Community. Det er et mål i produktstrategien at en eventuell tjeneste fra eduCSC skal tilbys fra andre halvdel av 2024.

Siden Sikt ikke har markedsført eduCSC aktivt overfor de rundt 100 kundene av Forskningsnettet som ikke er tilknyttet eduCSC, vet de lite om vekstpotensialet og etterspørselen etter tjenester fra denne gruppen.

8.3.3 Ikke alle de planlagte tiltakene departementet la opp til, er gjennomført

De fleste av de «nye» leveransene som ble utviklet i fireårssatsingen, ble plassert i plusspakken/totalpakken eller definert som tilleggstjenester. Av de 24 forskningsvirksomhetene under Kunnskapsdepartementet har imidlertid kun 7 valgt plusspakken og 1 valgt totalpakken.[361] Av dem som har valgt enten pluss- eller totalpakken, har 6 virksomheter så langt valgt å kjøpe tilleggstjenester.

Leveransene i basispakken, som to tredjedeler av virksomhetene abonnerer på, bygger på det Uninett CERT leverte tidligere. Forskjellene mellom det Uninett CERT leverte tidligere, og det som eduCSC leverer i dag, er kort forklart

- **mer infrastruktur, verktøy og informasjon:** Det er i løpet av programperioden investert i infrastruktur og verktøy for å understøtte hendelseshåndteringen bedre. eduCSC har også fått et større tilfang av informasjon.
- **videreutvikling av nettverk for hendelseshåndtering:** eduCSC har videreutviklet tillitsnettverket som nå heter «**IRT Community**». Dette er et nettverk for dem som jobber operativt med IT-sikkerhet/hendelseshåndtering, og inkluderer en formalisert prosess for å tas opp som deltaker. Antallet virksomheter som er tilknyttet nettverket, har økt fra 35 i 2018 til 51 i 2023. Det er hyppige møter i forumet.
- **lynmeldingstjeneste for hendelseshåndtering:** Det er etablert en lynmeldingstjeneste for IRT-nettverket («**IRT Chat**») der medlemmene av nettverket kan ha dialog i sanntid. Løsningen blir blant annet brukt av eduCSC til å sende ut varsler. Mange av forskningsvirksomhetene vi har undersøkt, særlig de mindre virksomhetene, peker på dette som svært nyttig i det operative IT-sikkerhetsarbeidet.
- **etablering av fagfellesskap:** Det er etablert et fagfellesskap for informasjonssikkerhetsledere, **CISO-forum**. Det fantes tidligere et tilsvarende forum som ble ivaretatt av Sekretariat for informasjonssikkerhet i Uninett, men dette ble borte med omorganisering i sektoren 2018, da ansatte i sekretariatet ble overført fra Uninett til Unit. eduCSC gjenopptok dette i 2020 og er i dag fasilitator for forumet. Det er etablert et årshjul med kvartalsvise møter.

[361] [redacted]

- **webinarer:** eduCSC arrangerer også **webinarer** om ulike temaer innenfor informasjonssikkerhet, som er inkludert i prisen for alle betalende kunder.

Ekstern sårbarhetsskanning er også en «ny» tjeneste, som i utgangspunktet er definert som tilleggstjeneste men tilbys uten ekstra kostnader til alle universiteter og høyskoler. I løpet av programperioden ble det inngått et tverrsektorielt samarbeid med HelseCert, som har lengre erfaring med sårbarhetsskanning i egen sektor. Det ble gjennomført en engangs sårbarhetsskanning for hele sektoren i 2021, før samarbeidet ble formalisert og etablert som en kontinuerlig tjeneste. Fra 2022 gjennomføres det en ukentlig ekstern sårbarhetsskanning med rapportering til virksomhetene. HelseCert skanner Forskningsnettet og ikke virksomhetenes interne nettverk, jf. kapittel 5. [redacted]

Sikts sårbarhetsskanning og begrensningene i denne er omtalt tidligere i kapittel 5.3.3.

Fagmiljøet som tilbød rådgivning og kompetanseheving, ble delt opp da sektoren ble omorganisert, og tilbudet har ikke blitt som opprinnelig planlagt

Prosjektet «rådgivningstjenester og kompetanseheving» hadde som mål å få på plass rådgivningstjenester for implementering og helhetlig praktisering av ledelsessystemer for informasjonssikkerhet, herunder tiltak for å heve kompetansen innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte. Prosjektet skulle utrede og anbefale tjenester og foreslå organisering og leveransemodell for hvordan tjenestene skulle leveres til sektoren.[363]

Målet var ambisiøst og skisserte tiltak for kompetanseheving innenfor to fagområder, rettet mot ulike målgrupper:

- operativ IT-sikkerhet og IRT (hendelseshåndtering), rettet mot virksomhetenes sikkerhetsmiljøer
- informasjonssikkerhet og personvern, rettet mot ledelse, ansatte og studenter

Prosjektmandatet skisserte seks tjenester som relevante for sektoren:

- bistand til institusjonene med revisjoner av informasjonssikkerhet og personvern, og forslag til nødvendige tiltak basert på revisjonene
- bistand og kompetanseheving for å bidra til at institusjonene gjennomfører regelmessige risikovurderinger
- bistand på institusjonsnivå for å skaffe oversikt over informasjonsverdier og klassifisering av informasjon
- styrking av sikkerhetskompetanse lokalt på institusjonsnivå innenfor hendelseshåndtering, rapportering og avviks- og hendelseshåndtering
- bistand til institusjonene i planlegging for gjenopprettelse av normal drift i etterkant av alvorlige sikkerhetshendelser, samt bidrag til utarbeidelse, revisjon og testing av slike planer
- bistand til å utvikle og gjennomføre beredskapshendelser på IT-området

Målet med prosjektet var langt mer ambisiøst enn hva Sikt beskriver i sluttrapporten fra sikkerhetssatsingen. I vurderingen av resultatoppnåelsen som ble gjort i her,[364] er det listet kun ett resultatmål som handler om rådgivning og kompetanseheving: «Etablert samhandlingsarena for erfarings- og kunnskapsutveksling om informasjonssikkerhet i sektoren.» Resultatet Sikt viser til her, er etableringen av CISO-forum og IRT Community, som er videreutviklinger av tidligere leveranser fra

[362] [redacted] vil ikke ha sårbarhetsskanning fra Sikt fordi de opplever at det er for dyrt.
[363] Kilde: Prosjektmandat for prosjektet «Rådgivningstjenester og kompetanseheving» innenfor programmet «UH Sikkerhetssatsning 2019–2022».
[364] Sluttrapport UH-sikkerhetssatsing 2019–2022.

Uninett AS. I tillegg har eduCSC utarbeidet en egen veileder om verdivurdering, samt gjort noen revisjoner av enkelte andre veiledere.[365]

Fra og med 2023 gjennomføres webinarer som er gratis for eduCSCs betalende kunder, og i løpet av det siste året har eduCSC gjennomført enkelte webinarer innenfor temaer hvor vi ser det er etterspørsel blant virksomhetene i undersøkelsen, for eksempel verdivurdering og kontroll med kunnskapsoverføring. I oppsummeringen fra sistnevnte kommer det fram at mange ønsker tydeligere og konkrete retningslinjer fra myndighetene med eksempler, søkbare og digitale varelister, samt opplæring og kursing.[366]

Alle med basisabonnement har tilgang til eduCSCs webinarer og til CISO-forum og IRT Community. Øvrige rådgivningstjenester er tilleggstjenester.

I risikohåndteringsplanen for 2022–2023 fra HK-dir er det hele seks tiltak som dreier seg om rådgivning og opplæring.[367] Et av tiltakene er at Sikt skal tilby veiledning og rådgivning tilpasset den enkelte institusjonen. Risikohåndteringsplanen for 2021–2022 inneholdt et lignende tiltak som gikk enda lenger: at rådgivnings- og veiledningstjenesten i Sikt skulle avholde årlige møter med den enkelte virksomhet med bakgrunn i HK-dirs anbefalingsbrev. Dette tiltaket har ikke blitt gjennomført.

Per juni 2023 var det tre ansatte i Sikt som kunne tilby rådgivning og kompetanseheving, men disse brukte kun i overkant av ett årsverk til dette.

I perioden 2013–2018 fantes det et sekretariat for informasjonssikkerhet, etablert av Kunnskapsdepartementet og lagt til Uninett AS. Sekretariatet tilbød både opplæring, rådgivning og revisjoner til virksomhetene i sektoren. De fleste som var ansatt i sekretariatet, ble som følge av en virksomhetsoverdragelse i 2018 flyttet fra Uninett AS til Unit. Fagmiljøet som hadde tilbudt opplæring, rådgivning og revisjoner, ble dermed flyttet ut av Uninett AS og fantes ikke lenger i Uninett AS da selskapet ble innlemmet i Sikt 1. januar 2022.

Både HK-dir og Sikt påpeker i intervju at det tilbys langt mindre rådgivning og kompetanseheving enn man opprinnelig hadde sett for seg, og mindre enn tiden før fireårssatsingen.[368]

Dokumentanalyse og intervjuer med Sikt og HK-dir viser at det er flere årsaker til at eduCSC ikke har tilbudt rådgivningstjenester og kompetanseheving i det omfanget man opprinnelig hadde sett for seg:

- Prosjektet «rådgivningstjenester og kompetanseheving» kom senere i gang enn prosjektet «analysesenter og responsmiljø». Oppstarten ble utsatt til sommeren 2020 i påvente av at Unit (HK-dir) skulle gjennomføre den første tilstands- og risikovurderingen slik at informasjon om virksomhetenes behov fra vurderingen kunne brukes i prosjektet.
- Informasjonssikkerhetsprogrammet utviklet seg i retning av å ha mer oppmerksomhet på operativ IT-sikkerhet og mindre på rådgivning, og mer av midlene enn opprinnelig planlagt ble prioritert til prosjektet «analysesenter og responsmiljø».
- Sikt/eduCSC bygget ikke opp kapasitet på rådgivning og kompetanseheving på samme nivå som det forhenværende sekretariatet hadde hatt.
- Digitaliseringsstyret besluttet hvilke tjenester eduCSC skulle tilby. Sikt ga i 2021 en orientering til Digitaliseringsstyret om innhold og pris på de ulike tjenestene. Sikt opplyste i intervju at det lå mer rådgivning og kompetanseheving i forslaget enn det Digitaliseringsstyret besluttet, selv om det i liten grad var konkretisert hva slags rådgivningstjenester som skulle tilbys.

[365] Sikt. (u.å.). *Anbefalinger for arbeid med sikkerhet og beredskap i forskning og utdanning*. https://sikt.no/anbefalinger-sikkerhet-og-beredskap
[366] Det er også avholdt webinar om tjenestenektangrep (DDOS-angrep). Det framgår av produktstrategien til eduCSC at det skal gjennomføres flere webinarer/temamøter i løpet av 2023.
[367] Videreutvikle møteplassene i sektoren for informasjonsutveksling og erfaringsdeling (CISO- og personvernforum), styrke rådgivnings- og veiledningstjenesten hos Sikt, tilby rådgivning og veiledning tilpasset den enkelte institusjon eller virksomhet, gjennomføre revisjoner av arbeidet med informasjonssikkerhet og personvern hos den enkelte institusjon eller virksomhet, styrke veiledning om innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet, tilby kurs for ledere i informasjonssikkerhet og personvern.
[368] Referat fra intervju med HK-dir, referat fra intervju med Sikt.

- Sikt mener virksomhetene i sektoren har liten vilje til å betale for disse tjenestene. Dersom Sikt skal gjøre mer innenfor opplæring, rådgiving og revisjon, må det finansieres gjennom brukerbetaling eller bevilgning, eventuelt også gjennom sterkere føringer fra Kunnskapsdepartementet.

Sikt vurderer at eduCSCs evne til å oppdage dataangrep er uendret i perioden

Det meste av satsingsmidlene fra departementet ble brukt på prosjektet «analysesenter og responsmiljø». Det framgikk av det opprinnelige budsjettet for programmet at brorparten av midlene skulle prioriteres til dette prosjektet,[369] men en enda større andel av midlene enn opprinnelig planlagt ble brukt her.[370] Et sentralt mål med prosjektet var å forbedre deteksjons-, analyse- og responskapasiteten i UH-sektoren. Dette skulle gjøres ved å utvikle og innføre felles sikkerhetstjenester for sektoren på dette området, blant annet gjennom å etablere en sentral plattform for håndtering av data til analyseformål.

Sikt vurderer selv at deres egen evne til å oppdage dataangrep er uendret etter fireårssatsingen. Dette skyldes hovedsakelig to forhold:

[redacted] Sikt peker i intervju på at nettverkssensorene er et viktig verktøy for dem som jobber med hendelseshåndtering i eduCSC. Virksomheter som ikke har nettverkssensor, vil ifølge Sikt ikke kunne motta like god bistand i forbindelse med hendelseshåndtering.

Sikt overvåker kun trafikken i Forskningsnettet og ikke det som skjer på innsiden av virksomhetenes egne nettverk.[372] [redacted]

Felles infrastruktur og programvare for logganalyse tas ikke i bruk. Sikt/eduCSC har også brukt mye av ressursene i prosjektet på infrastruktur og programvare for logganalyse.[373] En konkret leveranse i fireårssatsingen er tilbud om logganalyseverktøy fra Crowdstrike (Falcon Logscale) med et sentralt data-/loggmottak som også Sikt har tilgang til. Bruk av felles logganalyseverktøy og loggmottak gir enklere tilgang for eduCSC, som dermed kan yte raskere og bedre bistand ved behov. Med denne tjenesten lagres loggene sentralt og ikke i kundens egen infrastruktur – noe som kan være en fordel dersom det inntreffer en hendelse som setter kundens infrastruktur ut av spill. Kundene får også tilgang til å benytte til dels kraftige analyseverktøy selv, dersom de har kapasitet og kompetanse til dette.

Logganalyse er en tilleggstjeneste, jf. faktaboks 18, og per første halvår 2023 benyttet seks av forskningsvirksomhetene seg av logganalyseverktøyet til Sikt. De som abonnerer på denne tilleggstjenesten, har tilgang til logganalyseverktøyet og loggene sine i det sentrale loggmottaket. Per i

[369] Vedlegg til sluttrapport: *Prosjektmandat Analysesenter og Responsmiljø*, *Prosjektmandat Rådgivningstjenester og Kompetanseheving*.
[370] Det går ikke fram av felles sluttrapport for de to prosjektene, eller av annen dokumentasjon fra prosjektene, hvor mye som ble brukt på henholdsvis «analysesenter og responsmiljø» og «rådgivningstjenester og kompetanseheving». Det framgår imidlertid av sluttrapporten at de kostnadsdrivende leveransene har vært infrastruktur og programvare for data-/logganalyseverktøy, sårbarhetsskanning og finansiering av et prosjekt for Nasjonal klientdrift. Det er opplyst at prosjektet om klientdrift ble inkludert i prosjektet fordi en sentralisering av klientdriften i sektoren potensielt ville kunnet bidra til bedre informasjonssikkerhet.
[371] [redacted]
[372] Unntaket er virksomhetene som abonnerer på «plusspakken», hvor Sikt også drifter lokalt nettverk. Blant virksomhetene under departementet gjelder dette kun [redacted].
[373] Sluttrapport side 10.

dag gjør Sikt imidlertid ikke noen analyser av loggdataene som ligger i det sentrale loggmottaket for å kunne oppdage sikkerhetshendelser. Sikt mener at flere må bruke denne tjenesten dersom det skal gjøres et felles løft for å øke deteksjonsevnen i sektoren. Ifølge Sikt er det først når en stor andel logger ligger i et sentralt register, *og* Sikt har kapasitet til å gjøre analyser av dataene, at felles logganalyse vil gi gevinster gjennom økt deteksjonsevne.

Undersøkelsen viser at det har vært utfordrende for eduCSC å få en samlet sektor med på logganalysearbeidet. UiO og NTNU, som har vært med i styringsgruppen for delprosjektet «analysesenter og responsmiljø», har vært uenige i valget av logganalyseløsning, blant annet fordi de selv allerede hadde tatt i bruk et annet verktøy.

[redacted]

- [redacted]
- [redacted]

8.3.4 Sikt mener at de kan ta en større rolle i risikovurderinger på sektornivå, men har ikke undersøkt betalingsviljen for dette

I kapittel 7 viste vi at flere av virksomhetene som er undersøkt, etterlyser at Sikt tar en større rolle i å risikovurdere fellessystemer og andre IT-systemer som brukes på tvers i sektoren, i tillegg til å følge opp leverandører av slike systemer. [redacted]

Da vi ba virksomhetene om å oversende risikovurderinger som de hadde gjennomført i perioden 2019–2022, fikk vi blant annet oversendt en risikoanalyse av Office 365 gjennomført av Uninett i 2017. Denne risikovurderingen ble tilrettelagt av sekretariatet for informasjonssikkerhet i UH-sektoren[374], som i praksis ble lagt ned i 2018.

Risikovurderinger som gjennomføres på sektornivå, kan ikke erstatte risikovurderinger som gjøres i virksomhetene. Uansett må hver enkelt virksomhet gjøre egne vurderinger av risiko i forbindelse med innføring av systemer i egen organisasjon og IT-infrastruktur. Felles risikovurderinger kan imidlertid gi et bedre grunnlag når den enkelte virksomhet skal vurdere risiko lokalt.

I intervju trekker Sikt fram at de har «*flere av komponentene på plass som enkelt kan videreutvikles for å kunne tilby en fellestjeneste som kan dekke dette behovet*»:

- en felles teknisk plattform for å dele personvern- og informasjonssikkerhetsvurderinger (Feide)
- et kompetansemiljø som kan gjennomføre og kvalitetssikre personvern- og informasjonssikkerhetsvurderinger:
  - Cybersikkerhetssenter for forskning og utdanning
  - nasjonalt kompetansemiljø for personvern (tidl. NSD)
  - et eksisterende kompetansemiljø for innkjøp av fellestjenester i UH-sektoren

[374] Sekretariatet ble opprettet av KD og lagt til Uninett AS. Ifølge mandatet skulle sekretariatet tilrettelegge for risiko- og sårbarhetsvurderinger for enkeltinstitusjoner og formidle erfaringer fra hele sektoren.

Sikt skal være hele kunnskapssektorens tjenesteleverandør, og mange av IT-systemene som brukes i høyere utdanning og forskning, brukes også i grunnopplæringen (grunnskole og videregående opplæring). Dette gjelder for eksempel Office 365.

Sikt har foreløpig ikke undersøkt betalingsviljen eller etablert en forretningsmodell for en fellestjeneste for denne typen vurderinger av personvern og informasjonssikkerhet.

Sikt skulle kjøpe inn et felles risikostyringsverktøy for sektoren, men prosessen strandet da anskaffelsen ble felt i KOFA

Som det framgår av kapittel 7.4, har mange av virksomhetene utfordringer med å holde oversikt over risikovurderinger som er gjennomført.

Virksomhetene ønsker et bedre risikostyringsverktøy, og i 2021 opprettet Uninett et prosjekt for å kjøpe inn en løsning for som kunne tilbys sektoren. I mars 2022 ble det valgt en leverandør[375], men beslutningen ble påklaget av tilbyderen som var rangert som nummer to[376], til Klageorganet for offentlige anskaffelser (KOFA). KOFA konkluderte i november 2022 at Sikt hadde brutt regelverket ved ikke å kompensere for informasjonsasymmetri i konkurransen. Sikt besluttet deretter å avlyse den pågående anskaffelsesprosessen.[377]

Sikt har i dialog med virksomhetene gjennom CISO-forum avklart at det fortsatt er interesse for å arbeide for en fellesavtale for risikostyringsverktøy i UH-sektoren, og Sikt opplyste i intervju at de vil lyse ut en ny konkurranse.

8.4 Departementets styringsinformasjon

8.4.1 Departementet får en del informasjon om status for arbeidet i sektoren, men lite informasjon om det faktiske sikkerhetsnivået

Kunnskapsdepartementet mottar informasjon om trusler og sårbarheter gjennom de årlige risiko- og tilstandsvurderingene fra HK-dir. Her sammenfatter HK-dir informasjon fra kartleggingene i virksomhetene[378], vurderer virksomhetenes modenhetsnivå innenfor informasjonssikkerhet og personvern og sannsynligheten for at virksomhetene etterlever kravene som er formulert i policyen for informasjonssikkerhet og personvern i høyere utdanning og forskning. HK-dir trekker også inn informasjon fra andre kilder, slik som statistikk om IT-sikkerhetshendelser i forskningsnettet fra sektorvist responsmiljø (eduCSC) og risiko- og trusselvurderinger fra nasjonale myndigheter.[379]

Departementet får også oppdateringer om trusselbildet og informasjon om hendelser som er nyttig for departementet å kjenne til, fra HK-dir i kvartalsvise møter.[380] Departementet har videre løpende dialog med PST, Etterretningstjenesten og NSM og opplyste i intervju å ha vært i dialog om å få mer faste møtepunkter.[381]

HK-dir har ifølge årshjulet tre måneder til å gjennomføre kartleggingsmøter med til sammen 28 virksomheter.[382] Det er dermed begrenset hvor dypt de kan gå ned i de tolv punktene som er angitt i policyen. Vurderingene av virksomhetenes modenhetsnivå, samt sannsynlighet for at de etterlever

[375] Diri.
[376] Corporater.
[377] Begrunnelsen for dette var at Sikt vurderte at det ikke var mulig å tildele kontrakt til den ene av tilbyderne uten at det påløp en signifikant risiko for ytterligere forsinkelser og potensiell midlertidig forføyning, samt negativ eller positiv kontraktsinteresse.
[378] HK-dir sammenfatter resultatene fra kartleggingsmøtene i en intern risiko- og tilstandsvurdering som oversendes departementet. I henhold til årshjulet mottar departementet den interne versjonen av rapporten som unntas offentlighet i april, mens en offentlig versjon av rapporten publiseres i juni.
[379] Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten (E-tjenesten).
[380] Referat fra intervju med HK-dir.
[381] Referat fra intervju med Kunnskapsdepartementet.
[382] HK-dir gjennomfører ikke kartleggingsmøter med «seg selv». Kunnskapsdepartementet kjøpte imidlertid inn en ekstern modenhetsvurdering av HK-dirs eget arbeid med informasjonssikkerhet og personvern i 2022.

policyen, blir dermed i stor grad basert på det virksomhetene selv forteller i kartleggingsmøtene.[383] HK-dir erkjenner de metodiske begrensningene og redegjør også for disse i rapportene sine.[384]

Det finnes flere områder som ikke dekkes så godt av HK-dirs kartlegging, for eksempel

- **risikovurderinger.** HK-dir stiller spørsmål om hvordan virksomhetene vil beskrive risikostyringen foregående år, og om det ble gjennomført risikovurderinger. Dette gir informasjon om konkrete risikovurderinger som er gjennomført, men gir mindre informasjon om systematikken i risikostyringen og i hvilken grad virksomhetene bruker risikovurderinger til å fange opp svakheter. Det gjøres heller ingen vurderinger av kvaliteten på risikovurderingene.
- **nivået på sikkerhetstiltakene i virksomhetene.** HK-dir får årlig opplyst hvilke nye sikringstiltak virksomhetene har iverksatt foregående år. HK-dir gjør imidlertid ikke en systematisk gjennomgang av tiltakene. Det er dermed vanskelig å vurdere det generelle sikkerhetsnivået i virksomhetene, og om virksomhetene har valgt riktige eller de viktigste tiltakene. Men hvis virksomhetene har iverksatt «åpenbare» tiltak som tofaktorautentisering, blir det fanget opp.
- **opplæring og kompetanseheving.** Virksomhetene får mulighet til å rapportere om opplæringstiltak som er gjennomført, men det gjøres ikke vurderinger av systematikken i virksomhetenes arbeid med opplæring/kompetanseheving. HK-dirs kartlegging fanger heller ikke opp omfanget eller innholdet i opplæringen eller om opplyste tiltak er gjennomført i praksis.

Verken HK-dir eller andre gjennomfører tester for å kartlegge hva som faktisk er status, eller om tiltakene virksomhetene oppgir, er implementert og fungerer i praksis.

HK-dir påpekte i intervju at det hadde vært en fordel om Sikt kunne ha gjennomført enkelte sikkerhetstester, og at dette ville vært nyttig informasjon for Kunnskapsdepartementet for å vurdere sikkerhetstilstanden i sektoren. Som nevnt ovenfor har inntrengingstester inngått som tiltak i risikohåndteringsplanene, men det er uklart hvordan testene skal finansieres. Sikt peker på at det hittil har kommet svært få forespørsler fra virksomhetene om denne tjenesten. I senterets produktstrategi fram mot 2025 står det at senteret skal utforske om det skal tilbys inntrengingstester framover. Samtidig uttrykker Sikt i intervju at hvis inntrengingstester skal komme på plass som en fast tjeneste, tror eduCSC at det er nødvendig at departementet bevilger midler og/eller stiller krav om at tjenesten skal brukes.

Sikt påpeker i intervju at eduCSC kunne bidratt i risiko- og tilstandsvurderingene med mer kvantifiserbar informasjon, som resultater fra sårbarhetsskanninger, speilinger på DNS-server som er svartelistet, og trusselinformasjon, som mengden nettfiske/phishing.

Departementet har ikke fått rapportering om måloppnåelse i fireårssatsingen

Departementet har ikke fått noen rapportering om måloppnåelse for informasjonssikkerhets-programmet eller for prosjektene Uninett/Sikt hadde ansvar for. Sikt utarbeidet en sluttrapport for de to prosjektene de hadde ansvar for, som departementet ikke fikk tilsendt og ikke hadde sett før vi gjennomførte intervju, i juni 2023.[385] Denne rapporten ble heller ikke lagt fram for Digitaliseringsstyret, hvor departementet som nevnt er observatør.[386]

[383] I Risiko- og tilstandsvurderingen for 2023 skriver HK-dir at «Utsagn og påstander fra institusjonene og virksomhetene ble ikke forsøkt verifisert på annen måte enn ved gjennomgang av årsrapporter, rapporter behandlet i styremøter og informasjon publisert på hjemmesider.»
[384] Se f.eks. Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2023.
[385] Departementet opplyser at de har etterspurt og mottatt sluttrapporten etter dette.
[386] Rapporten ble kun lagt fram og behandlet i styringsgruppene for de to prosjektene.

8.4.2 NOKUT har fått ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren, men har ikke hatt kapasitet til å følge opp

NOKUT fikk i tildelingsbrevet for 2021 ansvar for å føre uavhengig kontroll med etterlevelse av krav til informasjonssikkerhet og personvern. Kunnskapsdepartementet opplyste i intervju at departementet ikke har pålagt NOKUT å følge opp dette oppdraget, fordi NOKUT har kommunisert at de ikke har ressurser til dette nå. Derfor har det heller ikke blitt diskutert konkret hva slags kontroller av informasjonssikkerhet og personvern NOKUT eventuelt kan gjøre.

Departementet opplyser at det ikke har vært meningen at NOKUT skal gjøre tekniske kontroller, og at det ikke vil være hensiktsmessig å bygge opp kompetanse på dette hos NOKUT.

NOKUT har imidlertid prioritert å føre kontroll med samfunnssikkerhet og beredskap, et ansvar de fikk i 2019. NOKUT kan gjøre kontroller på tre nivåer. De to første nivåene gjennomføres årlig, mens det tredje, som er mer ressurskrevende, kun gjennomføres ved behov:

- **Nivå 1** består av en gjennomgang av det som rapporteres om samfunnssikkerhet og beredskap i årsrapportene. Gjennomgangen på nivå 1 blir brukt som grunnlag for risikovurdering på nivå 2.
- **Nivå 2** består av mer målrettede kontroller. De bruker en sjekkliste basert på konkrete kriterier. NOKUT vil da innhente kriseplaner, ROS-analyser og lignende. De velger ut mellom fem og åtte virksomheter. Utvalget bestemmes ut fra avvik i rapporteringen og annen informasjon.
- **Nivå 3** består av «stedlig kontroll», med intervjuer og gjennomgang av mer dokumentasjon. Dette er foreløpig ikke gjort av ressurshensyn. Det er tenkt at slike kontroller skal benyttes om det er store avvik.

Kontroller på de to første nivåene gjennomføres hvert år. I 2020 innhentet NOKUT dokumenter (nivå 2) for alle virksomhetene og gjorde en særskilt rapportering. Dette viste seg å være nyttig, og NOKUT vil gjennomgå dokumenter fra alle virksomhetene med en syklus på hvert femte år.

HK-dir peker på at NOKUT verken har kapasitet eller kompetanse til å gjennomføre kontroller som er grundige nok til kunne kvalitetssikre eller verifisere direktoratets funn og vurderinger. Derfor stiller direktoratet mer generelt spørsmål ved merverdien av NOKUT-kontroller på informasjonssikkerhetsområdet, spesielt sett i lys av det økte kontrolltrykket i sektoren som disse kontrollene kan innebære.

9 Vurderinger

9.1 Beskyttelsesverdige forskningsdata i forskningsvirksomhetene under Kunnskapsdepartementet er ikke i tilstrekkelig grad sikret mot dataangrep

Forskningsdata skal i hovedsak tilrettelegges for åpen tilgang, men hensyn til sikkerhet, personvern, immaterielle rettigheter, forretningshemmeligheter og lignende tilsier i en del tilfeller at forskningsdata ikke kan gjøres helt åpent tilgjengelige. En rekke lover og regler stiller krav til hvordan slike data skal sikres. Lovverket stiller også konkrete krav til virksomhetene om at de skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset risikoen. For å oppnå dette bør virksomhetene følge faglige standarder som angir god praksis.

Etter vår vurdering er forskningsdata i virksomheter under Kunnskapsdepartementet ikke tilstrekkelig sikret mot dataangrep, gitt kravene i lovverket. Inntrengingstester mot tre forskningsinstitusjoner viser at det er mulig å stjele, manipulere, eller slette forskningsdata med høy informasjonsverdi fra virksomhetene ved hjelp av offentlig kjente metoder og standardverktøy. Undersøkelser av tekniske og organisatoriske sikkerhetstiltak ved ti forskningsinstitusjoner viser også betydelige svakheter ved flertallet av disse. [redacted]

9.1.1 Inntrengingstester mot tre forskningsinstitusjoner ga full kontroll over IT-infrastruktur ved to av dem og kontroll over forskeres IT-utstyr og skylagring ved det tredje

Vi gjennomførte inntrengingstester mot tre forskningsinstitusjoner. Målet i inntrengingstestene var å få tilgang til sensitive forskningsdata, enten via administrative rettigheter til systemene eller ved å utnytte rettigheter hos enkeltforskere.

Inntrengingstestene ved [redacted] ga full kontroll på institusjonenes IKT-infrastruktur. Vi oppnådde tilgang som domeneadministrator, som gir full kontroll over et Windows-nettverk. Ved [redacted] ble dette oppnådd den første dagen av inntrengingstesten, og det ble funnet flere veier for å oppnå denne rettigheten.

Oppnådd kontroll innebar at vi kunne administrere alle tilknyttede brukere, PC-er og servere i Windows-nettverket. Med slik tilgang kunne vi tildele oss selv alle ønskede rettigheter og skaffe oss tilgang til all informasjon, inkludert sensitiv forskningsinformasjon, som var lagret i nettverket. Med rettighetene vi oppnådde, hadde det også vært mulig å endre, slette eller kryptere all informasjon dersom motivasjonen hadde vært økonomisk vinning eller sabotasje.

Noe sensitiv forskningsinformasjon er lagret i særskilte tjenester som TSD, som er bedre beskyttet. Disse har ikke vært omfattet av inntrengingstesten, men kontrollen vi oppnådde over forskeres brukerkontoer og IT-utstyr kunne vært brukt som utgangspunkt for et angrep for å få tilgang til forskernes informasjon også på slike plattformer.

Ved den tredje forskningsinstitusjonen, [redacted], fikk vi kontroll med de fleste klientmaskiner, noe som ga muligheter til å hente ut eller manipulere informasjon lagret lokalt på PC-er og på eiernes skylagringsløsning. Denne skylagringsløsningen er en av lagringsmulighetene for sensitive forskningsdata (opp til nivået «fortrolig») ved [redacted] og flere av de andre virksomhetene. Tilgangen kunne videre vært brukt til målrettede angrep mot forskere med kunnskap og tilgang til sensitiv informasjon, for eksempel ved å endre sikkerhetsinnstillinger på maskinen og/eller legge inn

skadevare som fanger opp alt som tastes på maskinen eller all lyd rundt maskinen. Vi fikk ikke kontroll med servere og [redacted] datanettverk generelt, fordi de sentrale delene av virksomhetens IT-infrastruktur er bedre beskyttet.

Et av formålene med inntrengingstestene var å undersøke virksomhetenes evne til å oppdage aktiviteter i et dataangrep. Vi gjorde ingen forsøk på å skjule angrepene, men produserte mye nettverkstrafikk og kjente tegn på angrep. Ved [redacted] ble få eller ingen av aktivitetene oppdaget. Ved [redacted] ble inntrengingstesten oppdaget den fjerde testdagen, og de fleste aktivitetene ga spor i logger som virksomheten samler inn. Disse loggene kan analyseres av virksomheten for å danne et bilde av hvordan et angrep har blitt gjennomført og hvilke systemer som er berørt av angrepet.

Inntrengingstestene ga full kontroll i to virksomheter hovedsakelig fordi det er enkelt å koble seg til virksomhetenes nettverk, det benyttes svake passord, mange brukerkontoer tildeles store rettigheter, og det er svakheter i beskyttelsen av nettverk. I tillegg ble lite oppdaget fordi overvåkningen var mangelfull. Revisjon av sikkerhetstiltak på tvers av ti virksomheter, jf. punkt 9.1.2, viser at disse svakhetene er vanlige for de [redacted] Det gir grunn til å tro at inntrengingstester ved andre virksomheter i sektoren kunne gitt lignende resultater.

9.1.2 Det er stor variasjon i gjennomføringen av tekniske sikkerhetstiltak, og mange av virksomhetene har vesentlige svakheter

Vi har undersøkt tekniske sikkerhetstiltak både ved de tre virksomhetene i dybdeundersøkelsen, samt ved ytterligere syv forskningsvirksomheter. Undersøkelsen viser at sentrale anbefalinger i NSMs Grunnprinsipper for IKT-sikkerhet, som anses som god praksis, ikke følges av mange av de undersøkte virksomhetene. Nivået på sikkerhetstiltakene i forskningsvirksomhetene varierer imidlertid betydelig, [redacted]

Undersøkelsen viser:

- **Mangelfull kontroll med brukerkontoer og tilgangsrettigheter**: Flere av virksomhetene har mange brukerkontoer med høye rettigheter og benytter ikke ulike brukerkontoer for ulike driftsoperasjoner slik som anbefalt. Dette gjør det lettere for en angriper å eskalere rettigheter og få kontroll med all IKT-infrastrukturen når et fotfeste er etablert.
- **Svake krav til brukerautentisering**: Krav til passord varierer, og det er ofte ikke satt høyere krav til passord for kontoer som har høye rettigheter. Lave krav gjør det mulig å gjette eller knekke passord. Tofaktor-autentisering er innført mange steder, men det gjelder ikke alle tjenester og påloggingsmuligheter.
- **Mangelfull sårbarhetsstyring av IT-utstyr og programvare**: De fleste virksomhetene har på plass rutiner for sikkerhetsoppdatering av programvare for å fjerne kjente sårbarheter, men [redacted] har ikke god helhetlig sårbarhetsstyring med skanning for sårbarheter og herding ved å fjerne funksjonalitet man ikke trenger. Dette øker risikoen for at en angriper kan finne og utnytte sårbarheter i et dataangrep.
- **Det er svakheter i nettverkssikkerheten.** [redacted]

- **Mangelfull logging og overvåkning**: Det er mangler i datagrunnlaget for å oppdage og håndtere dataangrep ved at det logges mindre enn anbefalt ved [redacted]. [redacted] har etablert et godt grunnlag for å oppdage dataangrep, men de øvrige virksomhetene har enklere overvåkningsløsninger og mindre kapasitet til å gjennomgå overvåkningsdata. [redacted]

Videre viser undersøkelsen at det er store forskjeller mellom [redacted] og at virksomhetene har ulike sikkerhetsmessige utfordringer:

- [redacted]
- [redacted]

Undersøkelsen viser forbedringer i tekniske sikkerhetstiltak de seneste årene, som kan ha sammenheng med økt oppmerksomhet på risikoen i sektoren og i samfunnet generelt. For eksempel er tofaktorautentisering innført for mange tjenester og ekstern sårbarhetsskanning er etablert av Sikt.

De tre virksomhetene som inngikk i dybdeundersøkelsen har alle, i etterkant av våre undersøkelser, planlagt og til dels gjennomført en rekke tiltak som øker deres sikkerhet.

9.1.3 Det er svakheter i organisatoriske sikkerhetstiltak som er etablert for å beskytte forskningsdata

For alle de ti virksomhetene har vi gjennomgått utvalgte organisatoriske sikkerhetstiltak som er ment å beskytte forskningsdata, og undersøkt om disse er i tråd med god praksis. Undersøkelsen viser at det er en del svakheter i gjennomføringen av disse tiltakene:

- **Det mangler full oversikt over forskningsdata som grunnlag til å vurdere hva som bør beskyttes, og hvordan dette bør gjøres.** De fleste virksomhetene har en relativt god oversikt over personopplysninger i forskning, men oversiktene er ikke komplette. [redacted] Flere av virksomhetene i undersøkelsen forvalter kunnskap innenfor fagområder som anses som relevante for fremmede staters etterretning.
- **Det gis lite veiledning om sikker behandling av forskningsdata.** Ni av ti virksomheter gir føringer om at informasjon som behandles, skal klassifiseres etter konfidensialitet, og angir hvilke lagringsløsninger som er tillatt for de ulike konfidensialitetsklassene. Disse virksomhetene har også utarbeidet rutiner for behandling av personopplysninger i forskning. [redacted]
- **Opplæring og bevisstgjøring om informasjonssikkerhet og håndtering av forskningsdata er lite systematisk ved de fleste av virksomhetene.** Alle virksomhetene har gjennomført enkeltstående opplæringstiltak og tilbyr noe administrativ støtte innenfor informasjonssikkerhet og personvern hvor forskere, veiledere og studenter kan få hjelp ved behov. Likevel tyder undersøkelsen på at disse i varierende grad kjenner til regler om informasjonssikkerhet, og at mange opplever klassifisering av data som skal beskyttes som vanskelig.

- **IT-systemer driftet lokalt i fakulteter, institutter og lignende omfattes ofte ikke av virksomhetenes sentrale retningslinjer og rutiner.** Det er i liten grad stilt krav eller gitt føringer om sikkerhetstiltak til lokale driftsansvarlige for drift av disse systemene. Lokale driftsansvarlige har også i liten grad laget skriftlige retningslinjer eller andre kravdokumenter for løsningene de drifter. [redacted] Undersøkelsen viser imidlertid at trenden går i retning av sentralisering av IT-drift og/eller skjerping av kravene til lokale IT-miljøer.
- **Sikkerheten hos leverandører av IT-systemene blir i liten grad fulgt opp av virksomhetene.** Virksomhetene har tjenesteutsatt store deler av databehandlingen i forskning, undervisning, administrasjon og formidling. Mange av virksomhetene oppgir at de gjør vurderinger av informasjonssikkerhet hos leverandørene ved innkjøp av nye IT-løsninger, men det er svært begrenset oppfølging i etterkant av dette.

Undersøkelsen viser at det er gjort forbedringer i gjennomføringen av disse organisatoriske sikkerhetstiltakene de siste årene. Spesielt har virksomhetene, som en oppfølging av den nye personopplysningsloven i 2018, arbeidet med å kartlegge og forbedre rutiner for behandling av personopplysninger. Arbeidet med andre organisatoriske sikkerhetstiltak har imidlertid virksomhetene kommet kortere med.

9.2 Virksomhetene har i stor grad lagt rammene for informasjonssikkerhetsarbeidet, men oppnår ikke ønsket sikkerhetsnivå på grunn av mangler i gjennomføringen

Virksomhetene skal ha et ledelsessystem for informasjonssikkerhet. Ledelsessystemet skal sette planlegging, gjennomføring, kontroll/evaluering og oppfølging av informasjonssikkerhetsarbeidet i system. Systemet skal sikre at passende sikkerhetstiltak gjennomføres og tilfredsstillende sikkerhet oppnås.

Undersøkelsen viser at de fleste virksomhetene har lagt rammene for arbeidet med informasjonssikkerhet i hovedsak ved å etablere de overordnede dokumentene i et ledelsessystem. Alle virksomhetene i undersøkelsen unntatt [redacted] hadde dokumentert et ledelsessystem på undersøkelsestidspunktet. Arbeidet med informasjonssikkerhet har fått mer oppmerksomhet de siste årene, og ansvaret for dette arbeidet i virksomhetene er i hovedsak klarlagt.

Selv om arbeidet med informasjonssikkerhet har kommet lenger, er det fortsatt mangler i implementeringen av ledelsessystemene i virksomhetene. De viktigste utfordringene er

- **ledelsessystem.** Implementeringen av systemet på et konkret nivå er ofte mangelfull, selv om overordnede policyer er vedtatt. Undersøkelsen viser for eksempel at bare tre av virksomhetene stiller tydelige krav i temaspesifikke policyer til tekniske sikkerhetstiltak som vi har kontrollert i denne undersøkelsen. Tre av virksomhetene stiller noen krav, mens fire av virksomhetene ikke har utarbeidet slike policyer i det hele tatt. Der det ikke stilles konkrete krav, blir det i stor grad opp til den enkelte IT-ansatte å vurdere hva som er tilstrekkelig sikkerhet ved oppsett av systemer og lignende.
- **gjennomføring av besluttede tiltak.** Planer for å iverksette strategier ut fra policyer som ledelsen har vedtatt, er ofte mangelfulle fordi de ikke dekker hele virksomheten, plangrunnlaget er mangelfullt og tidsfrist og ansvar for oppgaver ikke er definert. Samtidig viser undersøkelsen at virksomhetene har utfordringer med å gjennomføre tiltak som er besluttet.

- **risikostyring.** Undersøkelsen viser at det gjøres langt færre risikovurderinger enn hva virksomhetene selv setter krav om, og at det i liten grad gjennomføres systematiske risikovurderinger av IT-infrastruktur. Videre bygger ikke overordnede risikovurderinger klart på informasjon fra mer detaljerte risikovurderinger av de enkelte IT-systemer mv. Svakhetene i risikostyringen gjør at mange av virksomhetene har et dårlig grunnlag for å vurdere hvilke sikkerhetstiltak som skal implementeres, og for å gjennomføre vedtatte tiltak.
- **evaluering og etterkontroller av sikkerhetstilstanden.** I de fleste virksomhetene er det begrenset med kontroll og evalueringer av arbeidet med informasjonssikkerhet og personvern samt av hvordan forskningsdata behandles. Noen virksomheter har ikke satt krav om kontroller og evalueringer i ledelsessystemet. Andre har satt krav, men sliter med å gjennomføre vedtatte kontroller og evalueringer. Dermed har mange av virksomhetene lite kunnskap om ledelsessystemet og sikkerhetstiltakene fungerer som forutsatt, og om hva som faktisk er sikkerhetstilstanden i virksomheten.
- **avklaringer om roller og ansvar.** Selv om ansvar på et overordnet nivå er avklart i de fleste virksomheter, er det eksempler på at arbeidet med informasjonssikkerhet har blitt hemmet av at det mangler en overordnet/samlende rolle. I flere virksomheter er det noe uklarhet både om hvilke tekniske sikkerhetstiltak som skal implementeres, og hvem som har ansvaret for å følge opp at tiltakene blir iverksatt i IT-driften. I flere virksomheter er det ikke klart hvem som har ansvaret for organisatoriske sikkerhetstiltak som opplæring og bevisstgjøring.
- **kompetanse og ressurser.** Det er store forskjeller mellom virksomhetene med hensyn til tilgang til ressurser og kompetanse om informasjonssikkerhet. [redacted] Kompetanse og ressurser er nødvendig for å identifisere og iverksette nødvendige sikkerhetstiltak, ikke minst tiltak som kan gi virksomheten kapasitet til å oppdage dataangrep.
- **ledelsens informasjonsgrunnlag.** I syv av ti virksomheter har toppledelsen gjennomgått status for ledelsessystemet og sikkerhetstilstanden ett eller flere av årene i undersøkelsesperioden. Innholdet i gjennomgangene varierer imidlertid betydelig, og få av virksomhetene bruker resultatet fra risikoarbeidet eller statusen for gjennomføring av tiltaksplaner i særlig grad. Dermed har ledelsen ofte ikke et fullstendig bilde av hvordan sikkerhetstilstanden er, og et svakt grunnlag for å kunne vurdere tiltak.
- **styrets rolle.** I flere virksomheter mottar styret lite av informasjonen de trenger for å ivareta sin rolle som det organet med det øverste ansvaret for informasjonssikkerheten. I noen virksomheter er det heller ikke definert hva som er styrets rolle og ansvar i ledelsessystemet, eller det er uklart hvilken informasjon styret skal motta.

Det er stor variasjon i virksomhetenes arbeid med informasjonssikkerhet. Dette er til dels naturlig da de har svært ulik størrelse, ulikt omfang av forskningsdata og ulik kompleksitet i IT-infrastruktur. Hvordan utfordringene i punktlisten ovenfor skal tas tak i, må være tilpasset virksomhetene. Kompliserte ledelsessystemer med omfattende krav til dokumentasjon passer ikke i små virksomheter. Etter vår vurdering er det imidlertid nødvendig at det finnes løsninger i sektoren som sikrer at ledelsessystemene også i små virksomheter fungerer etter sin hensikt og sikrer et akseptabelt sikkerhetsnivå.

Undersøkelsen viser at [redacted] er det [redacted] som jobber mest systematisk med informasjonssikkerheten. Dette viser seg fra planlegging og risikostyring til evaluering og etterkontroller, samt rapportering til ledelsen og styret.

[redacted] har i varierende grad svakheter på disse områdene. [redacted] skiller seg også ut ved at de hadde et godt utgangspunkt i starten av undersøkelsesperioden, med ressurser til arbeidet, en avklart sikkerhetsorganisering sentralt i IT-avdelingen og rimelig god kontroll med sikring av IT-infrastrukturen. Til sammenligning har det ved [redacted] vært nødvendig å omprioritere ressurser for å gjennomføre større «løft», bygge opp en sentral sikkerhetsorganisasjon og/eller gjøre avklaringer om roller og ansvar.

Selv om informasjonssikkerhet har fått mer oppmerksomhet de senere årene og ledelsessystem er utarbeidet i virksomhetene, gjenstår det betydelig arbeid for å implementere systemene fullt ut slik at de sikrer ønsket sikkerhetsnivå. Styret har det øverste ansvaret for å håndtere risikoen for informasjonssikkerheten og for at virksomheten har systemer som hindrer at sensitive forskningsdata i virksomheten kommer på avveier. Etter vår vurdering mottar de fleste styrene for lite informasjon om informasjonssikkerhetsrisikoen til å kunne ta stilling til sikkerhetsnivået. Trusselsituasjonen i sektoren er betydelig skjerpet de siste årene, og etter vår vurdering er det viktig at styrene tar sitt ansvar for å påse at virksomhetene har god nok informasjonssikkerhet.

9.3 Kunnskapsdepartementet har justert virkemiddelbruken de siste årene, men det er en del utfordringer i sektoren som dagens virkemidler ikke treffer

Departementet har ansvar for å avklare sentrale roller og ansvarsområder på informasjonssikkerhetsområdet og sørge for at den overordnede organiseringen og virkemiddelbruken på området er ressurseffektiv. Departementet har videre ansvar for å følge opp at underliggende virksomheter jobber for å nå mål og oppfylle krav på informasjonssikkerhetsområdet. Det innebærer blant annet å gi føringer på området og sørge for at virksomhetene gir dem et tilstrekkelig informasjonsgrunnlag for styringen. Departementet bør også vurdere hensiktsmessige virkemidler overfor de aktørene i sektoren der departementet mangler direkte styringslinjer.

I 2019 satte Kunnskapsdepartementet i gang et fireårig informasjonssikkerhetsprogram i universitets- og høyskolesektoren. Målet med programmet var å styrke informasjonssikkerheten i sektoren. Programmet skulle forbedre sektorens evne til å forebygge, oppdage og håndtere trusler mot forskningsnettet, og det skulle inkludere tiltak som analyseverktøy og kompetanseheving.

Sentrale resultater av satsingen er at det ble etablert

- en styringsmodell for informasjonssikkerhet, hvor ansvaret ble gitt til HK-dir – Direktoratet for høyere utdanning og kompetanse
- et Cybersikkerhetssenter for høyere utdanning og forskning, eduCSC, hvor ansvaret er gitt til Sikt – Kunnskapssektorens tjenesteleverandør

9.3.1 Styringsmodellen for informasjonssikkerhet har gjort at den enkelte forskningsvirksomhet har fått tettere oppfølging

Gjennom **styringsmodellen** er HK-dir – Direktoratet for høyere utdanning og kompetanse gitt ansvaret for den løpende sektorstyringen av informasjonssikkerhet og personvern i til sammen 29 virksomheter direkte underlagt departementet. Kunnskapsdepartementet har fastsatt en overordnet *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*, som sammenfatter krav og føringer på området og skal ligge til grunn for virksomhetenes arbeid. HK-dir gjennomfører årlige kartleggingsmøter med virksomhetene hvor de tar utgangspunkt i krav og føringer i policyen, og leverer forslag til konkrete tilbakemeldinger som departementet kan bruke i sin oppfølging av virksomhetene.

HK-dir gir også konkrete anbefalinger til virksomhetene om det videre arbeidet med informasjonssikkerhet og personvern. En del av virksomhetene som er undersøkt, oppgir at de har hatt nytte av HK-dirs kartlegging, og at det har bidratt til å rette virksomhetenes oppmerksomhet mot informasjonssikkerhet og sette retning for arbeidet. Dette er særlig tilfellet for de minste virksomhetene.

Undersøkelsen viser at departementet har fulgt opp virksomhetene som er omfattet av styringsmodellen gjennom etats- og eierstyringen. Departementet har også brukt pedagogiske virkemidler overfor enkelte virksomheter i sektoren der styringsmulighetene er mer begrensede. De har gitt *anbefalinger* til private høyskoler som ikke er omfattet av styringsmodellen, gjennom tilskuddsbrev.

Etter vår vurdering er det positivt at Kunnskapsdepartementet er tydelig om hvilke krav og føringer som gjelder for underliggende virksomheter, og følger opp dette gjennom styringsmodellen. Vi vurderer at dette har bidratt til større oppmerksomhet om informasjonssikkerhetsarbeidet i virksomhetene som er omfattet av styringsmodellen. Samtidig har personvernforordningen blitt innført og trusselbildet skjerpet etter konkrete hendelser i sektoren. Det er også positivt at departementet bruker pedagogiske virkemidler overfor enkelte virksomheter i sektoren der departementet ikke har en direkte styringslinje.

Departementet har ikke uttrykt forventninger om hvordan universiteter og høyskoler skal følge opp informasjonssikkerheten i selskapene de eier. Departementet framholder at de på generelt grunnlag forventer at eierinstitusjonene utøver sitt eierskap på en god måte og etterlever gjeldende lover og krav. Undersøkelsen viser at de tre største universitetene ikke har gitt føringer eller forventninger til informasjonssikkerheten gjennom eierdialogen til selskaper som driver med forskning eller teknologioverføring.

9.3.2 Kunnskapsdepartementet har i begrenset grad lyktes med å nå målet med informasjonssikkerhetssatsingen, og virkemidlene treffer i for liten grad virksomhetene som har størst behov for støtte

Som ledd i fireårssatsingen fikk Sikt (den gang Uninett) ansvar for å etablere et analysesenter og ta rollen som sektorvist responsmiljø for å forbedre sektorens evne til å håndtere trusler. Videre fikk de ansvaret for å få på plass rådgivningstjenester som skulle bistå sektoren i å implementere ledelsessystemer for informasjonssikkerhet på en helhetlig måte, og for å etablere et program for kompetanseheving innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte i sektoren. Leveransene fra Sikt ble samlet i et eget **Cybersikkerhetssenter for høyere utdanning og forskning, eduCSC.** Senteret tilbyr også tjenester til virksomheter i sektoren som ikke er underlagt Kunnskapsdepartementet.

For å dekke ulike behov i virksomhetene har eduCSC fra 2023 etablert ulike abonnementer, eller «pakker» av tjenester, som kunder av senteret kan velge blant. Enkelte tjenester leveres som tilleggstjenester. Både prismodell og tjenesteinnholdet er forankret i Digitaliseringsstyret, som er øverste nivå i universitets- og høyskolesektorens samstyringsmodell for digitalisering. Digitaliseringsstyret har bestemt at abonnementet «basispakken» skal være obligatorisk for alle høyskoler og universiteter. Det har foreløpig vært utfordrende for eduCSC å få senteret finansiert via brukerbetaling. Sikt anslår at senteret vil gå cirka ti millioner kroner i underskudd det første året med ny prismodell.

Undersøkelsen viser at leveransen eduCSC har kommet lengst med, er rollen som sektorvist responsmiljø. På dette området har departementet sørget for et rammeverk for håndtering av IT-sikkerhetshendelser i sektoren.

Når det gjelder evnen til å oppdage dataangrep, vurderer Sikt at denne har vært uendret i perioden. Dette skyldes at felles infrastruktur og logganalyse som eduCSC har kjøpt inn som del av satsingen, ikke tas i bruk, og at overvåking av nettverk ved hjelp av sensorer er lagt til abonnementet «plusspakken», mens flertallet av virksomhetene har valgt «basispakken».

Leveransene fra eduCSC med dårligst måloppnåelse er tiltakene innenfor rådgivningstjenester og kompetanseheving. Rådgivningstjenester er blant senterets tilleggstjenester, og så langt har få virksomheter valgt å benytte seg av dette tilbudet. De mest konkrete leveransene innenfor kompetanseheving er

- de to forumene for informasjonssikkerhet, CISO-forum og IRT Community
- utarbeidelse av en veileder
- revisjoner av enkelte andre veiledere
- gjennomføring av enkelte webinarer

Både HK-dir og Sikt vurderer at omfanget av rådgivning og kompetanseheving som tilbys er mindre enn tiden før fireårssatsingen.

[redacted]
Departementets virkemiddelbruk ved opprettelse av eduCSC ser foreløpig ikke ut til å ha løst disse problemene.

Spesielt evnen til å oppdage dataangrep avhenger av sterkt spesialisert kompetanse. [redacted]. eduCSC overvåker kommunikasjonen inn og ut av virksomhetene, på linje med det Uninett CERT gjennomførte før opprettelsen av senteret. Men senteret overvåker ikke virksomhetenes egne nettverk og systemer. [redacted]

[redacted]
Innhentede data viser at mange virksomheter leier inn konsulenter til å sette opp systemer og lignende, også med tanke på sikkerhet.

De fire største universitetene har gått sammen om et eget sikkerhetssamarbeid, BOTT Digital Sikkerhet, og ønsker at færrest mulig av tjenestene til eduCSC burde være obligatoriske. Undersøkelsen viser at disse virksomhetene har mye IT-sikkerhetskompetanse, og dermed noe mindre behov for tjenester fra eduCSC. De har også en del felles utfordringer, og etter vår vurdering en del å lære av hverandre. At de fire største universitetene samarbeider, løser imidlertid ikke problemene som sektoren som helhet har på informasjonssikkerhetsområdet.

Vi vurderer det som positivt at departementet har etablert et cybersikkerhetssenter med tjenester til hele sektoren, også til virksomheter i sektoren der departementet mangler direkte styringslinjer. Per dags dato greier imidlertid eduCSC verken å treffe behovene til [redacted]. Departementet har i stor grad overlatt vurderingene av hva eduCSC skal tilby til de underliggende virksomhetene, gjennom universitets- og høyskolesektorens samstyringsmodell for digitalisering. Etter Riksrevisjonens vurdering styres imidlertid senterets tjenestetilbud i dag i for stor grad av den enkelte virksomhets etterspørsel og betalingsvilje, og i for liten grad av behovene til sektoren som helhet.

Kunnskapsdepartementet har definert rollene til de sentrale aktørene i sektoren innenfor informasjonssikkerhetsområdet. Undersøkelsen viser imidlertid at det i praksis er uklarheter i forholdet mellom Kunnskapsdepartementet, HK-dir og Sikt når det gjelder styring og gjennomføring av informasjonssikkerhetstiltak i sektoren. Videre viser undersøkelsen at NOKUT verken gjennomfører eller har kapasitet til å gjennomføre det som er definert som deres rolle.

Samlet sett vurderer vi derfor at organiseringen og virkemiddelbruken på området for sektoren som helhet er mindre ressurseffektiv og målrettet enn den kunne ha vært.

9.4 Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren, og risikoreduserende tiltak som er besluttet på sektornivå, blir ikke fulgt opp

Departementet skal utarbeide og vedlikeholde systematiske risiko- og sårbarhetsanalyser, ta stilling til sikkerhetsnivået i egen sektor samt iverksette nødvendige kompenserende tiltak. Departementet skal også sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater. Hvor ofte og i hvilken utstrekning et område som informasjonssikkerhet bør evalueres, må bestemmes ut fra blant annet risiko og vesentlighet, samt kvaliteten på og omfanget av øvrig rapportering. Mer generelt har departementet overordnet ansvar for blant annet at virksomhetene bruker ressurser effektivt, og at det gjennomføres kontroll med virksomhetene.

Som del av styringsmodellen for informasjonssikkerhet har HK-dir fra og med 2019 levert årlige risiko- og tilstandsvurderinger til departementet. Gjennom disse mottar departementet informasjon om trusler og sårbarheter. Her sammenfatter HK-dir informasjon fra kartleggingene i virksomhetene, vurderer virksomhetenes modenhetsnivå innenfor informasjonssikkerhet og personvern og sannsynligheten for at virksomhetene etterlever kravene som er formulert i *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*. HK-dir trekker også inn informasjon fra andre kilder, slik som statistikk om IT-sikkerhetshendelser i forskningsnettet fra sektorvist responsmiljø (eduCSC) og risiko- og trusselvurderinger fra nasjonale myndigheter. På bakgrunn av dette utarbeider HK-dir også årlige risikohåndteringsplaner på sektornivå med forslag til tiltak for å håndtere risikoen. Kunnskapsdepartementet tar stilling til og slutter seg til planene.

Men HK-dir baserer risiko- og tilstandsvurderinger på virksomhetenes egenrapportering og gjør ingen form for sikkerhetstesting eller kontroller av den faktiske sikkerhetstilstanden. Verken HK-dir eller andre gjennomfører tester for å kartlegge den faktiske statusen eller om tiltakene institusjonene oppgir, er implementert og fungerer i praksis. Informasjonen departementet mottar fra HK-dir, dreier seg i hovedsak om virksomhetenes arbeid med organisatoriske sikkerhetstiltak, men sier lite om virksomhetenes tekniske sikkerhetstiltak og om tiltakene har effekt. Funnene fra de tekniske testene og inntrengingstestene i denne undersøkelsen viser at det er svakheter i de tekniske sikkerhetstiltakene hos alle virksomhetene.

Flere av virksomhetene i undersøkelsen har kjøpt inntrengingstester fra private konsulentselskaper/revisjonsfirmaer, men departementet får ikke informasjon om resultatene fra disse testene. Det er også en mulighet at eduCSC gjennomfører for eksempel inntrengingstester, men dette har senteret ikke kapasitet til per i dag.

Departementet har gitt NOKUT ansvar for å føre uavhengig kontroll med informasjonssikkerheten i sektoren, men det er ikke avklart hvordan en slik kontroll skal gjennomføres. NOKUT har ikke et kompetansemiljø innenfor informasjonssikkerhetstesting og har hittil ikke hatt kapasitet til å følge opp.

Samtidig viser undersøkelsen at risikoreduserende tiltak på sektornivå som er identifisert, og som departementet er orientert om, ikke blir gjennomført. Dette gjelder tiltak som inntrengingstesting og revisjoner av den enkelte virksomhets arbeid med informasjonssikkerhet og personvern og med kompetanseheving overfor virksomhetene. Ansvaret for å følge opp flertallet av tiltakene er gitt til Sikt ved Cybersikkerhetssenter for forskning og utdanning (eduCSC). En del av tiltakene har ikke blitt gjennomført, og har heller ikke vært realistiske å gjennomføre, da de i praksis har forutsatt både at Sikt/eduCSC etablerer nye tjenester og at virksomhetene i sektoren betaler for gjennomføringen.

Som vist i kapittel 9.1.3 mangler virksomhetene oversikt over egne informasjonsverdier i forskning som ikke er personopplysninger. Departementet har igangsatt et kartleggingsarbeid med utgangspunkt i sikkerhetsloven for å få bedre oversikt over informasjonsverdier i sektoren det er særlig viktig å beskytte. Dette arbeidet er ikke ferdigstilt.

Vi vurderer det som positivt at Kunnskapsdepartementet har etablert en prosess for risikostyring av sektoren som gir informasjon om arbeidet med informasjonssikkerhet i virksomhetene som er omfattet av styringsmodellen. Samtidig mottar departementet lite systematisk informasjon om de tekniske sikkerhetstiltakene som er iverksatt ute i virksomhetene, og om virkningen av tekniske og organisatoriske sikkerhetstiltak. Kunnskap om den faktiske sikkerhetstilstanden og verdiene i sektoren er viktig for at departementet skal kunne målrette krav og tiltak slik at sektoren er bedre i stand til å forbedre sikkerheten.

10 Referanseliste

Regelverk

Lover

- *Lov om arkiv* (arkivlova) (1. januar 2009)
- *Lov om behandling av personopplysninger* (personopplysningsloven) (20. juli 2018)
- *Lov om helseregistre og behandling av helseopplysninger* (helseregisterloven) (1. januar 2015)
- *Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.* (eksportkontrolloven) (18. desember 1987)
- *Lov om medisinsk og helsefaglig forskning* (helseforskningsloven) (1. juli 2009)
- *Lov om nasjonal sikkerhet* (sikkerhetsloven) (1. januar 2019)
- *Lov om organisering av forskningsetisk arbeid* (forskningsetikkloven)
- *Lov om rett til innsyn i dokument i offentleg verksemd* (offentleglova) (1. januar 2009)

Forordninger

- *Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]*

Reglement

- *Bevilgningsreglementet* vedtatt gjennom St.prp. nr. 48 (2004−2005) Om bevilgningsreglementet, jf. Innst. S. nr. 187 (2004–2005)
- *Reglement for økonomistyring i staten* fastsatt 12. desember 2003 med endringer, senest 20. desember 2022 (økonomireglementet)

Instrukser

- *Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter* (beskyttelsesinstruksen) (1. juli 1972)
- *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen) (1. september 2017)

Stortingsdokumenter

Stortingsmeldinger

- Meld. St. 22 (2020-2021) *Data som ressurs – Datadrevet økonomi og innovasjon*
- Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*
- Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*
- Meld. St. 29 (2011-2012) *Samfunnssikkerhet*

Innstillinger

- Innst. 568 S (2020–2021) *Innstilling fra næringskomiteen om Data som ressurs – Datadrevet økonomi og innovasjon*
- Innst. 275 S (2020−2021) *Innstilling fra justiskomiteen om Samfunnssikkerhet i en usikker verden*
- Innst. 187 S (2017−2018) *Innstilling fra justiskomiteen om IKT-sikkerhet. Et felles ansvar*

Stortingsproposisjoner

- Prop. 1 S (2018–2019) Kunnskapsdepartementet

Anbefalinger og standarder

- Center for Internet Security (2021) CIS Controls, version 8
- Nasjonal Sikkerhetsmyndighet (2020) Grunnprinsipper for IKT-sikkerhet, versjon 2.0
- Informasjonsteknologi – Sikringsteknikker – Tiltak for informasjonssikring, NS-ISO/IEC 27002:2017
- Ledelsessystemer for informasjonssikkerhet, NS-ISO/IEC 27001:2017

Styringsdokumenter

Tildelingsbrev

- Kunnskapsdepartementet. (2023). *Tilskuddsbrev 2023 til private høyskoler*
- Kunnskapsdepartementet. (2022). *Statsbudsjettet for 2022 – Tildelingsbrev til Kunnskapssektorens tjenesteleverandør (Sikt)*
- Kunnskapsdepartementet. (2022). *Statsbudsjettet for 2022, kap. 260 post 70 – Tilskuddsbrev til private høyskoler*
- Kunnskapsdepartementet. (2021). *Statsbudsjettet for 2021, kap. 260 post 70 – Tilskuddsbrev til private høyskoler*
- Kunnskapsdepartementer. (2021). *Tildelingsbrev 2021 for Nasjonalt organ for kvalitet i utdanningen (NOKUT)*
- Kunnskapsdepartementet. (2020). *Statsbudsjettet for 2020 kap. 260 post 70 – Tilskuddsbrev for private høyskoler*
- Kunnskapsdepartementet. (2019). *Statsbudsjettet for 2019 kap. 260 post 70 – Tilskuddsbrev for private høyskoler*
- Unit. (2019). *Statsbudsjettet 2019 kap. 280 post 72 – tilskuddsbrev til UNINETT AS*
- Unit. (2020). *Tilskuddsbrev UNINETT AS 2020*
- Unit. (2021). *Tilskuddsbrev UNINETT AS 2021*

Andre styringsdokumenter

- Kunnskapsdepartementet. (2021). *Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor*
- Kunnskapsdepartementet. (u.å.). *Oversikt over Kunnskapsdepartementets styringsmodell for informasjonssikkerhet*
- HK-dir (2023) *Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren. Vedlegg til NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser. Versjon 2.1*
- Simula. (2020). Protokoll fra generalforsamlingen i SIMULA AS 2020
- Universitetssenteret på Svalbard AS. (2020). Protokoll fra generalforsamlingen i Universitetssenteret på Svalbard AS 2020
- UNINETT. (2019). *Prosjektmandat for prosjektet «Analysesenter og responsmiljø» innenfor programmet «UH Sikkerhetssatsning 2019–2022»*
- UNINETT. (2019). *Prosjektmandat for prosjektet «Rådgivningstjenester og Kompetanseheving» innenfor programmet «UH Sikkerhetssatsning 2019–2022*
- Unit (2020) *Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren. Vedlegg til NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser. Versjon 1*

Rundskriv, veiledere og retningslinjer

Rundskriv

- Kunnskapsdepartementet. (2020). *Rundskriv F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning*

Veiledere og retningslinjer

- UNINETT. (2017). UFS136: Veiledning i klassifisering av informasjon
- Utenriksdepartementet. (2020). *Retningslinjer for kontroll med kunnskapsoverføring*

Rapporter, planer og rapportering

Offentlige utredninger

- NOU (2016: 19) *Samhandling for sikkerhet − Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*

Rapporter

- Etterretningstjenesten. (2023). *Fokus 2023*
- Etterretningstjenesten. (2022). *Fokus 2022*
- Etterretningstjenesten. (2021). *Fokus 2021*
- Etterretningstjenesten. (2020). *Fokus 2020*
- HK-dir. (2023). *Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2023*

- HK-dir. (2023). *Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2023, versjon unntatt offentlighet*
- HK-dir. (2022). *Temarapport 2022 – informasjonssikkerhet og personvern i høyere utdanning og forskning. Praktisering av krav til informasjonssikkerhet og personvern*
- HK-dir. (2021). *Temarapport 2021 – informasjonssikkerhet og personvern i høyere utdanning og forskning. Ledelsens styring og kontroll av arbeidet med informasjonssikkerhet*
- HK-dir. (2021). *Temarapport 2021 – informasjonssikkerhet og personvern i høyere utdanning og forskning. Pandemihåndteringen og betydningen for arbeidet med informasjonssikkerhet og personvern i UH-sektoren*
- Kunnskapsdepartementet. (2020). *Risiko- og sårbarhetsanalyse av Kunnskapsdepartementets sektor 2020. Arbeidsgrupperapport, avgitt i november 2020 (unntatt offentlighet)*
- Nasjonal sikkerhetsmyndighet. (2020). Risiko 2020
- Nasjonal sikkerhetsmyndighet. (2021). Risiko 2021
- Nasjonal sikkerhetsmyndighet. (2022). Risiko 2022
- Nasjonal sikkerhetsmyndighet. (2023). Risiko 2023
- Politiet. (2023). Politiets trusselvurdering 2023
- PST. (2023). Nasjonal trusselvurdering 2023
- PST. (2022). Nasjonal trusselvurdering 2022
- PST. (2021). Nasjonal trusselvurdering 2021
- PST. (2020). Nasjonal trusselvurdering 2020
- Sikt. (2022). Sluttrapport UH – Sikkerhetssatsing 2019-2022
- Unit. (2020). *Temarapport 2020 – informasjonssikkerhet og personvern i høyere utdanning og forskning. Tjenesteutsetting av digitale systemer og tjenester*
- Unit. (2020). *Temarapport 2020 – informasjonssikkerhet og personvern i høyere utdanning og forskning. Kontinuitet, beredskap og øvelser*

Strategier
- Justis- og beredskapsdepartementet og Forsvarsdepartementet. (2019). *Nasjonal strategi for digital sikkerhet*
- Kunnskapsdepartementet. (2017). *Nasjonal strategi for tilgjengeliggjøring og deling av forskningsdata*
- Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdselsdepartementet og Fornyings-, administrasjons- og kirkedepartementet. (2012). *Nasjonal strategi for informasjonssikkerhet*

Rapportering
- Sikt. (2022). *Sluttrapport UH – Sikkerhetssatsing 2019–2022*

Brev, notater og nettkilder

Brev/e-post
- Kunnskapsdepartementet. (2019) *Kunnskapsdepartementets styringsmodell for informasjonssikkerhet i høyere utdanning og forskning.* Brev sendt fra statsråden til Kunnskapsdepartementets underliggende virksomhetet i forbindelse med innføring av styringsmodellen.
- NTNU. (2023). *Svar på Riksrevisjonens spørsmål om forventninger/krav til informasjonssikkerhet i NTNU Technology Transfer AS.* Notat sendt på e-post til Riksrevisjonen 12. juni 2023
- Sikt. (2023). *Oversendelsesnotat – dokumentbestilling.* Brev til Riksrevisjonen, 11. mars 2023
- Universitetet i Bergen. (2023). *Forventninger til informasjonssikkerhet i NORCE Norwegian Research Centre AS.* E-post til Riksrevisjonen 12. juni 2023
- Universitetet i Oslo. (2023). *Re: Forventninger/krav til informasjonssikkerhet i Inven2 AS.* E-post til Riksrevisjonen 14. juni 2023

Nettkilder
- Sikt/eduCSC. (u.å.). *Cybersikkerhetssenter for forskning og utdanning.* Oversikt over abonnementer og tilleggstjenester. Hentet 8. mai 2023