Direktoratet for høyere utdanning og kompetanse

Risiko- og tilstandsvurdering 2023

Informasjonssikkerhet og personvern i høyere utdanning og forskning

Rapportnummer: **4/23**
ISSN: **2703-9102**

Innhold

Figurer

Sammendrag

I denne rapporten presenteres resultatene fra HK-dir sin årlige kartlegging av arbeidet med informasjonssikkerhet og personvern i UH-sektoren. Kartleggingen gjelder arbeidet i 2022 og omfatter de 28 virksomhetene som inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[1]

Som tidligere år, gir rapporten en oversikt over hvor langt de 28 virksomhetene er kommet i etterlevelsen av «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». Policyen er fastsatt av Kunnskapsdepartementet og gjort gjeldende fra 1. oktober 2020.

Deretter vurderer vi risikoen for uønskede hendelser som kan medføre at sektorens informasjonsverdier – opplysninger, datamaskiner og programvare – skades, ødelegges, eksponeres for uvedkommende eller er utilgjengelige.

Vi vurderer også mulighetene for at målene om informasjonssikkerhet og personvern i «Strategi for digital omstilling i universitets- og høyskolesektoren, 2021-2025» kan nås.

Avslutningsvis gir vi enkelte anbefalinger til sektortiltak som kan bidra til å styrke arbeidet med informasjonssikkerhet og personvern.[2]

Nedenfor oppsummerer vi hovedfunnene i rapporten og våre anbefalinger til tiltak for å forbedre informasjonssikkerheten og personvernet i UH-sektoren.

De kartlagte virksomhetene

HK-dir sin årlige kartlegging omfatter alle de 21 statlige universitetene og høgskolene.

I tillegg kartlegges sju direktorater og selskaper: Norges forskningsråd, Nasjonalt organ for kvalitet i utdanningen, Sikt – kunnskapssektorens tjenesteleverandør, Simula Research Laboratory, Norsk utenrikspolitisk institutt, Universitetssenteret på Svalbard og De nasjonale forskningsetiske komiteene.

1 Oversikt over styringsmodellen finnes her: https://hkdir.no/vaare-tenester/styring-av-informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning.

2 Arbeidet med rapporten – metodikk og datagrunnlag – gjøres rede for i vedlegg 1 og 2.

Inventarkontroll og trusselbildet

- Sektoren hadde styrket sin oversikt over de informasjonsverdier – opplysninger, datamaskiner og programvare – som skal beskyttes mot trusler og håndteres i henhold til rettslige krav.

- 9 universiteter og høgskoler oppga at de jobbet med å få oversikter over informasjonsverdier som er undergitt eksportkontroll og sikkerhetsloven.

- De 21 universitetene og høgskolene rapporterte om en nedgang i antallet brudd på informasjonssikkerheten og krenkelser av personvernet på omkring 30 prosent fra året før. Ingen av hendelsene hadde ført til alvorlige skadevirkninger.

- Samtidig med at antallet rapporterte brudd og krenkelser gikk ned, hadde universitetene og høgskolene styrket sin evne til å oppdage, varsle og håndtere hendelser og avvik.

- Hos de sju direktoratene og selskapene hadde det vært en mindre økning i antall brudd og hendelser (fordi flere virksomheter ble kartlagt i 2022 enn i 2021). Ingen av hendelsene medførte alvorlige skadevirkninger.

- Nettkriminelle grupper og tekniske eller menneskelige feil og uhell utgjorde de viktigste truslene. Rapporterte tilfeller av forsøk på statlig hacking (kunnskapsspionasje) var vesentlig redusert sammenliknet med 2021.

- Universitetene og høgskolene rapporterte om ca. 22 prosent færre personvernsaker (brudd og avvik) sammenliknet med året før.

- Antallet brudd på personopplysningssikkerheten som universitetene og høgskolene meldte til Datatilsynet gikk ned med drøyt 40 prosent i 2022. Meldte brudd gjaldt små mengder personopplysninger og omhandlet et lite antall enkeltpersoner.

- Hos de sju direktoratene og selskapene ble det ikke rapportert om brudd som var meldepliktige til Datatilsynet.

Forbedringer og policyetterlevelse

- Antallet årsverk øremerket for arbeidet med informasjonssikkerhet og personvern økte med ca. 10 i 2022. Hos de 28 virksomhetene var det i 2022 omkring 128 årsverk øremerket til dette arbeidet.

- Tiltaksaktiviteten i sektoren var relativt høy i 2022, og noe høyere enn i 2021. Det ble iverksatt særlig mange organisatoriske og pedagogiske tiltak. I sum samsvarte ikke alltid tiltakene med de manglene (sårbarhetene) som sektoren mente at den hadde behov for å utbedre.

- 16 av 21 statlige universiteter og høgskoler hadde forbedret sin etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i 2022. De fem siste universitetene og høgskolene hadde ikke forbedret etterlevelsen vesentlig.

- Seks av universitetene og høgskolene etterlevde de særskilte kravene som policyen stiller til personvern (behandling av personopplysninger) på en tilfredsstillende måte. Tre universiteter og høgskoler etterlevde kravene til informasjonssikkerhet.

- Det er sannsynlig eller mulig at 12 nye universiteter og høgskoler vil kunne etterleve samtlige krav i departementets policy i løpet av 2023. Det forutsetter imidlertid at disse institusjonene øker tempoet i etterlevelsesarbeidet.

- Fem av de sju direktoratene og selskapene som også omfattes av kartleggingen, etterlevde policyens særskilte krav til personvern (behandling av personopplysninger). Tre av de sju gjorde det samme når det gjaldt kravene til informasjonssikkerhet.

Vurdering av risiko

- Risikoen for brudd på informasjons- og personopplysningssikkerheten som skyldes løsepengevirus og statlig kunnskapsspionasje vurderes fortsatt som høy.
- Risikoen for statlig kunnskapsspionasje er ujevnt fordelt i sektoren: høy hos virksomheter hvor det behandles informasjonsverdier som, ifølge nasjonale sikkerhetsmyndigheter, er av interesse for utenlandsk etterretning; lav i de deler av sektoren som i liten grad behandler slike verdier.
- Risikoen for brudd som gjelder utilsiktede feil og uhell, tjenestenekt (DDoS) og misbruk av lokale dataressurser[3] vurderes som middels.
- Risikoen for direktør- og fakturasvindel vurderes som lav.

Muligheter for måloppnåelse

- Flertallet av virksomhetene i sektoren kan oppnå målene om informasjonssikkerhet og personvern i «Strategi for digital omstilling i universitets- og høyskolesektoren, 2021-2025».
- For sju av de 28 virksomhetene er det noe mer usikkert om målene i strategien kan nås før strategiperiodens utløp. Vi regner det likevel som realistisk at også disse virksomheter vil kunne oppfylle målene (og etterleve policyen) innen 2025.

Anbefalte tiltak

Årets kartlegging indikerer at arbeidet med informasjonssikkerhet og personvern i sektoren fortsatt bør styrkes. Dette er nødvendig for å redusere risiko, styrke policyetterlevelse og bidra til måloppnåelse.

Vi foreslår derfor følgende sektortiltak:

1. Tilby råd og veiledning om hvordan kartlegging av informasjonsverdier best kan gjennomføres, inkludert hvilke arbeidsverktøy som kan benyttes.
2. Videreutvikling av sektorens evne til å oppdage og håndtere brudd på informasjonssikkerheten og krenkelser av personvernet.
3. Styrking av opplærings- og kompetansetiltak innen informasjonssikkerhet og personvern.
4. Stille tydelige forventninger til informasjonssikkerheten og personvernet hos virksomheter i sektoren som tilbyr IT-tjenester til andre virksomheter.
5. Innrette tiltakene ovenfor slik at risikoen for løsepengevirusangrep og statlig kunnskapsspionasje reduseres.

De foreslåtte tiltakene kommenteres nærmere i kapittel 5.

3 Med dette menes at trussel-aktører bruker lokale datamaskiner til utvinning av kryptovaluta, utsending av søppel-epost eller gjennomføring av dataangrep rettet mot andre virksomheter (typisk DDoS).

Innledning

Årets risiko- og tilstandsvurdering oppsummerer hovedfunnene i HK-dir sin kartlegging av arbeidet med informasjonssikkerhet og personvern i høyere utdanning og forskning. Kartleggingen gjelder arbeidet innen disse områdene i 2022.

Som tidligere år, er formålet med rapporten tredelt.

Først å gi en oversikt over tilstanden hos og endringer i arbeidet med informasjonssikkerhet og personvern hos 28 statlige universiteter, høgskoler og øvrige virksomheter (direktorater og selskaper) som omfattes av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[4]

Dernest å vurdere følgende forhold:

- etterlevelsen i sektoren av kravene i departementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning»,[5]
- risikoen i sektoren for konkrete hendelser som innebærer brudd på informasjons- og personopplysningssikkerheten, og
- mulighetene for at sektoren vil oppnå målene om informasjonssikkerhet og personvern i strategien for digital omstilling i universitets- og høgskolesektoren.[6]

På bakgrunn av funnene fra årets kartlegging, anbefaler vi også enkelte tiltak på sektornivå som kan bidra til å styrke arbeid med informasjonssikkerhet og personvern hos de 28 virksomhetene.

4 Styringsmodellen ble presentert for Kunnskapsdepartementets underliggende virksomheter i brev fra statsråden av 7. januar 2019. Beskrivelse av styringsmodellen finnes på https://hkdir.no/vaare-tenester/styring-av-informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning#content-section-2. Sist besøkt 28.03.2023.

5 Policyen er fastsatt av Kunnskapsdepartementet i rundskriv F-04-20, og er gjort gjeldende fra 1. oktober 2020.

6 Se https://www.regjeringen.no/no/dokumenter/strategi-for-digital-omstilling-i-universitets-og-hoyskolesektoren/id2870981/. Sist besøkt 28.03.2023.

Kort om informasjonssikkerhet og personvern

Med informasjonssikkerhet menes evnen til å beskytte informasjonsverdier – opplysninger, datamaskiner og programvare – mot at de eksponeres for uvedkommende, skades eller ødelegges, endres eller slettes på uautoriserte måter eller er utilgjengelige for rettmessige brukere.[7]

Med personvern menes i denne sammenheng at enkeltpersoner (studenter, ansatte, forskningsdeltakere, osv.) sikres medinnflytelse over og en viss kontroll med bruken (behandlingen) av opplysninger som gjelder dem selv.[8] Hensikten med dette er å unngå urettmessige inngrep i privat- og familieliv, hjem og korrespondanse, krenkelser av anseelse og den personlige integriteten.

Personvern er et mål i seg selv – det er en grunnleggende rettighet nedfelt i internasjonale konvensjoner og i den norske Grunnloven. Informasjonssikkerhet er derimot et virkemiddel for å ivareta en rekke ulike formål, blant annet personvernet når det behandles opplysninger om den enkelte. Eksempler på andre formål inkluderer effektiv forvaltning, forsvarlig saksbehandling, tilfredsstillende økonomistyring og beskyttelse av offentlige eller kommersielle interesser.

Policy, styringsdokument og strategi

Kravene som stilles til informasjonssikkerhet og personvern i UH-sektoren fremgår av «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».[9] I policyen oppsummeres og tydeliggjøres de viktigste rettslige kravene som gjelder.

Overordnet innebærer dette at arbeidet med informasjonssikkerhet skal være risikobasert og skje innenfor rammen av et ledelsessystem for informasjonssikkerhet.

Samtidig skal det etableres og vedlikeholdes en internkontroll for personvern (GDPR) som sørger for at personopplysninger behandles på en lovlig og forsvarlig måte.

Tilsvarende krav og forventninger til arbeidet med informasjonssikkerhet og personvern følger av «Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor».[10]

Videre fremheves det i «Strategi for digital omstilling i universitets- og høgskolesektoren, 2021-2025»[11] at informasjonssikkerhet og personvern er forutsetninger for den digitale omstillingen i sektoren.

7 ISO/IEC 27001: 2013: Information Technology Security Techniques. Information Security Management Systems – Requirements. Se også Håkon Bergsjø, Ronny Windvik og Lasse Øverlier (red.) (2020): Digital sikkerhet. En innføring. Oslo: Universitetsforlaget.

8 Se for eksempel Dag W. Schartum (2020): *Personvernforordningen – en lærebok*. Bergen: Fagbokforlaget, eller Jon Wessel-Aas og Magnus Ødegaard (2018): *Personvern. Publisering og behandling av personopplysninger.* Oslo: Gyldendal.

9 Den ser også hen til regjeringens nasjonale strategi for digital sikkerhet og delstrategien for digital sikkerhetskompetanse. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/. Sist besøkt 28.03.2023.

10 Se spesielt kapittel 5-9 i styringsdokumentet. https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/. Sist besøkt 28.03.2023.

11 Se fotnote 6.

Relevante dommer og uttalelser

Kravene som Kunnskapsdepartementets policy stiller til arbeidet med personvern (behandling av personopplysninger) er ikke statiske. Forståelsen av dem utvikler seg over tid. Særlig viktig i denne sammenheng, også i Norge, er dommer fra EU-domstolen. For å vite hvordan kravene i policyen skal tolkes og etterleves, kan det derfor være nødvendig å gjøre seg kjent med avgjørelser fra domstolen og lovtolkninger fra EUs generaladvokat.

Nedenfor gis en oversikt over GDPR-relevante dommer fra EU-domstolen og uttalelser fra generaladvokaten i 2023.

No 72/2023: 4. mai 2023. Judgment of the Court of Justice in Case C-300/21
- Om erstatning til den registrerte ved brudd på GDPR.

No 71/2023: 4. mai 2023. Judgment of the Court of Justice in Case C-487/21
- Om retten til å motta kopi av egne personopplysninger.

No 67/2023: 27. april 2023. Opinion of the Advocate General in the case C-340/21
- Om erstatningsansvar når behandlingsansvarlig gir tredjeparter tilgang til personopplysninger.

No 54/2023: 30. mars 2023. Judgment of the Court of Justice in Case C-34/21
- Om videostrømming av undervisning i skolen.

No 16/2023: 26. januar 2023. Judgment of the Court of Justice in Case C-205/21
- Om politiets innsamling av biometriske og genetiske opplysninger.

No 4/2023: 12. januar 2023. Judgment of the Court of Justice in Case C-154/21
- Om retten til å vite hvem mottaker av den registrertes opplysninger er.

No 3/2023: 12. Januar 2023. Judgment of the Court of Justice in Case C-132/21
- Om forholdet mellom administrative og sivilrettslige sanksjoner.

Se også Case C-60/22 (om retten til sletting), generaladvokatens uttalelse i Case C-807/21 (om vilkår for erstatning) og Case T-557/20 (om anonymisering og pseudonymisering av opplysninger).

Informasjonsverdier, trusler og sårbarheter

Drøftelsene i denne rapporten er organisert langs tre hoveddimensjoner:

Informasjonsverdier
Dette er de verdiene som arbeidet med informasjonssikkerhet og personvern skal beskytte mot fare, skade og uforsvarlig håndtering. Det handler primært om (i) data og opplysninger i forskning, undervisning, administrasjon og formidling, og (ii) dataressurser (datamaskiner og programvare, IT-tjenester, osv.) som benyttes til å utføre disse oppgavene.

I hvilken grad virksomhetene i sektoren har oversikt over sine informasjonsverdier, drøftes i kapittel 1 (universitetene og høgskolene) og kapittel 4 (øvrige virksomheter).

Trusler
Dette er kilder til fare, skade eller uforsvarlig håndtering av informasjonsverdier som arbeidet med informasjonssikkerhet og personvern er ment å forebygge, oppdage og håndtere. Eksempler på kilder til fare (trusler) er nettkriminelle grupper og statlige hackere.

Trusler mot informasjonssikkerheten og personvernet i sektoren drøftes i kapittel 2 (universitetene og høgskolene) og kapittel 4 (øvrige virksomheter).

Sårbarheter
Dette er svakheter eller mangler som kan utsette informasjonsverdiene for fare, skade eller uforsvarlig håndtering. Eksempler på vanlige sårbarheter er manglende kompetanse om lovlig behandling av personopplysninger, uklar organisering av arbeidet med informasjonssikkerhet og sikkerhetshull i dataprogrammer.

Sårbarheter i sektoren – og tiltak som er iverksatt for å utbedre sårbarhetene – drøftes i kapittel 3 (universitetene og høgskolene) og kapittel 4 (øvrige virksomheter).

Risiko, etterlevelse og anbefalinger

Risikoen for brudd på informasjons- og personopplysningssikkerheten vurderes i kapittel 5. Vurderingene bygger på drøftelsene i de foregående kapitlene.

I kapittel 5 vurderer vi også mulighetene for at målene om informasjonssikkerhet og personvern i sektorens strategi for digital omstilling kan realiseres.

Til slutt gir vi enkelte anbefalinger om sektortiltak som kan iverksettes for å redusere risiko, styrke policyetterlevelse og forbedre måloppnåelse.

Om begrensninger

Funn, vurderinger og konklusjoner i denne rapporten bygger primært på informasjon innhentet av HK-dir i møter med den enkelte virksomhet, se vedlegg 1. Det ble ikke er bedt om tilgang til interne dokumenter som beskriver virksomhetenes arbeid med informasjonssikkerhet og personvern.

Det er heller ikke gjennomført kontroller av personverntiltak eller tester av informasjonssikkerheten. Kvalitetssikring av det lokale arbeidet med informasjonssikkerhet og personvern må skje gjennom sikkerhetstester og etterlevelsesrevisjoner.

Vedlegg

Vedlegg 1: redegjørelse for datagrunnlaget som rapporten baserer seg på, og arbeidet med innsamling og analyse av datagrunnlaget.

Vedlegg 2: spørsmålene (kartleggingsskjemaet) som ble benyttet i kartleggingen av universitetene, høgskolene og de øvrige virksomhetene.

Vedlegg 3: rammeverket som ble benyttet ved vurdering av risiko for konkrete informasjonssikkerhets- og personvernhendelser.

Kapittel 1

Informasjonsverdier og digitale ressurser

Kapittel 1

Informasjonsverdier og digitale ressurser

Innledning

Grunnlaget for arbeidet med å etterleve kravene i departementets policy om informasjonssikkerhet og personvern, er å vite hva som omfattes av policyen – hva er det som skal sikres og håndteres på en sikker, forsvarlig og lovlig måte?

Her handler det i første omgang om oversikt over informasjonsverdier i form av personopplysninger, forskningsdata og annen viktig informasjon som sektoren behandler. Samtidig forvalter sektoren andre informasjonsverdier – datamaskiner, programvare, mobiltelefoner, nettverksutstyr, osv. – som det er viktig å ha oversikt over. Dersom disse verdiene går tapt, eksponeres for uvedkommende eller håndteres på ulovlig vis, kan det skade sektorens evne til å utføre sine kjerneoppgaver på en effektiv, forsvarlig og tillitsvekkende måte.

Det kan også få negative konsekvenser for enkeltpersoner og tredjeparter, for eksempel studenter, ansatte, eksterne samarbeidspartnere og deltakere i forskningsprosjekter.

I dette kapittelet ser vi nærmere på de informasjonsverdiene som arbeidet med informasjonssikkerhet og personvern har til hensikt å ivareta. Som tidligere år,[12] er formålet med kapitlet å vurdere i hvilken grad universitetene og høgskolene har tilfredsstillende oversikt over de informasjonsverdiene som omfattes av departementets policy.

Når det gjelder de sju siste virksomhetene som er underlagt policyen for informasjonssikkerhet og personvern, drøftes disse problemstillingene i kapittel fire.

Nedenfor følger først en kort drøftelse av verdiutviklingen i sektoren, det vil si digitaliseringen av ulike deler av virksomhetenes kjernevirksomhet.

Deretter drøftes i hvilken grad universitetene og høgskolene har den pålagte oversikten over sine informasjonsverdier, inkludert kunnskap som omfattes av regler om internasjonal kunnskapsoverføring og eksportkontroll.

12 Se for eksempel «Risiko- og tilstandsvurdering 2021», kapittel 1. https://hkdir.no/vaare-tenester/styring-av-informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning#content-section-6. Sist besøkt 07.03.2023.

Kort om digitalisering og verdivekst

I fjorårets risiko- og tilstandsvurdering ble det fremhevet at pandemien hadde medført et taktskifte i digitaliseringen hos universitetene og høgskolene. Taktskiftet var særlig knyttet til bruk av hjemmekontor, nettundervisning, digitale vurderingsformer, onlinemøter, nettbaserte disputaser og arrangementer.

En gjennomgang av saker behandlet i universitets- og høgskolestyrene de siste to årene, antyder også at tempoet i digitaliseringen har økt. Her fremgår det at tempoøkningen har skjedd relativt uavhengig av de særskilte tiltakene som ble iverksatt for å håndtere pandemisituasjonen.

Dersom vi ser på utvalgte årsrapporter for de to siste årene, kan det virke som at taktskiftet i den digitale omstillingen har vært særlig tydelig innen utdanningsområdet. Dette inkluderer etter- og videreutdanning, og omfatter også endringer i ulike typer vurderingsformer (disputaser, eksamen, sensur, osv.). Noen av disse endringene, for eksempel når det gjelder digitale disputaser, er reversert etter pandemien, mens andre i større grad virker å være beholdt (blant annet hjemmekontor og digital hjemmeeksamen).

I tillegg til undervisning, er formidling ett av kjerneområdene hvor årsrapportene vitner om at tempoet i digitaliseringen har vært høyt og hvor endringene beskrives som dyptgripende.

Administrasjon og virksomhetsstyring er områder hvor digital omstilling kan synes å være noe mindre uttalt enn i utdanning og formidling. I årsrapportene for 2021, opplyser institusjonene derfor om flere av de samme digitaliseringstiltakene som ble nevnt i rapportene fra året før. Det inkluderer blant annet digitale rutiner og bilagsflyt i regnskapsarbeidet, utvikling av digitale løsninger i arbeidsplanprosessen (datavarehus) og innføring av nettbaserte kvalitetsstyringssystemer.

Andre viktige administrative digitaliseringstiltak som nevnes i 2021-rapportene, inkluderer robotisering og automatisering av arbeidsprosesser. UiO regner for eksempel med at dette har ført til besparinger på 13-14 årsverk.[13]

For BOTT-universitetene er innføring av nye systemer innen sak og arkiv, lønn og økonomi viktige tiltak.

Forskning virker å være det kjerneområdet hvor årsrapportene opplyser om færrest konkrete digitaliseringstiltak. Viktige tiltak som likevel nevnes inkluderer oppgradering av «Norwegian Research and Education Cloud» og arbeidet med «Open Science». Flere institusjoner jobber også med digitale løsninger for samhandling med forskere ved andre universiteter eller høgskoler.

Selv om årsrapportene antyder at digitaliseringen er noe ulikt fordelt mellom kjerneområder, gir universitetene og høgskolene uttrykk for at det digitale «omstillingstrykket» kan være i ferd med å nå sin grense. Dette ble blant annet formidlet i svarene som universitetene og høgskolene ga til HK-dir da «Handlingsplan for digital omstilling i høyere utdanning og forskning» var på høring høsten 2022.

En tilnærmet samstemt tilbakemelding fra de institusjonene som svarte på høringen, var at digitalisering i sektoren, spesielt at flere store fellesprosjekter er iverksatt, setter den lokale omstillingskapasiteten under press. Tempoet i den digitale omstillingen bør, ifølge disse institusjonene, derfor ikke øke ytterligere.

Slike synspunkter indikerer flere forhold. For det første, at omfanget av de informasjonsverdier som omfattes av departementets policy for informasjonssikkerhet og personvern er økende. For det andre, at institusjonene blir mer avhengige av digital teknologi for å utføre sine kjerneoppgaver. Og, for det tredje, at konsekvensene kan bli mer omfattende dersom digitale systemer og tjenester utsettes for uønskede informasjonssikkerhets- eller personvernhendelser.

Det betyr at viktigheten av å ha oversikt over informasjonsverdiene øker samtidig som det kan bli mer krevende for institusjonene å etablere og vedlikeholde slike oversikter.

13 UiO årsrapport 2021, side 40. https://www.uio.no/om/strategi/planer-rapporter/uio-arsrapport-2021.pdf. Sist besøkt 07.03.2023.

«Verdilandskapet» – hovedtyper informasjonsverdier

I fjorårets rapport ble det gitt en oversikt over de 10 viktigste verdikategoriene som universiteter og høgskoler forvalter.[14] Oversikten inkluderte følgende informasjonsverdier:

1. **Studentadministrasjon**. Informasjon som typisk behandles i studentadministrative systemer.
2. **Læring, vurdering og undervisning**. Informasjon knyttet til gjennomføring og administrasjon av undervisning og eksamen eller andre vurderingsformer.
3. **Forskning og utvikling**. Informasjon om innholdet i, administrasjon og gjennomføringen av forskningsprosjekter.
4. **Medarbeidere og ledere**. Informasjon om ansettelsesforhold som blant annet behandles i HR-systemer.
5. **Økonomi og regnskap**. Informasjon om finansiering av virksomheten og forvaltning og styring av økonomiske verdier.
6. **Virksomhetsstyring og -strategi**. Informasjon om viktige forhold i virksomheten og planer for den videre administrative eller faglige utviklingen, for eksempel utviklingsavtaler med departementet.
7. **Eiendom og fysisk infrastruktur**. Informasjon om bygningsmessige forhold og andre deler av det fysiske miljøet.
8. **IT-ressurser og digital infrastruktur**. Informasjon om IT-ressurser (datamaskiner, programvare, nettverksutstyr, osv.) og forvaltning og styring av IT-porteføljen.
9. **Media og kommunikasjon**. Informasjon som benyttes i det interne og eksterne formidlings- og kommunikasjonsarbeidet.
10. **Alumni**. Kontaktinformasjon til tidligere studenter og annen relevant informasjon.

Det er primært verdier i kategoriene 1-6 og 8 som er rettslig regulert. Økonomi- og regnskapsinformasjon skal for eksempel behandles (og sikres) i henhold til økonomiregelverket i staten. Studentinformasjon omfattes av personvernlovgivningen og offentligrettslige reguleringer, mens FoU-informasjon kan være omfattet av regler om internasjonal kunnskapsoverføring (eksportkontroll). Informasjon knyttet til virksomhetsstyring og -strategi kan ha betydning for ivaretakelse av departementets krav til rapportering.

Personopplysninger som behandles i medisinsk og helsefaglig forskning er undergitt særlig forskningsetisk regulering.

14 Se «Risiko- og tilstandsvurdering 2022», side 16-18.

Verdiklassifisering

Hvordan universitetene og høgskolene klassifiserer sine informasjonsverdier med hensyn til viktighet eller kritikalitet, påvirkes av om de er omfattet av juridiske krav til håndtering og sikring (se tekstboksen ovenfor). Det er opp til den enkelte institusjon å vurdere viktigheten av andre typer informasjonsverdier enn de som er undergitt rettslig regulering.

Våre kartlegginger viser at vurderinger av viktighet (kritikalitet) kan variere noe mellom institusjoner, blant annet på grunn av forskjeller i forsknings- og utdanningsprofil. Det er likevel vanlig at slike vurderinger skjer på en relativt ensartet måte, det vil si med utgangspunkt i et felles rammeverk for verdiklassifisering.[15]

Mange institusjoner opplyser også om at de stiller krav til hvor informasjonen skal behandles og lagres. Viktig eller kritisk informasjon skal for eksempel behandles og lagres i IT-tjenester som er ekstra godt sikret mot brudd på informasjons- og personopplysningssikkerheten.

Inventarkontroll – oversikt over informasjonsverdier

Selv om det finnes rutiner og retningslinjer for klassifisering av informasjonsverdier, har universitetene og høgskolene etablert tilfredsstillende inventarkontroll? Har de utarbeidet dekkende og oppdaterte oversikter over verdier som omfattes av departementets policy?

Under kartleggingen i 2022 spurte vi institusjonene om dette. Vi var i første rekke opptatt av om de hadde oversikter over hvilke personopplysninger de behandler, men institusjonene opplyste også om de har oversikt over andre typer informasjonsverdier. I tillegg til IT-ressurser (maskiner, programvare, osv.), inkluderte det data innenfor sensitive forskningsområder, for eksempel navigasjons- og sensorteknologi, informatikk og datasikkerhet, romfart og satellitteknologi, undervannsteknologi, kryptografi, biovitenskap og materialteknologi.

Behandlingsprotokoll – universiteter og høgskoler

Personvernregelverket – personopplysningsloven og personvernforordningen (GDPR) – stiller krav om at universitetene og høgskolene har oversikt over personopplysninger som behandles innenfor de 10 virksomhetsområdene som nevnes i tekstboksen ovenfor. Oversikten, omtalt som behandlingsprotokollen, skal blant annet angi hvilke typer personopplysninger som behandles og hvem opplysningene gjelder.[16]

Figur 1 viser hvor mange universiteter og høgskoler som i 2022 oppga at de hadde utarbeidet en dekkende og oppdatert behandlingsprotokoll – og hvor mange som mente at de ikke hadde det.

Figuren viser at 10 universiteter og høgskoler opplyste om at behandlingsprotokollen var fullstendig og oppdatert. Dette er to flere enn i 2021.

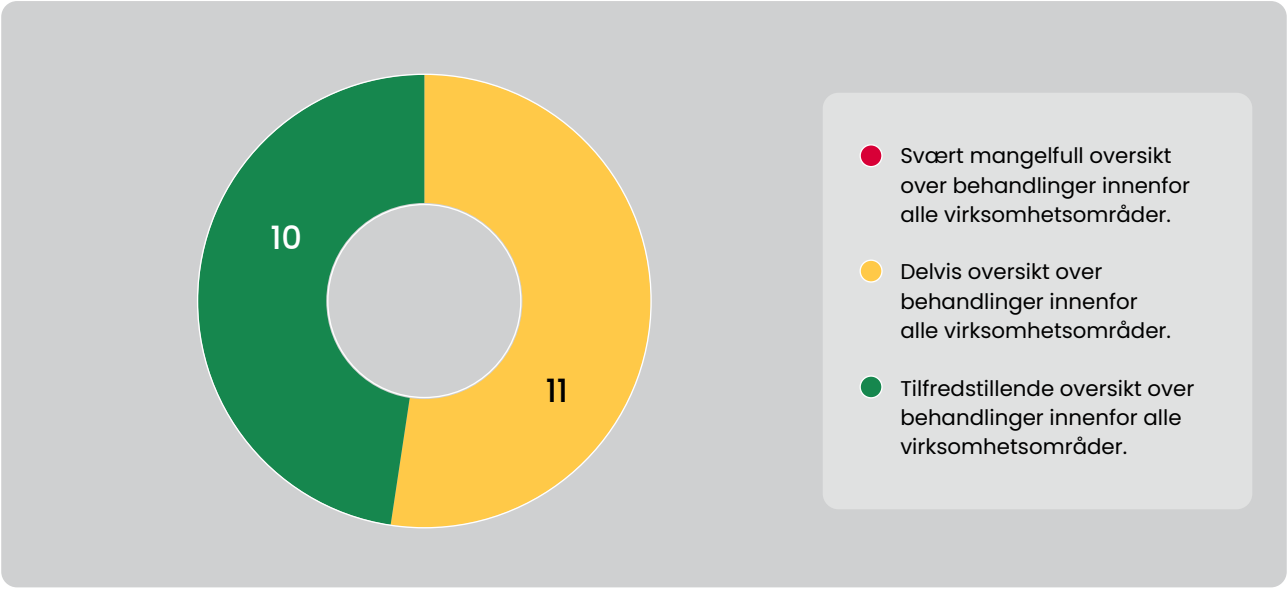
11 universiteter og høgskoler mente at behandlingsprotokollen var ufullstendig – ikke dekkende innenfor alle virksomhetsområder – eller at den ikke var oppdatert. I 2021 oppga 13 institusjoner at protokollen var ufullstendig eller ikke oppdatert.

Ingen av institusjonene mente at protokollen var generelt mangelfull. Det er det samme som i 2021.

15 Rammeverket ble utarbeidet av Uninett AS. Det er tilgjengelig på https://www.unit.no/klassifisering-av-informasjon-og-informasjonssikkerhet. Sist besøkt 07.03.2023.

16 For nærmere informasjon om kravene til behandlingsprotokoll, se Datatilsynets veiledning på https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/. Sist besøkt 28.03.2023.

Figur 1: Status for behandlingsprotokoll 2022, universiteter og høgskoler



Store og små institusjoner

De litt mindre og små institusjonene er godt representert blant de som oppga å ha en fullstendig og oppdatert behandlingsprotokoll. Tendensen til at de mindre institusjonene har noe bedre oversikt over personopplysninger enn de større forsterkes dersom vi inkluderer virksomhetene som drøftes i kapittel fire (de sju øvrige virksomhetene).

Det betyr at selv om de større institusjonene har flere ressurser å sette inn i arbeidet med informasjonssikkerhet og personvern, har de likevel utfordringer med å få oversikt over «verdilandskapet». Det kan skyldes at viktige deler av digitaliseringen – og den elektroniske behandlingen av personopplysninger – skjer desentralt, det vil si hos et stort antall fakulteter, institutter, forskningssentre og støttemiljøer. Behandlingene kan dermed bli lite oversiktlige, vanskelige å registrere og protokollen kan bli utfordrende å oppdatere.

Meldingsarkivet og andre protokolløsninger

Hos alle universitetene og høgskolene var det etablert en egen behandlingsprotokoll for forskning. Dette var Sikt sitt meldingsarkiv.[17] Meldingsarkivet er en fellestjeneste for registrering og gjennomgang av forsknings- og studentprosjekter som behandler personopplysninger. Prosjektene følges også opp av Sikt ved prosjektslutt, spesielt at opplysninger enten er anonymisert eller slettet.

I tillegg til Sikt sitt meldingsarkiv, hadde enkelte institusjoner utviklet egne applikasjoner for registrering av nøkkelinformasjon om forsknings- og studentprosjekter.

Innenfor de øvrige virksomhetsområdene, spesielt undervisning og administrasjon, tilbys ikke en tilsvarende fellestjeneste som Sikt sitt meldingsarkiv. Institusjonene må derfor finne sine egne protokolløsninger, vanligvis i form av Excel-ark eller kommersielt tilgjengelige protokollverktøy. Ifølge flertallet av institusjonene, fører dette til at behandlingsprotokollen i undervisning og administrasjon er noe mer mangelfull enn i forsknings- og studentprosjekter.

17 Informasjon om meldingsarkivet og øvrige personverntjenester som Sikt tilbyr, er tilgjengelig her: https://sikt.no/tjenester/personverntjenester-forskning. Sist besøkt 08.03.2023.

Andre informasjonsverdier enn personopplysninger

I forsknings- og utviklingsaktiviteter behandler universitetene og høgskolene en rekke andre informasjonsverdier enn personopplysninger. Det gjelder blant annet vær- og klimadata, maritime data og geologiske data, men også data innen forskningsfelt som navigasjons- og sensorteknologi, romfart og satellitteknologi, undervannsteknologi og biovitenskap.[18]

I våre årlige kartlegginger har vi vært opptatt av om institusjonene har oversikt over informasjonsverdier i forskning og utvikling som ikke er personopplysninger.

Konsoliderte oversikter

Vi har tidligere registrert at det i begrenset grad finnes slike oversikter. I løpet av de siste årene har imidlertid flere institusjoner opplyst om at de vil kartlegge andre informasjonsverdier i forskning enn personopplysninger. Frem til i år har vårt inntrykk vært at planlagte kartlegginger ofte ikke blir gjennomført.

Under årets kartlegging opplyste imidlertid åtte institusjoner om at de hadde gjennomført eller var i ferd med å gjennomføre større kartleggingsprosjekter. Flere av prosjektene inkluderte personopplysninger, men omfattet også forskningsdata som ikke er personopplysninger.

Utfordringen som institusjonene beskriver er at hvert enkelt forsknings- eller utviklingsprosjekt har oversikt over egne informasjonsverdier, inkludert digitale infrastrukturtjenester som anvendes. Institusjonene har likevel behov for å konsolidere disse prosjektoversiktene i fellesoversikter på virksomhetsnivå.[19] Det var dette de pågående kartleggingsprosjektene er ment å etablere.

Inventarkontroll – datamaskiner, programvare og IT-tjenester

Nytt av året, er at universitetene og høgskolene ble spurt om de har inventarkontroll når det gjelder digitale ressurser og utstyr: har institusjonene oversikt over datamaskiner og programvare som finnes i datanettverket deres og IT-tjenester som medarbeiderne benytter i arbeidet?

Omkring halvparten av institusjonene mente at de hadde tilfredsstillende inventarkontroll med hensyn til digitale ressurser og utstyr. Oversiktene forelå i form av sentrale inventarregistre hos IT-avdelingene. Her dreide det seg om system- eller tjenesteregistre, programvarekataloger og registre over sluttbrukerutstyr (datamaskiner, mobiltelefoner, osv.). Oversiktene besto typisk av digitale ressurser og utstyr som IT-avdelingene var ansvarlige for, og applikasjoner eller tjenester som lokale enheter meldte inn til IT-avdelingene, for eksempel fordi bruken formelt måtte godkjennes av IT-avdelingene.

I tillegg opplyste disse institusjonene om at det ble benyttet tekniske verktøy, for eksempel «Microsoft Defender» eller «Intune», for å oppdage og registrere applikasjoner som ikke var meldt til IT-avdelingene.

Slike sentrale inventarregistre forelå også hos de øvrige universitetene og høgskolene. Her ble det imidlertid gitt uttrykk for at inventarkontrollen hadde enkelte mangler. Det handlet

18 Hvilke forskningsområder som vurderes som særskilt betydningsfulle, omtales i «Langtidsplan for forskning og høyere utdanning 2019-2029». Det gjelder områdene (i) hav, (ii) klima, miljø, miljøvennlig energi, (iii) fornyelse i offentlig sektor og bedre offentlige tjenester, (iv) muliggjørende og industrielle teknologier og (v) samfunnssikkerhet og samhørighet i en globalisert verden. https://www.regjeringen.no/no/dokumenter/meld.-st.-4-20182019/id2614131/. Sist besøkt 08.03.2023.

19 Tilsvarende utfordringer drøftes i sluttrapport fra utredningsgruppen som har vurdert problemstillinger og muligheter knyttet til deling og gjenbruk av forskningsdata. Se «Infrastruktur og tjenester for FAIR forskningsdata – status og forslag til videre arbeid». https://www.openscience.no/oa-i-norge/felles-infrastruktur-og-tjenester-fair-forskningsdata. Sist besøkt 08.03.2023.

vanligvis om at oversikten over digitale ressurser og utstyr på enhetsnivå (fakulteter, institutter, osv.) ikke er like uttømmende og oppdaterte som når det gjaldt ressurser og utstyr i fellesadministrasjonen.

Det ble også i år rapportert om utfordringer knyttet til «skygge-IT». Dette er IT-tjenester som ansatte (spesielt vitenskapelig ansatte) tar i bruk uten formell godkjenning og uten at institusjonen er kjent med bruken. Det innebærer for eksempel at behandlinger av personopplysninger ved bruk av «skygge-IT» ikke ble registrert i behandlingsprotokollen.

Det var likevel flere institusjoner enn tidligere som opplyste om at de hadde forbedret sin evne til å oppdage ikke-godkjent bruk av IT-tjenester og applikasjoner, blant annet ved hjelp av tekniske kartleggingsverktøy. Problematikken med bruk av «skygge-IT» fremsto derfor som noe redusert sammenliknet med hva som tidligere har blitt rapportert.

Internasjonal kunnskapsoverføring og eksportkontroll

Oversikter over forskningsdata på enhetsnivå (fakulteter, institutter, osv.) som omfattes av regler for internasjonal kunnskapsoverføring (eksportkontroll), ble også vurdert som noe mangelfulle. Eksportkontrollregelverket innebærer at institusjonene må søke Utenriksdepartementet om lisens for overføring av kunnskap som har eller kan ha militære anvendelsesområder.[20] Dette skal sikre at kunnskapsoverføringer skjer i tråd med norske sikkerhets- og forsvarsinteresser, og ivaretar Norges internasjonale forpliktelser.[21]

I år rapporterte ni institusjoner om at de hadde iverksatt tiltak, spesielt kartlegginger på enhetsnivå, for å få oversikt over kunnskap som omfattes av reglene om internasjonal kunnskapsoverføring.

12 institusjoner ga ikke uttrykk for at det var iverksatt eller gjennomført liknende kartlegginger i 2022. Mange av disse institusjonene har trolig heller ikke behov for slike tiltak: de forvalter ikke (eller i liten grad) kunnskap som omfattes av overføringsbegrensninger.[22] Det er derfor ikke overraskende at spesielt de mindre høgskolene ikke opplyste om denne typen kartlegginger.

---

20 Se «Retningslinjer for kontroll med kunnskapsoverføring» (UD). https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/. Sist besøkt 09.03.2023.

21 Formålet med og hovedinnholdet i regelverket omtales blant annet i «Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor», kapittel 9. Se https://www.regjeringen.no/contentassets/48beea7da45f4918bfaef82f411b7cb3/no/pdfs/revidert-styringsdok-sikkerhet_godkjent.pdf. Sist besøkt 09.03.2023. Jf. også «Panorama 2021-2027», side 12. https://www.regjeringen.no/contentassets/13e7862e6c064321af97fe0c58a8f7cb/f-4462-b_panorama_strategi.pdf. Sist besøkt 09.03.2023. HK-dir og Norges forskningsråd har utarbeidet forslag til retningslinjer for ansvarlig internasjonalt samarbeid. Forslaget ble sendt på høring i sektoren i februar 2023. Se https://hkdir.no/vaare-tenester/retningslinjer-for-ansvarlig-internasjonalt-samarbeid#content-section-0. Sist besøkt 09.03.2023.

22 For eksempel innen forskningsområder som materialteknologi, biovitenskap, robotikk, informatikk og datasikkerhet, navigasjons- og sensorteknologi, kryptografi og undervannsteknologi.

Oppsummering og anbefalinger

Utgangspunktet for arbeidet med etterlevelse av departementets policy for informasjonssikkerhet og personvern, er at universitetene og høgskolene har oversikt over de informasjonsverdiene som omfattes av policyen.

Ovenfor har vi sett at de 21 institusjonene har enkelte mangler når det gjelder inventarkontroll – oversikt over sine informasjonsverdier. Det skyldes i noen grad taktskiftet i digitaliseringen som har skjedd i løpet av de siste årene.

Sektoren er likevel i ferd med å etablere tilfredsstillende oversikter over behandling av personopplysninger, og flere institusjoner enn tidligere opplyste om at protokollen nå er fullstendig og oppdatert. Behandlingsprotokollene var mest komplett i forskning, inkludert studentforskning. Én viktig årsak til dette er at det er etablert en fellestjeneste – Sikt sitt meldingsarkiv – hvor behandlinger i forskning kan registreres og administreres.

Innenfor andre virksomhetsområder, særlig administrasjon og undervisning, opplyste omkring halvparten av universitetene og høgskolene om at protokollen ikke er fullstendig og oppdatert. Det samme gjaldt i forsknings- eller utviklingsprosjekter hvor det ikke behandles personopplysninger. Her ble mangel på verktøystøtte – løsninger for registrering og vedlikehold av verdioversikter – oppgitt å være en viktig utfordring.

Flere institusjoner enn tidligere hadde likevel iverksatt kartleggingsprosjekter innen forskningsområder hvor det kan finnes informasjonsverdier som er undergitt regler om internasjonal kunnskapsoverføring og eksportkontroll.

Omkring halvparten av institusjonene mente at de hadde tilfredsstillende inventarkontroll med hensyn til digitale ressurser (programvare, nettjenester) og IT-utstyr (datamaskiner, mobiltelefoner, osv.).

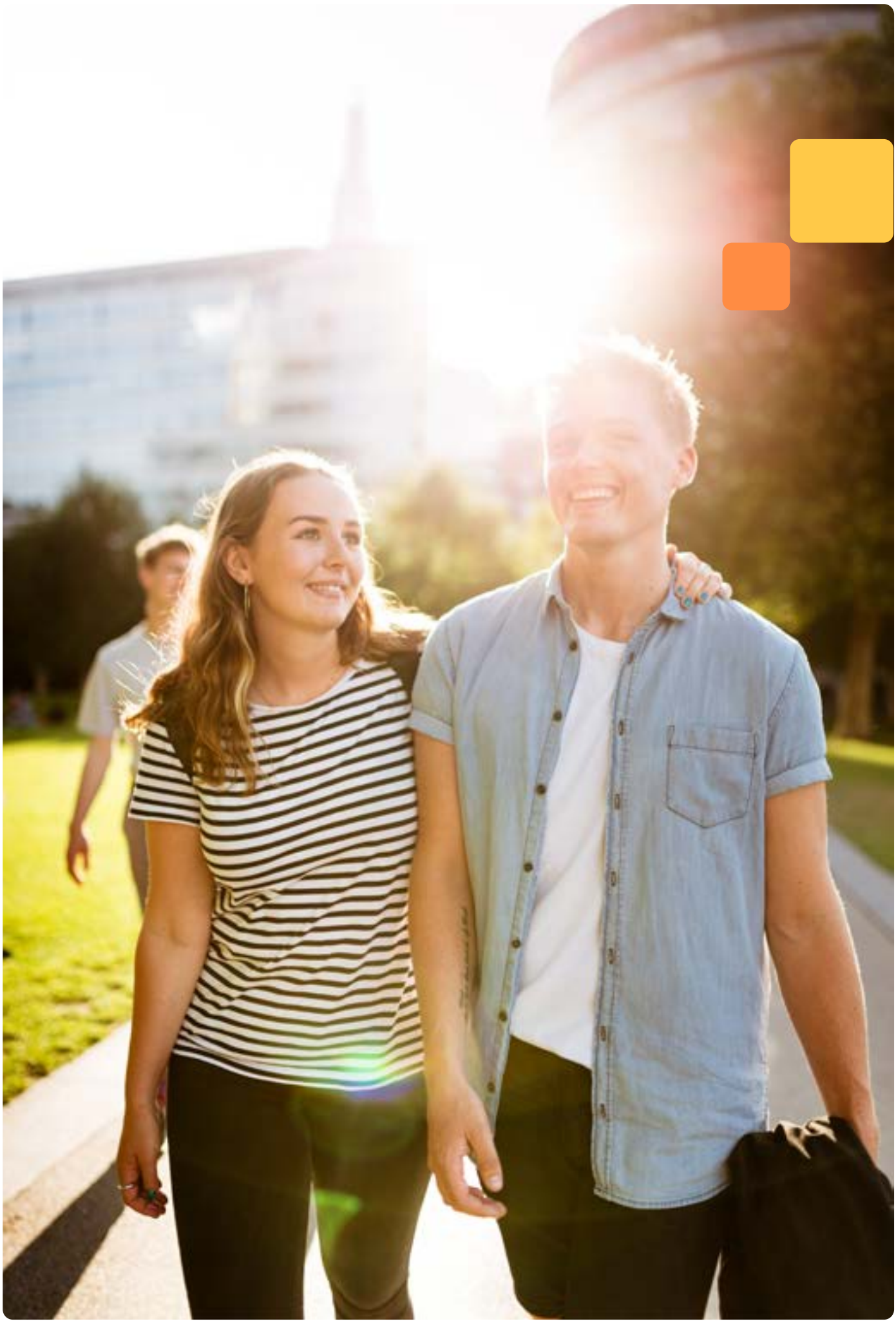
Med bakgrunn i funnene diskutert i dette kapitlet, mener vi at anbefalingene fra fjorårets risiko- og tilstandsvurdering fortsatt er gyldige.

Vi anbefaler derfor at det iverksettes tiltak for å gi institusjonene konkret veiledning om

(i) hvordan oversikter over informasjonsverdier bør være, spesielt innholdselementer og detaljeringsgrad, og
(ii) hvordan kartlegging og vedlikehold av verdioversikter best kan gjennomføres i praksis, inkludert hvilke arbeidsverktøy som kan benyttes.

Veiledningen kan skje med utgangspunkt i allerede eksisterende informasjonsmateriell utarbeidet av Sikt.[23]

23 Se https://sikt.no/anbefalinger-sikkerhet-og-beredskap. Sist besøkt 28.03.2023.



Kapittel 2

Universiteter og høgskoler – brudd og hendelser

Kapittel 2

Universiteter og høgskoler – brudd og hendelser

Innledning

I hvilken grad ble informasjonsverdier utsatt for tilsiktede eller utilsiktede brudd på informasjonssikkerheten og krenkelser av personvernet i 2022? Hvor mange brudd og hendelser ble registrert hos universitetene og høgskolene, og hvilke skadevirkninger (om noen) førte de til?

I dette kapitlet drøftes disse spørsmålene. Kapitlet gir en oversikt over omfanget av og typer brudd og hendelser som universitetene og høgskolene rapporterte om. Dette gir innsikt i hvilke trusler som institusjonenes informasjonsverdier utsettes for, og er viktig for å vurdere risiko for fremtidige brudd og hendelser. Det vil også ha betydning for hvilke forbedringstiltak som bør prioriteres, både på sektor- og virksomhetsnivå.

Brudd og hendelser utløses av «kilder til fare» (trusselkilder[24]).

Når det gjelder informasjons- og personopplysningssikkerheten kan det dreie seg om eksterne trusler, for eksempel tilsiktede brudd eller hendelser som nettkriminelle grupper og statlige hackere (APT[25]) står bak. Det kan også dreie seg om utilsiktede brudd på informasjonssikkerheten eller krenkelser av personvernet som skyldes tekniske eller menneskelige feil og uhell.

---

24 Denne definisjonen av trusler er hentet fra Direktoratet for digitalisering sin begrepsliste. https://internkontroll-infosikkerhet.difi.no/begrepsliste#Trusler%20eller%20trusselkilder. Sist besøkt 07.03.2023.

25 APT (Advanced Persistent Threats) er trusselaktører som "(…) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time". https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. Sist besøkt 07.03.2023. I denne rapporten benyttes APT om statlige eller statsstøttede grupper. Se også Kristian Malmkvist Eie (2020): «Trusler og etterretning». I Håkon Bergsjø, Ronny Windvik og Lasse Øverlier (red.): Digital sikkerhet. En innføring. Oslo: Universitetsforlaget. Side 154-155.

I tillegg kan det finnes en rekke andre «kilder til fare» (for eksempel inkompetente tjenesteleverandører, oversvømmelser, brann i datarom, osv.).

I det følgende gis først en kort oversikt over endringer i det generelle trusselbildet i samfunnet, spesielt EOS-tjenestenes vurderinger av trusler mot norske virksomheter.

Deretter gis en oversikt over informasjonssikkerhetsbrudd og -hendelser som de 21 universitetene og høgskolene opplyste om i 2022, og endringer sammenliknet med 2021.

Til slutt gis en oversikt over personvernhendelser og avvik som universitetene og høgskolene rapporterte om.

Definisjoner – brudd og hendelser

Med brudd menes at informasjonsverdier faktisk ble utsatt for uautorisert tilgang, skade, ødeleggelse eller utilgjengelighet.[26] Datainntrenging eller dataangrep er eksempler på brudd. Brudd omfatter også krenkelser av personvernet på grunn av (i) ulovlig behandling av personopplysninger eller (ii) avvik fra interne rutiner for behandling av opplysninger.

Med hendelser menes tilfeller (tilsiktet eller utilsiktet) hvor informasjonsverdier har vært i fare for uautorisert tilgang, skade, ødeleggelse eller utilgjengelighet, men hvor dette likevel ikke har skjedd. Forsøk på datainntrenging eller dataangrep er eksempler på hendelser. Det omfatter også ulovlig behandling av personopplysninger eller behandlinger i strid med interne rutiner, men hvor det ikke ble rapportert om krenkelser av personvernet.

26 Se for eksempel Kristian Malmkvist Eie (2020): «Trusler og etterretning». I Håkon Bergsjø, Ronny Windvik og Lasse Øverlier (red.): *Digital sikkerhet. En innføring.* Oslo: Universitetsforlaget. Se også Håkon Bergsjø og Ronny Windvik (2018): *Datasikkerhet for ledere. Hvordan beskytte din virksomhet.* Oslo: Universitetsforlaget. Side 25-27.

EOS-tjenestene – risiko- og trusselvurderinger 2022

EOS-tjenestene[27] har over flere år vurdert statlig etterretningsvirksomhet som en av de viktigste truslene mot norske interesser og virksomheter, inkludert virksomheter i UH-sektoren. Dette budskapet forsterkes i tjenestenes vurderinger for 2023, spesielt med bakgrunn i Ukraina-konflikten.

EOS-tjenestene er også i år samstemte i sin vurdering av at Russland og Kina – og i noe mindre grad Iran og Nord-Korea – er de viktigste etterretningstruslene mot norske virksomheter.[28] Det nevnes for eksempel at Kina gjerne benytter akademiske institusjoner som verktøy for innhenting av strategisk viktig teknologi og kunnskap i utlandet. Høyteknologi som kan brukes både til sivile og militære formål er særlig ettertraktet.[29] I Khrono har det vært spekulasjoner om dette kan være noe av bakgrunnen for at kinesiske universiteter tilknyttet landets væpnede styrker søker forskningssamarbeid med norske (og nordiske) UH-institusjoner.[30]

EOS-tjenestene tillegger innsidevirksomhet, illegalister og rekruttering av norske borgere større oppmerksomhet i sine siste risiko- og trusselvurderinger enn tidligere. For UH-sektoren er denne trusselen relevant. I oktober 2022 ble en gjesteforsker ved UiT pågrepet mistenkt for å være russisk etterretningsoffiser, og i november samme år ble en iransk-tysk NTNU-professor dømt for brudd på eksportkontrollregelverket.[31]

Videre nevner EOS-tjenestene flere utviklingstrekk som utfordrer norske virksomheters evne til å håndtere trusselbildet. Eksempler på dette er økende avhengighet av digital infrastruktur og digitale tjenester, lange og komplekse leverandørkjeder og sårbarheter i vanlig brukt maskin- og programvare. Nasjonal sikkerhetsmyndighet understreker betydningen av at virksomheter har oversikt over sine informasjonsverdier.

Dette påpekes også av NSM i «Sikkerhetsfaglig råd». I tillegg fremhever NSM at økende avhengighet av IT-løsninger og digital infrastruktur, sammen med kontinuerlige «ondsinnede cyperoperasjoner» rettet mot norske virksomheter, øker risikoen for brudd på informasjonssikkerheten.[32]

Utsatte teknologi- og forskningsområder

Alle de tre EOS-tjenestene mener at en rekke teknologi- og forskningsområder kan være utsatt for cyberoperasjoner fra fremmede stater.[33] Figur 2 gir en oversikt over hvilke områder dette dreier seg om.

I tillegg mener EOS-tjenestene[34] at andre lands etterretning kan være interesserte i opplysninger om dissidenter eller flyktninger i Norge. Dette kan være relevant for UH-institusjoner med studenter eller forskere fra særlig utsatte land.

---

27 Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Etterretningstjenesten (E-tjenesten).

28 PST nevner i tillegg Pakistan i årets åpne trusselvurdering. Også private sikkerhetsselskaper advarer mot etterretningstrusselen fra de nevnte landene i 2023. Se for eksempel «Mandiant Cyber Security Forecast 2023». Mandiant Cyber Security Forecast 2023 | Mandiant. Sist besøkt 13.03.2023.

29 Se «Nasjonal trusselvurdering 2023», side 12-16. _globalassets_ntv_2023_ntv_2023_nor_web (3).pdf. Sist besøkt 13.03.2023.

30 Se for eksempel Advarer om gjeste¬forskere fra sju kinesiske universiteter (khrono.no). Sist besøkt 13.03.2023.

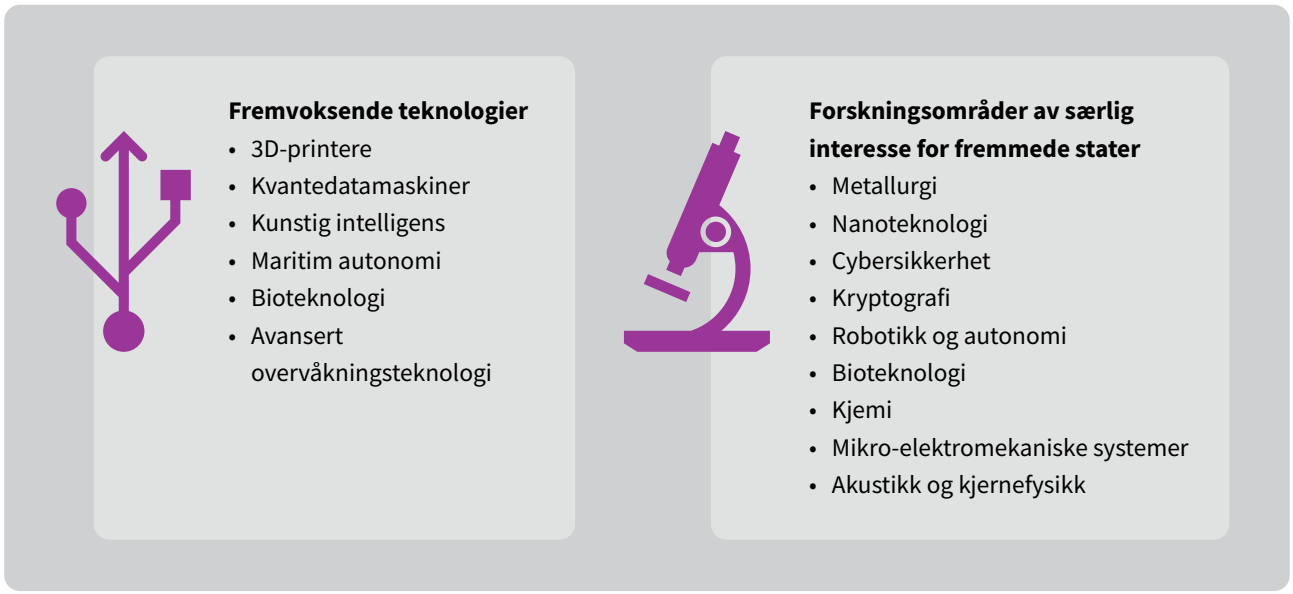
31 Se «Nasjonal trusselvurdering 2023», side 20. _globalassets_ntv_2023_ntv_2023_nor_web (3).pdf. Sist besøkt 13.03.2023.

32 Se «Sikkerhetsfaglig råd. Et motstandsdyktig Norge», side 53-57. Sikkerhetsfaglig råd - Et motstandsdyktig Norge - Nasjonal sikkerhetsmyndighet (nsm.no). Sist besøkt 18.05.2023.

33 Se «Nasjonal trusselvurdering 2023», side 21-22. _globalassets_ntv_2023_ntv_2023_nor_web (3).pdf. Sist besøkt 07.03.2023.

34 Se «Nasjonal trusselvurdering 2023», side 20-21. _globalassets_ntv_2023_ntv_2023_nor_web (3).pdf. Sist besøkt 07.03.2023.

Figur 2: Fremvoksende teknologier og forskningsområder av særlig interesse for fremmede stater



Det digitale trusselbildet

I NSM sin siste risikovurdering oppgis det at i 2022 har antallet alvorlige digitale sikkerhetshendelser holdt seg på samme nivå som i 2021. Antallet brudd (vellykkede dataangrep) var imidlertid lavere enn i 2021. Statlige eller statsstøttede hackergrupper sto, ifølge NSM, bak flere av hendelsene.[35]

NSM viser blant annet til tjenestenektangrep mot flere nettsteder tilhørende norske virksomheter og myndigheter i juni 2022.[36] Det vises i tillegg til at nettkriminelle grupper har gjennomført andre typer dataangrep mot norske virksomheter, blant annet Stangeland,[37] Domeneshop[38] og Norkart.[39]

Økonomisk nettkriminalitet

I Økokrim sin siste trusselvurdering legges det også stor vekt på trusselen som nettkriminelle aktører representerer.[40] Økokrim mener at løsepengevirus[41] og datainnbrudd hvor personopplysninger eller annen sensitiv informasjon stjeles og selges på det mørke nettet, utgjør en betydelig trussel mot norske virksomheter. I politiets trusselvurdering for 2022 fremheves nettfiske, løsepengevirus og datainnbrudd som viktige trusler.[42]

Internasjonale studier underbygger Økokrim og politiet sine vurderinger.[43] Verizon oppgir for eksempel at 95 prosent av bruddene på informasjonssikkerheten og krenkelsene av personvernet i utdanningssektoren internasjonalt er økonomisk motivert.[44] Spesielt løsepengevirus vurderes å være en økende trussel.

I USA vurderes kompetanse og bevissthet om trusler mot informasjonssikkerheten og personvernet, spesielt nettkriminalitet som løsepengevirus, å være den nest viktigste barrieren mot vellykket digitalisering i høyere utdanning og forskning.[45]

35 Se «Risiko 2023», side 18-21. Risiko 2023 - Nasjonal sikkerhetsmyndighet.pdf (nsm.no). Sist besøkt 07.03.2023.

36 Se for eksempel Større dataangrep mot Norge: – Kriminell, prorussisk gruppering står bak (aftenposten.no). Sist besøkt 07.03.2023.

37 Se for eksempel Stangeland rammet av dataangrep – Dagsavisen. Sist besøkt 07.03.2023.

38 Se for eksempel Datainnbrudd hos Domeneshop – Siste nytt – NRK. Sist besøkt 07.03.2023.

39 Se for eksempel Gigantisk dataangrep: - Tar saken veldig alvorlig (tv2.no). Sist besøkt 07.03.2023.

40 «Nasjonal risikovurdering 2022», side 17-18. Nasjonal risikovurdering 2022 - Økokrim (okokrim.no). Sist besøkt 07.03.2023.

41 Også ENISA – EUs organ for cybersikkerhet – fremhever løsepengevirus som den viktigste trusselen mot informasjonssikkerheten i EU-området. Se «ENISA Threat Landscape 2022», https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. Sist besøkt 21.05.2023.

42 Se «Politiets trusselvurdering 2022», side 40-42. politiets-trusselvurdering-2022.pdf. Sist besøkt 10.03.2023.

43 Se også Europol: «Internet Organised Crime Threat Assessment», https://www.europol.europa.eu/publications-events/main-reports/iocta-report. Sist besøkt 21.05.2023.

44 Verizon: «2022 Data Breach Investigations Report», side 57-58. 2022-data-breach-investigations-report-dbir.pdf (verizon.com). Sist besøkt 13.03.2023.

45 Se Top 10 IT Issues, 2023: Foundation Models | EDUCAUSE. Sist besøkt 13.03.2023.

Informasjonssikkerhet – brudd og hendelser i 2022

I hvilken grad rapporterte universitetene og høgskolene om de samme truslene og hendelsene som er beskrevet ovenfor? Dette spørsmålet drøftes i resten av kapitlet.

Alle de 21 universitetene og høgskolene opplyste om at de i løpet av fjoråret hadde vært utsatt for flere av de samme typene brudd eller hendelser som er drøftet ovenfor. Totalt opplyste universitetene og høgskolene om ca. 1450 brudd og hendelser i 2022.

Totaltallet på ca. 1450 inkluderer ikke brudd på sikkerheten til personopplysninger som er meldepliktig til Datatilsynet eller andre typer personvernavvik, for eksempel manglende sletting av personopplysninger eller mangelfulle vurderinger av det rettslige grunnlaget for behandling av personopplysninger. Omfanget av slike hendelser og avvik drøftes senere i kapitlet.

Om rapporteringen

I kartleggingen for 2022 ble ikke institusjonene bedt om å rapportere på forhåndsdefinerte brudd eller hendelser. Vi ba isteden om at institusjonene ga en oversikt over hvilke brudd og hendelser de hadde vært utsatt for, og som de selv mente det var verdt å nevne (se vedlegg 2). Det ble derfor rapportert på noe ulik måte fra de forskjellige institusjonene. I enkelte tilfeller førte dette til at vi har vært i tvil om hvordan rapporterte brudd og hendelser skal forstås: hvilke brudd eller hendelser er det snakk om? Likevel mener vi at fremstillingen nedenfor gir et rimelig dekkende bilde av sektortilstanden, slik den ble rapportert til HK-dir.

Det totale antallet brudd og hendelser inkluderer ikke rapporteringer hvor antallet ble oppgitt på en svært omtrentlig måte, for eksempel «gjentatte forsøk på nettfiske». Totaltallet inkluderer kun brudd eller hendelser hvor det ble rapportert et konkret tall eller hvor det ble gitt presise nok anslag til å få et tydelig bilde av omfanget, for eksempel «et par kompromitterte brukerkontoer».

Nedgang i rapporterte hendelser og brudd

Fra 2021 til 2022 ble antallet informasjonssikkerhetshendelser og -brudd hos universitetene og høgskolene redusert med omkring 30 prosent. 2022 er dermed det første året hvor vi har registret en reduksjon i antallet hendelser og brudd i denne delen av sektoren.

12 av de 21 universitetene og høgskolene opplyste om en reduksjon i antallet brudd og hendelser sammenlignet med 2021. De ni siste institusjonene rapporterte om en viss økning, men det var snakk om små endringer fra året før.

Det var de største institusjonene som rapporterte om flest hendelser og brudd. Dette er i overenstemmelse med funn fra tidligere års kartlegginger. Hovedårsaken til nedgangen i rapporterte brudd og hendelser er å finne hos de største institusjonene. Under fjorårets kartlegging opplyste for eksempel ett av de største universitetene om at den gjennomsnittlige årlige økningen i antall brudd og hendelser hadde vært på 26 prosent i perioden 2017-2020, og på hele 31 prosent i 2021. Fra 2021 til 2022 hadde denne trenden snudd. Da oppga den aktuelle institusjonen at antallet brudd og hendelser var redusert med 52 prosent.

Hos en annen større institusjon ble det rapporterte om 21 prosent færre brudd og hendelser enn i 2021.

Varierende oppdagelsesevne

Det store flertallet av rapporterte brudd og hendelser hos universitetene og høgskolene handlet også i 2022 om IT-sikkerhet, spesielt nettbaserte hendelser. De resterende tilfellene gjaldt i hovedsak utilsiktede feil og uhell (menneskelige og tekniske).

Etter som forhold knyttet til IT-sikkerhet utgjorde den klart største hendelseskategorien, vil evnen til å oppdage og håndtere denne typen brudd og hendelser påvirke rapporteringen: desto bedre evne institusjonene har til å identifisere uønsket IT-sikkerhetsaktivitet, jo flere brudd og hendelser vil bli registrert.

Variasjoner i rapporteringen – de store institusjonene registrerer flere hendelser og brudd enn de mindre – kan derfor i noen grad skyldes at de største har opprettet egne IT-sikkerhetsmiljøer og investert i avansert teknisk oppdagelsesutstyr. De øvrige institusjonene har ikke tilsvarende spesialiserte IT-sikkerhetsmiljøer. Dermed har de heller ikke den samme kapasiteten til å oppdage og rapportere om IT-sikkerhetshendelser som de største har.

I neste kapittel skal vi se at også de mindre universitetene og høgskolene har styrket sin evne til å oppdage uønsket IT-sikkerhetsaktivitet.

Typer hendelser og skadevirkninger

Nedenfor ser vi litt nærmere på de viktigste bruddene og hendelsene som universitetene og høgskolene rapporterte om i 2022, og i hvilken grad de førte til skadevirkninger.

De største institusjonene
Hos de største institusjonene, som registrerer flest hendelser og brudd, ble det rapportert om få eller ingen vesentlige skadevirkninger.

Én av disse institusjonene opplyste om fire sannsynlige forsøk på løsepengevirusangrep. Hos en annen større institusjon ble det rapportert om to sannsynlige forsøk på dette. I ett av tilfellene ble data kryptert, men de kunne gjenopprettes fra sikkerhetskopi. I de øvrige (sannsynlige) løsepengevirussakene ble ikke data kryptert.

I tillegg rapporterte én av de største institusjonene om et tjenestenektangrep (DDOS) som trolig hadde sin bakgrunn i krigen i Ukraina. Heller ikke denne hendelsen medførte vesentlige skadevirkninger.

Kompromitterte brukerkontoer utgjorde fortsatt en viktig del av sikkerhetsbruddene hos de største institusjonene, men antallet var redusert sammenliknet med tidligere år.

Øvrige institusjoner
De øvrige universitetene og høgskolene, som rapporterte om relativt få hendelser og brudd, utgjorde nettkriminalitet den klart største kategorien. Dette handlet primært om ulike typer nettsvindel, spesielt direktør- eller fakturasvindel, og sammenfaller med hva vi har funnet i tidligere kartlegginger. Det sammenfaller også med internasjonale trender i utdanningssektoren.[46]

Forsøkene på nettsvindel førte vanligvis ikke til skadevirkninger, for eksempel utbetaling av penger til nettkriminelle grupper. Det ble likevel rapportert om enkelte tilfeller hvor dette hadde skjedd (kjøp av gavekort). Det mest alvorlige tilfellet gjaldt urettmessig utbetaling av en månedslønn (dekanlønn).

Flertallet av de øvrige institusjonene rapporterte om nedgang i antallet kompromitterte brukerkontoer i 2022. Det ble også rapportert om ett sannsynlig og mislykket forsøk på løsepengevirusangrep.

APT-hendelser – statlig og statsstøttet hacking
Universitetene og høgskolene ble bedt å opplyse om de hadde vært utsatt for bekreftede eller mistenkte APT-hendelser: datatyveri eller kunnskapsspionasje utført av statlige eller statsstøttede hackergrupper (nettkriminelle grupper som utfører oppdrag for statlige myndigheter).[47]

I 2021 rapporterte seks institusjoner om bekreftede APT-hendelser.[48] Åtte andre institusjoner rapporterte om mistenkte hendelser. I 2022 var denne typen trusselaktivitet vesentlig redusert sammenliknet med året før: to institusjoner opplyste om til sammen fire mistenkte APT-hendelser.[49]

Tre av de mistenkte APT-hendelsene hadde ikke medført vesentlige skadevirkninger, blant annet fordi det dreide seg digital kartleggingsaktivitet (rekognosering[50]).

Den siste hendelsen fikk stor medieoppmerksomhet i 2022, og gjelder en påstått brasiliansk gjesteforsker som mistenkes å være tilknyttet russisk militæretterretning. Saken etterforskes nå av PST.

---

46 Verizon: «2022 Data Breach Investigations Report», side 57-58. 2022-data-breach-investigations-report-dbir.pdf (verizon.com). Sist besøkt 13.03.2023.

47 Se for eksempel Ben Buchanan (2020): «The Hacker and the State: Cyber Attack and the New Normal of Geopolitics». Cambridge, Mass.: Harvard University Press, eller Luca Follis og Adam Fish (2020): «Hacker States». Cambridge, Mass.: The MIT Press. Se også Fire-Eye: «M-Trends 2022». M-Trends-2022-Report.pdf (widen.net). Sist besøkt 18.05.2023.

48 I det mest alvorlige tilfellet lyktes trussel-aktøren med å ta kontroll over institusjonens datanettverk. Informasjon fra flere epostkontoer ble hentet ut. Epostkontoene tilhørte institusjonsledelsen, utvalgte forskere og ansatte i forskningsadministrasjonen.

49 I tillegg rapporterte to institusjoner om flere mislykkede påloggingsforsøk fra henholdsvis Russland og Kina. Nord universitet rapporterte om å ha mottatt varsel om at en «kjent trussel-aktør» hadde benyttet én av deres IP-adresser.

50 Med rekognosering menes at aktøren kartlegger institusjonene via internettet, trolig med tanke på å finne sårbarheter som kan utnyttes til å ta kontroll over lokale datamaskiner.

Hendelser og sårbarheter registrert hos Sikt

Cybersikkerhetssenteret for forskning og utdanning (eduCSC) hos Sikt fører statistikk over digitale sikkerhetshendelser i forskningsnettet og sårbarheter (tekniske sikkerhetshull) hos eduCSC sine kunder. Som tidligere år, har vi innhentet statistikk fra Sikt om slik aktivitet og sårbarheter.

For 2022 rapporterte eduCSC om 216 digitale sikkerhetshendelser og sårbarheter. Dette tallet gjaldt ikke bare hendelser og sårbarheter hos de 28 virksomhetene som HK-dir kartlegger hvert år, men omfatter alle eduCSC sine omkring 140 kunder.

Figur 3 viser utviklingen i antallet hendelser og sårbarheter registrert hos eduCSC (og Sikt sine kunder) fra 2018 til 2022.

Figuren viser at reduksjonen i antallet registrerte hendelser og sårbarheter har vært betydelig siden toppåret i 2018. I 2018 registrerte eduCSC 965 hendelser og sårbarheter. Tilsvarende tall for 2022 var altså 216.

Figuren viser også at nedgangen i hendelser og sårbarheter har vært særlig tydelig siden 2020. Nedgangen var klart størst fra 2021 til 2022.

Reduksjonen illustrert i figur 3, avspeiler seg bare til en viss grad i antall hendelser og brudd hos de 28 virksomhetene som HK-dir kartlegger årlig. Som allerede nevnt, er det kun i 2022 at vi har registrert en nedgang fra året før.

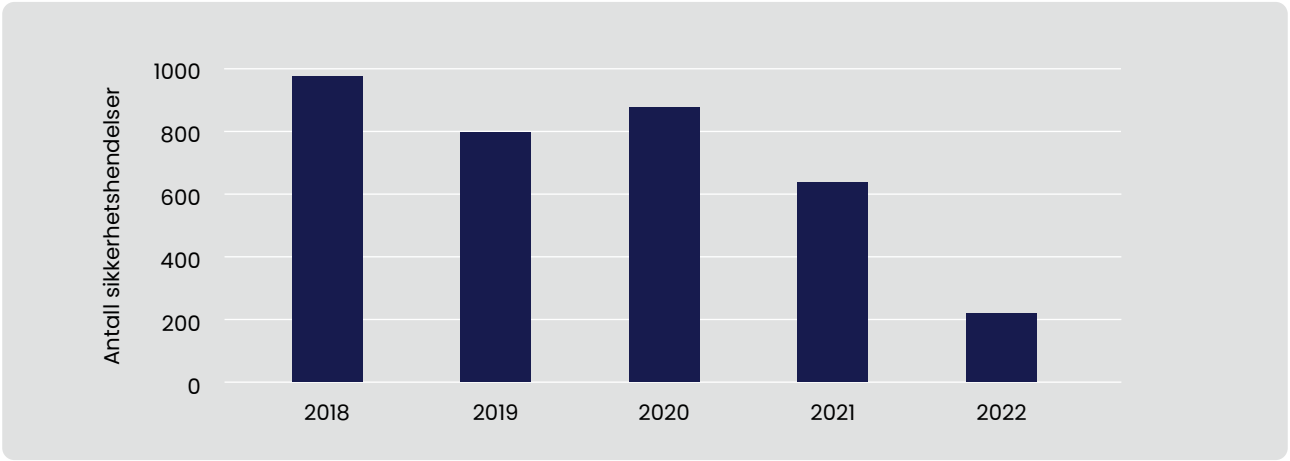
Endringer i statistikkgrunnlaget

Endringene i statistikken fra 2021 til 2022, ble i stor grad forklart med at NSM hadde sluttet å varsle eduCSC om tekniske sikkerhetshull (sårbarheter) i dataprogrammer. Slike varsler mottok eduCSC frem til 2022, og de ble dermed inkludert i eduCSC sin årsstatistikk til og med 2021.

I tillegg mente eduCSC at hendelser og sårbarheter oftere enn tidligere ble formidlet via sektorens varslingskanal – IRT-chat. Disse ble ikke registrert i statistikken for 2022.

Endringene i statistikkgrunnlaget kan likevel ikke forklare hele nedgangen fra 2021 til 2022. eduCSC fremhevet derfor at det hadde vært en reell reduksjon i antallet hendelser og sårbarheter i 2022.

Figur 3: Hendelser og sårbarheter registrert hos eduCSC, 2018-2022



Hovedtyper hendelser og sårbarheter
I 2022 utgjorde sårbare IT-systemer – datamaskiner som manglet nødvendige sikkerhetsoppdateringer – den klart største sakskategorien hos eduCSC: 48 prosent av alle registrerte saker. Forsøk på datainntrenging representerte åtte prosent av alle registrerte hendelser og sårbarheter. Dette var den nest største sakskategorien.

Andre viktige sakskategorier fra eduCSC sin årsstatistikk for 2022, inkluderte:

- Uønsket eksponering av datamaskiner: IT-tjenester som ikke burde vært eksponert mot internettet, men som likevel kunne nås via nettet.
- Infiserte systemer: IT-systemer (datamaskiner) som hadde fått installert ulike typer «ondsinnede dataprogrammer».
- Kompromitterte kontoer: trusselaktører som hadde fått tilgang til én eller flere kontoer med administrative rettigheter, vanligvis som følge av nettfiske.

Trusselen fra løsepengevirus ble også i år vurdert som høy av eduCSC.[51]

Personvern – brudd og hendelser i 2022

Universitetene og høgskolene ble bedt om å oppgi hvilke personvernsaker de hadde registrert i 2022. Dette inkluderer også saker hvor brudd på sikkerheten til personopplysninger ble vurdert å være meldepliktige til Datatilsynet.

I tillegg gjaldt det andre typer personvernsaker, det vil si saker som omhandlet andre forhold enn brudd på personopplysningssikkerheten. Eksempler på slike saker er manglende vurdering av behandlingsgrunnlag eller avvik fra interne rutiner for lagring av personopplysninger.

Antall personvernsaker
18 av de 21 universitetene og høgskolene opplyste om at de hadde registrert saker som gjaldt uønskede personvernhendelser i 2022. Tre institusjoner opplyste om at de ikke hadde registrert slike saker.

Til sammen rapporterte universitetene og høgskolene om ca. 300 personvernsaker. Dette er en nedgang på omkring 22 prosent sammenliknet med 2021 (da ble det rapportert om ca. 380 personvernsaker). Antallet er likevel høyere enn i 2019 og 2020.

Typer personvernsaker
Den klart største kategorien rapporterte personvernsaker gjaldt mangler eller feil ved registrering av forsknings- eller studentprosjekter i Sikt sitt meldingsarkiv. Dette var også den største sakskategorien i 2021.

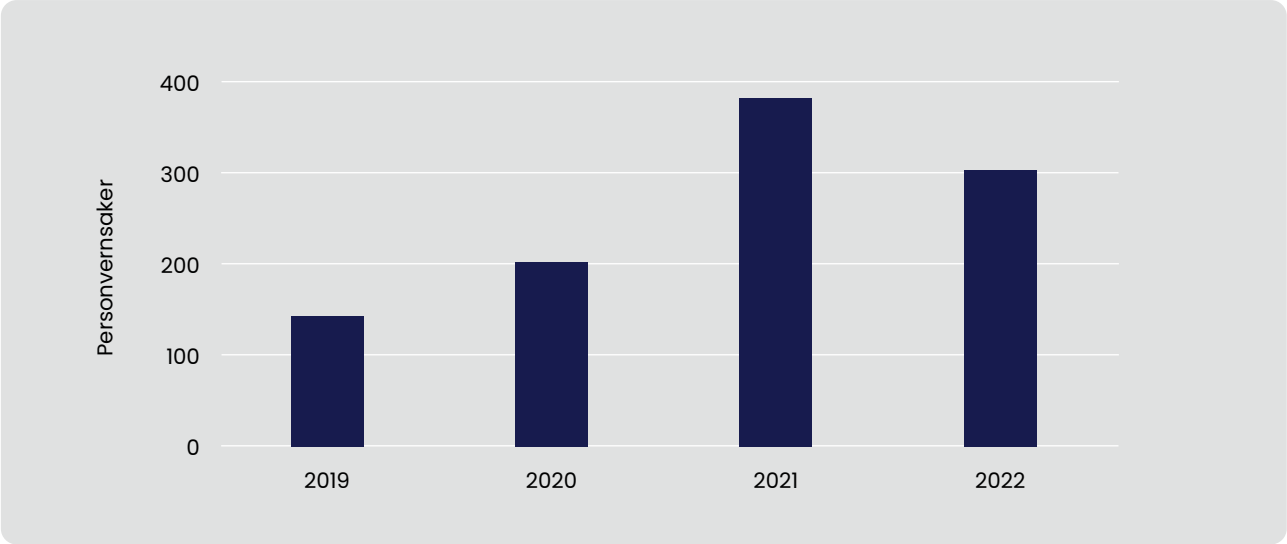
Om datagrunnlaget

Én institusjon rapporterte om 110 personvernsaker i 2022. Disse sakene ble imidlertid registrert over en 18-måneders periode. De inkluderer derfor også saker fra 2021.

Det betyr at nedgangen i det totale antallet rapporterte saker er noe større enn hva tallene ovenfor – og i figuren nedenfor – indikerer.

51 Her viste eduCSC blant annet vist til et tysk universitet som hadde blitt rammet av et løsepengevirusangrep. Se https://thecyberexpress.com/vice-society-claims-haw-hamburg-data-breach/. Sist besøkt 18.05.2023.

Figur 4: Antall rapporterte personvernhendelser, 2019-2022



Som tidligere år, handlet dette om to typer mangler. For det første at påbegynte registreringer av prosjekter i meldingsarkivet ikke var sluttført. For det andre at Sikt manglet bekreftelse på at personopplysninger ble slettet eller anonymisert ved prosjektslutt (sluttmelding).

I 2022 utgjorde slike mangler drøyt 74 prosent av det totale antallet personvernsaker. Tilsvarende tall for 2021 var 64 prosent.

De resterende personvernsakene (knapt 26 prosent) omhandlet forskjellige andre forhold knyttet til feil behandling av personopplysninger og brudd på interne rutiner (avvik). Vanlige feil og avvik inkluderte manglende oppdatering av behandlingsprotokollen ved innføring av nye applikasjoner eller IT-tjenester, behandlinger av personopplysninger uten lovlig grunnlag og manglende gjennomføring av konsekvensvurderinger (DPIA) før behandlinger av personopplysninger tok til.

Hos flertallet av institusjonene ble det i tillegg rapportert om ulike brudd på personopplysningssikkerheten og avvik fra egne rutiner for sikker behandling av personopplysninger. Eksempler på dette er feilsending av epost og lagring av personopplysninger på usikre/uegnede lagringsområder.

Andre avvik – de registrertes rettigheter

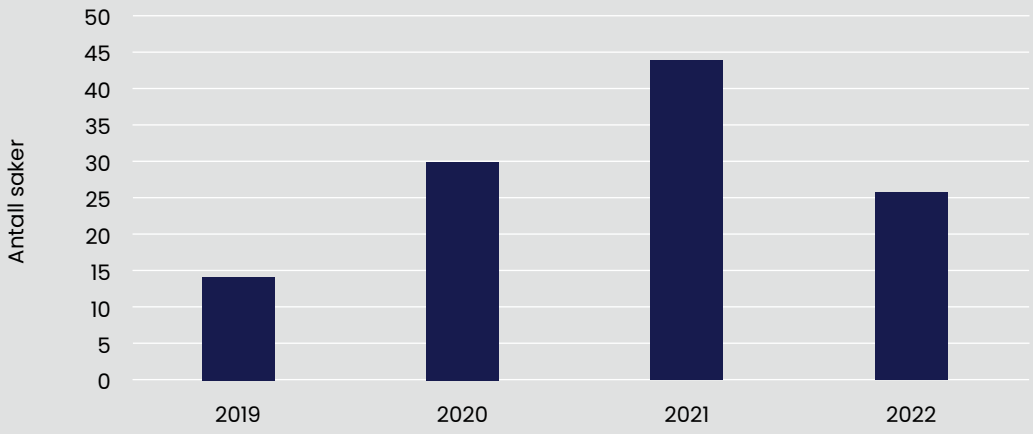
De registrerte – enkeltpersoner som opplysninger om personlige forhold omhandler (studenter, ansatte, forskningsdeltakere, osv.) – har visse personvernrettigheter, for eksempel retten til informasjon, innsyn, retting og sletting.[52] Universitetene og høgskolene er pålagt å utarbeide rutiner som ivaretar de registrertes rettigheter.

Ved tidligere kartlegginger har mange institusjoner rapportert om mangelfulle rettighetsrutiner. I 2022 oppga imidlertid 16 institusjoner at disse avvikene var lukket, det vil si at fullstendige rettighetsrutiner var utarbeidet. I 2021 rapporterte 12 institusjoner om det samme.

De fem siste institusjonene opplyste om enkelte avvik, men mente likevel at det var etablert rutiner for «de viktigste» rettighetene.

52 Se Datatilsynets oversikt over de registrertes rettigheter: https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/. Sist besøkt 14.03.2023.

Figur 5: Saker meldt til Datatilsynet, 2019-2022



Saker meldt til Datatilsynet

Brudd på personopplysningssikkerheten som innebærer risiko for krenkelser av personvernet, skal meldes til Datatilsynet.[53]

Som ved tidligere års kartlegginger rapporterte universitetene og høgskolene om hvor mange og hvilke typer saker de hadde meldt.

Figur 5 viser utviklingen i antallet meldinger fra 2019 til 2022.

Vi ser at antallet brudd på personopplysningssikkerheten som universitetene og høgskolene meldte til Datatilsynet økte i perioden 2019-2021. I 2022 hadde denne trenden snudd – antallet meldte brudd var redusert med over 40 prosent sammenliknet med året før (26 meldte brudd i 2021 mot 44 i 2021).

Åtte universiteter og høgskoler oppga at de hadde meldt brudd til Datatilsynet i 2022. Dette er det samme antallet som i 2021. Nedgangen skyldes derfor at de institusjonene som meldte om brudd i 2022 hadde færre brudd å melde om enn de som meldte i 2021.

De øvrige 13 institusjonene hadde ikke registrert saker som de mente var meldepliktige.

Meldingsinnhold og alvorlighetsgrad

23 av de 26 meldingene til Datatilsynet omhandlet brudd på konfidensialiteten til personopplysninger (opplysninger tilgjengelige for uvedkommende). Også i 2020 og 2021 gjaldt den typiske meldingen brudd på konfidensialiteten.

De vanligste årsakene til konfidensialitetsbrudd var feilsending av epost, feil publisering av personopplysninger og lagring av slike opplysninger på lagringsområder som var tilgjengelige for uvedkommende (egne ansatte eller studenter).

53 Der hvor det er snakk om høy risiko for krenkelser av personvernet, skal sakene også meldes til berørte personer («de registrerte»). Jf. EUs personvernforordning (GDPR) artikkel 33 og 34.

Det ble ikke opplyst om meldepliktige saker som gjaldt alvorlige brudd på personopplysningssikkerheten, for eksempel brudd som berørte et stort antall registrerte eller store mengder personopplysninger. Det ble heller ikke rapportert om at sensitive (særlige kategorier) personopplysninger hadde blitt tilgjengeliggjort for uvedkommende.

Det ble i tillegg meldt om enkelte saker som gjaldt andre forhold enn brudd på personopplysningssikkerheten, men som enkelte institusjoner likevel valgte å varsle Datatilsynet om. Det dreide seg blant annet om behandlinger av personopplysninger uten gyldig behandlingsgrunnlag.

Oppsummering og anbefalinger

EOS-tjenestene fremhever i sine årlige vurderinger at trusselbildet er mer utfordrende enn tidligere. Invasjonen av Ukraina har ført til et større etterretningsbehov for Russland, og etterretningstrusselen fra Kina vurderes å være på samme nivå som tidligere. Det advares også i årets trusselvurderinger om at norske forskningsmiljøer innen en rekke fagområder kan være aktuelle mål for cyberoperasjoner.

I årets kartlegging er antall rapporterte informasjonssikkerhetsbrudd og hendelser hos universitetene og høgskolene redusert med omkring 30 prosent sammenliknet med 2021. Den største nedgangen ble registrert hos enkelte av de største institusjonene.

Det ble ikke meldt om at hendelser og brudd hadde medført alvorlige skadevirkninger. Samtidig ble det opplyst om langt færre hendelser hvor det var mistanke om – eller det hadde blitt bekreftet – at statlige hackergrupper sto bak. Kartleggingen viser derfor et noe annet resultat enn det EOS-tjenestene advarer mot. Utviklingen er imidlertid i tråd med det som observeres hos Sikt (eduCSC) og i enkelte andre sektorer.[54]

Nettkriminalitet utgjorde fortsatt den klart største kategorien hendelser og brudd. Deretter fulgte utilsiktede menneskelige og tekniske feil eller uhell.

Vi ser også en reduksjon på ca. 22 prosent når det gjelder hendelser og avvik innen personvernområdet. Antallet meldinger til Datatilsynet om brudd på personopplysningssikkerheten ble redusert med ca. 40 prosent. Det ble opplyst om at disse sakene ikke innebar annet enn mindre krenkelser av personvernet.

På bakgrunn av disse funnene, anbefaler vi at sektoren fortsatt styrker sin tekniske og organisatoriske kapasitet til raskt å oppdage uønskede hendelser og begrense skadevirkningene av dem. Det vil bidra til ytterligere å redusere hendelsesomfanget og minimere eventuelle skadevirkninger.

Det innebærer at informasjons- og opplæringstilbudet til institusjonenes hendelseshåndteringsteam (IRT) styrkes. I tillegg anbefaler vi at følgende tiltak vurderes:

- videreutvikling av sektordekkende analyse- og responskapasitet,
- gjennomføring av sårbarhets- og inntrengingstesting,
- veiledning om håndtering av IKT-hendelser,
- kurs for operativt sikkerhetspersonell,
- bistand til beredskaps- og kontinuitetsarbeidet.

54 Se for eksempel «Mørketallundersøkelsen 2022», side 16. https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig. Sist besøkt 18.05.2023.

Kapittel 3

Universiteter og høgskoler – sårbarheter, forbedringer og status

Kapittel 3

Universiteter og høgskoler – sårbarheter, forbedringer og status

Innledning

For å forebygge, oppdage og håndtere hendelser og brudd drøftet i kapittel 2, er det avgjørende at universitetene og høgskolene kjenner egne sårbarheter og iverksetter tiltak for å utbedre dem. Dette oppnås ved at sektoren jobber systematisk med etterlevelse av Kunnskapsdepartementets policy for informasjons-sikkerhet og personvern.

I dette kapitlet drøftes tre hovedspørsmål:

1. Hvilke sårbarheter mente universitetene og høg-skolene at de har behov for å utbedre?

2. Hvilke tiltak hadde universitetene og høgskolene iverksatt i 2022 for å utbedre sårbarheter og å forebygge, oppdage og håndtere trusler mot informasjonssikkerheten og personvernet?

3. Hvor langt hadde universitetene og høgskolene kommet i etterlevelsen av departementets policy for informasjonssikkerhet og personvern?

Hovedtyper sårbarheter – definisjoner

Kompetanse: manglende kunnskap om eller erfaring med hvordan viktige informasjonssikkerhets- og personvernoppgaver kan utføres i praksis. Eksempler på slike oppgaver omfatter vurdering av behandlingsgrunnlag, gjennomføring av risikovurderinger, valg av hensiktsmessige sikringstiltak og evaluering av innholdet i databehandleravtaler.

Organisatoriske mangler: svakheter med måten arbeidet med informasjonssikkerhet og personvern er strukturert på, inkludert mangler ved eller fravær av rutiner og prosedyrer for sikker og lovlig håndtering av informasjonsverdier, spesielt personopplysninger.

Tekniske sårbarheter: ulike typer tekniske svakheter i IT-løsninger og digital infrastruktur. Eksempler på dette inkluderer sikkerhetshull i dataprogrammer, svakheter i måten datanettverket er oppbygd på og fravær av viktige tekniske sikringstiltak.

Kapasitet: personalressurser som helt eller delvis er øremerket for arbeidet med informasjonssikkerhet og personvern.

Bevissthet: forståelse for betydningen av informasjonssikkerhet og personvern, og kjennskap til vanlige trusler mot informasjonssikkerheten og personvernet, eventuelt også til interne rutiner og prosedyrer.

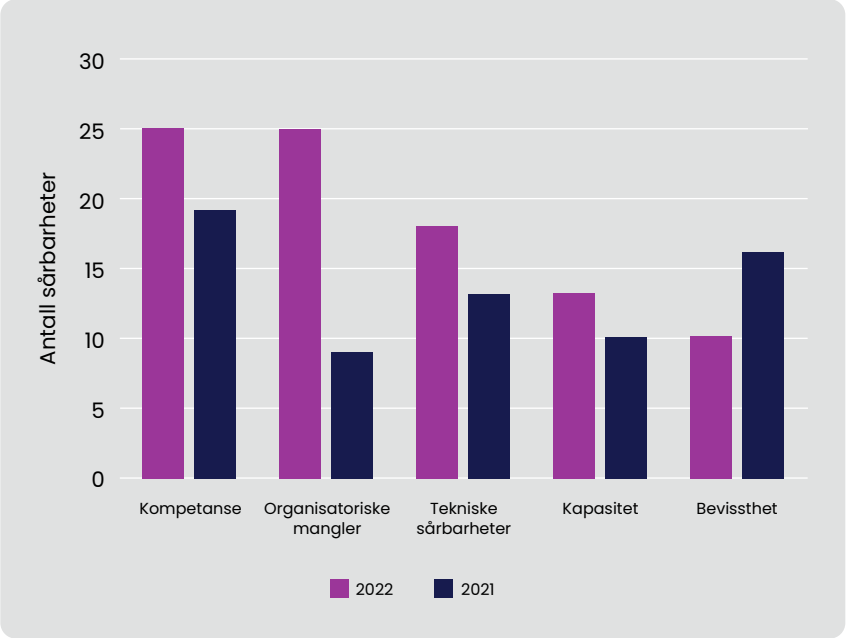
Rapporterte sårbarheter i 2022

Universitetene og høgskolene ble spurt om hvilke sårbarheter de hadde behov for å utbedre med tanke på å styrke informasjonssikkerheten og personvernet.

De 21 institusjonene oppga så mange sårbarheter som de selv mente det var grunnlag for. Antall og typer sårbarheter varierte derfor noe mellom institusjonene.

Figur 6 viser institusjonenes sårbarhetsprofil, det vil si de fem hovedtypene sårbarheter som de 21 universitetene og høgskolene rapporterte om. Sårbarhetsprofilen for 2022 sammenliknes med fjorårets profil.

Figur 6: Institusjonenes sårbarhetsprofil, 2022 og 2021



Sårbarhetsprofilen – endringer fra i fjor

I 2022 oppga de 21 institusjonene at den viktigste sårbarheten var manglende kompetanse om informasjonssikkerheten og personvernet blant ledere og medarbeidere. Førsteplassen var imidlertid delt med organisatoriske mangler. Deretter fulgte tekniske sårbarheter og manglende kapasitet.

Bevissthet om utfordringer knyttet til informasjonssikkerhet og personvern ble rangert som den minst viktige sårbarhetstypen.

Sårbarhetsprofilen for 2022 avviker noe fra fjorårets profil. Den største endringen er at organisatoriske mangler ble vurdert å være en viktigere utfordring i 2022 enn året før – fra å være minst viktig i 2021 til å være den viktigste i 2022.

I tillegg ser vi at i 2022 ble det rapportert om færre sårbarheter knyttet til bevissthetten blant ledere og medarbeidere om informasjonssikkerhet og personvern enn i 2021. Mens bevissthet var den nest viktigste sårbarheten i 2021, ble denne sårbarheten oppgitt å være minst viktig året etter.[55]

Om vi ser enda lengre tilbake i tid – til kartleggingene i 2019 og 2020 – avtegner det seg andre endringer. Én av de viktigste er at tekniske sårbarheter ble vurdert å være relativt lite viktig både i 2019 og 2020. I 2021 og 2022 hadde denne typen sårbarheter fått langt større oppmerksomhet hos de 21 universitetene og høgskolene.

55 «Risiko- og tilstandsvurdering 2021», side 31-33. https://hkdir.no/vaare-tenester/styring-av-informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning#content-section-6. Sist besøkt 18.03.2023.

Iverksatte tiltak i 2022

Sårbarhetene som universitetene og høgskolene rapporterte om indikerer hvor innsatsen for å styrke arbeidet med informasjonssikkerhet og personvern bør fokuseres. Vi spurte derfor institusjonene om hvilke tiltak de hadde iverksatt i 2022 for å utbedre sårbarheter og forbedre evnen til å forebygge, oppdage og håndtere brudd på informasjonssikkerheten og krenkelser av personvernet.

Nedenfor gis en oversikt over hvilke tiltak institusjonene opplyste om.

Vi ser også på sammenhengen mellom rapporterte sårbarheter og iverksatte tiltak: i hvilken grad ble det gjennomført tiltak som var egnet til å utbedre sårbarhetene?

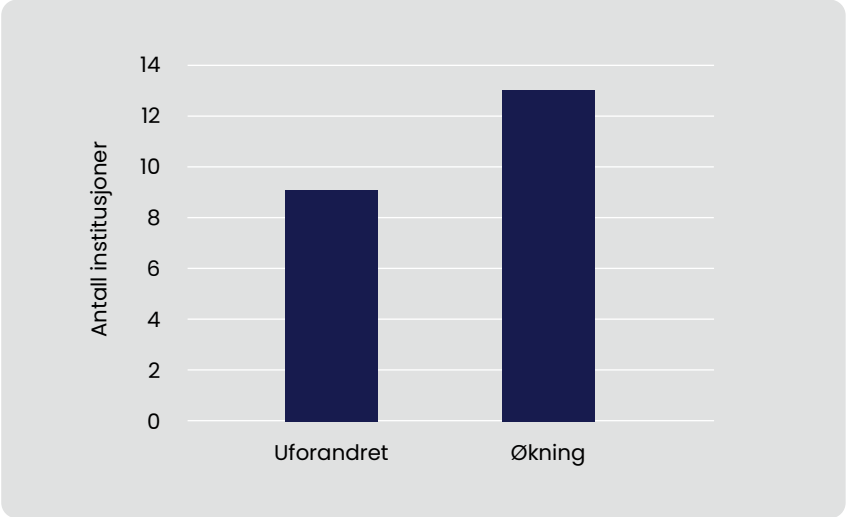
Kapasitetstiltak – årsverk
I 2022 oppga 18 av 21 institusjoner at kapasitet til å utføre informasjonssikkerhets- og personvernoppgaver var en viktig sårbarhet. Dette er en økning fra 10 institusjoner i 2021. Som ved tidligere kartlegginger, spurte vi derfor universitetene og høgskolene om hvor mange årsverk (anslagsvis) som helt eller delvis var øremerket for arbeidet med informasjonssikkerhet og personvern.

Figur 7 gir en oversikt hvor mange universiteter og høgskoler som opplyste om økning, stabilitet eller nedgang i årsverksinnsatsen sammenliknet med 2021.

Vi ser at 13 institusjoner opplyste om at de hadde økt antallet årsverk øremerket for arbeidet med informasjonssikkerhet og personvern fra 2021 til 2022.

Åtte institusjoner rapporterte om at årsverksinnsatsen ikke hadde endret seg.

Figur 7: Endringer i årsverksinnsatsen, 2021-2022



Ingen institusjoner oppga at ressursinnsatsen var redusert fra 2021 til 2022.

Samlet sett betyr dette at de 21 universitetene og høgskolene hadde økt årsverksinnsatsen med omkring 10 årsverk i 2022 (10,1). Dette er omtrent den samme veksten som i 2021 (11,1).

I perioden 2018-2022 har antallet årsverk som helt eller delvis er øremerket for arbeidet med informasjonssikkerhet og personvern økt fra omkring 69 i 2018 til ca. 111 i 2022.

Fordelingen av årsverkene
Årsverkstallene inkluderer institusjonenes personvernombud. I 2022 representerte personvernombudene omkring 12 årsverk. Det er det samme som i 2021.

De øvrige årsverkene fordeler seg på informasjonssikkerhetsansvarlig/-rådgiver (CISO) og institusjonenes IT-avdelinger, inkludert hendelseshåndteringsteam (IRT).

I tillegg ble det rapportert om øremerkede årsverk i HR- og økonomiavdelingene, avdelinger med ansvar for virksomhetsstyring og i studie- og forskningsadministrasjonen.

Hos enkelte institusjoner inkluderer det også sikkerhets- og beredskapsledere (CSO).

Årsverksoversikten inkluderte i liten grad arbeidet med informasjonssikkerhet og personvern blant vitenskapelig ansatte. Denne innsatsen omfatter blant annet søknader om godkjenning av eller meldinger om forskningsprosjekter, særlig til de regionale forskningsetiske komiteene og Sikt, og konsekvensvurderinger (DPIA) for visse typer forskningsprosjekter.

Det er grunn til å tro at årsverkstallene ville blitt noe høyere dersom innsatsen fra de vitenskapelige ansatte hadde blitt rapportert i større grad enn hva tilfellet virker å være.

Innleid kapasitet

Oversikten over årsverk inkluderer kun institusjonenes egne ansatte. Innleid kapasitet inngår ikke i oversikten. Oversikten gir derfor et noe ufullstendig bilde av institusjonenes ressursbruk innen informasjonssikkerhet og personvern i 2022.

Med innleid kapasitet menes at universitetene og høgskolene henter inn eksterne spesialister til oppgaver som institusjonene selv mangler kapasitet eller kompetanse til å utføre.

I 2022 rapporterte 10 institusjoner at de hadde kjøpt tjenester fra private aktører for å styrke arbeidet med informasjonssikkerhet og personvern. Dette handlet i hovedsak om bistand og rådgiving fra konsulentselskaper. På personvernområdet brukte enkelte institusjoner advokatfirmaer.

Institusjonene leide inn spesialistkapasitet for å løse en rekke oppgaver. Det gjaldt i særlig grad revisjoner av ledelsessystemet for informasjonssikkerhet eller internkontrollen for personvern (GDPR), etablering av beredskaps- og kontinuitetsplaner, gjennomføring av kriseøvelser og kartlegging av behandlinger av personopplysninger.

I kapittel 1 har vi i tillegg sett at Sikt sitt meldingsarkiv og tilhørende rådgivingstjeneste kan være viktige kapasitetsøkende ressurser for institusjonenes arbeid med personvern i forskning.[56] Institusjonene benytter også tjenester fra «Cybersikkerhetssenteret for forskning og utdanning» (eduCSC) hos Sikt, blant annet regelmessig testing av den tekniske sikkerheten i datamaskiner som er eksponert mot internettet.[57]

Sikkerhetsfunksjonalitet som kan kjøpes hos leverandører av viktige IT-tjenester bidrar også til å styrke institusjonenes kapasitet innen informasjonssikkerhet og personvern.

Hvor mye den innleide spesialistkapasiteten utgjorde i form av årsverk i 2022, har vi ikke informasjon om. Men det totale omfanget av denne kapasiteten er økende.

56 Norsk senter for informasjonssikring og Sikresiden er andre offentlige aktører som tilbyr vanlig brukte informasjonssikkerhets- og personverntjenester i UH-sektoren. Se https://norsis.no/ og https://www.sikresiden.no/. Sist besøkt 17.03.2023.

57 For oversikt over Sikt sine digitale sikkerhetstjenester, se https://sikt.no/tjenester/cybersikkerhetssenter-forskning-og-utdanning#abonnementer. Sist besøkt 19.03.2023.

Om tiltakene

Enkelte av tiltakene i figur 8 er konkrete informasjonssikkerhets- eller personverntiltak (slik som spesifisert i ISO/IEC 27001 vedlegg A eller i ISO/IEC 27002). Enkelte andre tiltak er systemtiltak. Dette er tiltak som har til hensikt å etablere eller videreutvikle et systematisk og helhetlig informasjonssikkerhets- eller personvernarbeid (ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR).

Det er også verdt å legge merke til at enkelte tiltak i figuren omfatter flere enkeltstående aktiviteter. Eksempelvis kan pedagogiske tiltak som «kurs for ansatte i GDPR» romme flere kurs- eller opplæringssamlinger. Vi regner imidlertid dette som kun ett tiltak.

Andre viktige tiltak i 2022

Vi spurte institusjonene om hva egne årsverk og den innleide kapasiteten hadde jobbet med i 2022: hvilke og hvor mange tiltak hadde universitetene og høgskolene iverksatt for å utbedre sårbarheter og styrke arbeidet med informasjonssikkerhet og personvern?

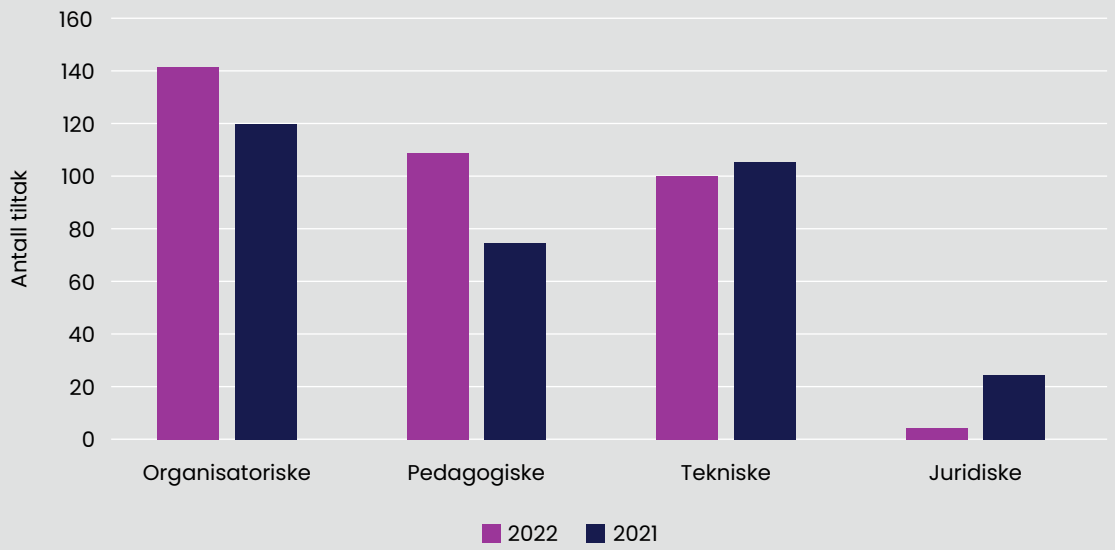
Figur 8 gir en oversikt over antall og hovedtyper rapporterte informasjonssikkerhets- og personverntiltak i 2021 og 2022. Tiltakene kategoriseres i fire hovedkategorier: organisatoriske, pedagogiske, tekniske og juridiske.

Figuren viser at universitetene og høgskolene totalt rapporterte om at 352 tiltak ble iverksatt i 2022. Dette er en liten økning sammenliknet med 2021. Da var det totale antallet rapporterte tiltak 322. Tiltaksaktiviteten har imidlertid økt vesentlig sammenliknet med hva den var i 2020 (220 rapporterte tiltak).

Tiltaksprofilen – hvordan tiltakene fordeler seg mellom de ulike kategoriene i figur 8 – var noe annerledes i 2022 enn i 2021. Organisatoriske tiltak var fortsatt den største tiltakskategorien både i 2021 og 2022. Men i 2022 hadde pedagogiske og tekniske tiltak byttet plass sammenliknet med 2021. Pedagogiske tiltak var nå den nest største tiltakskategorien og tekniske tiltak var den tredje største. I 2021 var det motsatt.

Antallet rapporterte juridiske tiltak ble redusert fra 2021 til 2022. Det kan delvis forklares med at institusjonene ikke lenger hadde det samme behovet for tiltak knyttet til Schrems II-dommen.

Figur 8: Informasjonssikkerhets- og personverntiltak, 2021-2022



Definisjoner

Organisatoriske tiltak: Utarbeidelse, innføring eller praktisering av ledelsessystemer for informasjonssikkerhet og internkontroll for personvern (GDPR). Eksempler på dette kan være fordeling av ansvar og oppgaver, revisjon av ledelsessystemet for informasjonssikkerhet, etablering av rutiner for ivaretakelse av de registrertes rettigheter, oppdatering av protokollen over behandlinger av personopplysninger eller utarbeidelse av kontinuitets- og beredskapsplaner.

Pedagogiske tiltak: Planlegging eller iverksetting av informasjons- eller opplæringsaktiviteter. Eksempler på dette kan være informasjon på hjemmesider, kurs i risikovurderinger, grunnleggende opplæring i GDPR, utarbeidelse av veiledere eller maler, deltakelse i sikkerhetsmåneden eller gjennomføring av øvelser på håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser.

Tekniske tiltak: Anskaffelse eller bruk av tekniske løsninger (maskin- eller programvare) som har til hensikt å styrke informasjonssikkerheten eller personvernet. Eksempler på dette er totrinnsinnlogging, segmentering av datanettverk, anskaffelse av brannmur, kryptering av elektronisk kommunikasjon, bruk av ny loggfunksjonalitet eller forbedret nettverksovervåkning.

Juridiske tiltak: Iverksetting av tiltak som følger av lov, forskrifter eller avtale og som har til hensikt å styrke kontrollen med informasjonssikkerheten og personvernet hos leverandører av IT-tjenester. Eksempler på dette kan være gjennomgang eller endring av vilkår i databehandleravtaler, eller avslutning av avtaler med databehandlere som ikke oppfyller lovpålagte krav til behandling av personopplysninger.

Oppfølging av anbefalinger
Økningen i og innretningen på tiltaksaktiviteten avspeiler seg i oppfølgingen av HK-dir sine anbefalinger til det enkelte universitet og høgskole. Anbefalingene ble formidlet i brev til institusjonene etter kartleggingen i fjor, og gjaldt hvilke tiltak som burde iverksettes i 2022 for å redusere sårbarheter og forbedre etterlevelsen av departementets policy for informasjonssikkerhet og personvern.

Av de totalt 76 hovedanbefalingene som HK-dir ga institusjonene, ble det rapportert om at 60 av dem enten var iverksatt eller var i ferd med å bli gjennomført. 14 anbefalinger hadde ikke blitt fulgt opp.

For de to siste hovedanbefalingene mangler vi empiri til å avgjøre om de hadde blitt iverksatt (helt eller delvis) eller ikke.[58]

Organisatoriske tiltak
Systemtiltak var også i 2022 de viktigste organisatoriske tiltakene som institusjonene rapporterte om. Dette er tiltak som har til hensikt å etablere eller forbedre systematikken og helheten i arbeidet med informasjonssikkerhet og personvern. Mange institusjoner rapporterte for eksempel om at de hadde videreutviklet ledelsessystemet for informasjonssikkerhet eller internkontrollen for personvern (GDPR), blant annet tydeliggjøring av rollene i sikkerhetsorganisasjonen og revisjoner av arbeidet med informasjonssikkerhet.

I 2022 oppga 18 institusjoner at de hadde opprettet informasjonssikkerhetsforum, faggrupper eller nettverk av personvernkontakter på enhetsnivå.[59] Det er det samme som i 2021. Formålene med slike forum, grupper eller nettverk er vanligvis sammensatt. Det kan blant annet dreie seg om erfaringsutveksling og kompetanseheving, planlegging og gjennomføring av større tiltak, og forankring av arbeidet med informasjonssikkerhet og personvern i alle deler av organisasjonen.

Universitetene og høgskolene rapporterte også om konkrete organisatoriske enkelttiltak. Som tidligere år, handlet dette i stor grad om rutiner for sikker behandling av personopplysninger, nye retningslinjer for klassifisering og lagring av informasjonsverdier, kartlegging av IT-systemer og programvare, ferdigstilling av behandlingsprotokoller og revidering av beredskapsplaner.

9 institusjoner opplyste om at de enten jobbet med retningslinjer for håndtering av informasjonsverdier undergitt eksportkontroll eller var i ferd med å kartlegge forekomsten av slike verdier.

Det ble også opplyst om tiltak for å styrke institusjonenes hendelseshåndteringsteam (IRT), for eksempel tydeliggjøring av mandat og utarbeidelse av nye rutiner for varsling av hendelser, brudd og avvik.

Pedagogiske tiltak
Heller ikke når det gjaldt pedagogiske tiltak hadde det skjedd vesentlige endringer i typer tiltak det ble rapportert om. Som ved tidligere kartlegginger, ble det derfor opplyst om to hovedtyper tiltak.

For det første, skreddersydd opplæring og kompetanseheving. Disse tiltakene var rettet mot medarbeidere med viktige roller i informasjonssikkerhets- eller personvernarbeidet.

For det andre, allmenn bevisstgjøring («folkeopplysning»). Dette var primært informasjon eller informasjonskampanjer rettet mot studenter eller ansatte som hadde til hensikt å opplyse om vanlige digitale trusler, for eksempel nettfiske eller svindelepost.[60] Men det kunne også handle om mer omfattende informasjon om GDPR og personvern, formidlet i møter med studenter og ansatte eller på virksomhetenes hjemmesider.

Et siste viktig pedagogisk tiltak var kriseøvelser – håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser. I 2022 rapporterte 20 universiteter og høgskoler om at de hadde gjennomført minst én kriseøvelse som omhandlet informasjonssikkerhet eller personvern.[61]

58 Det ble i tillegg gitt 139 anbefalinger om iverksetting av spesifikke enkelttiltak, for eksempel gjennomføre kriseøvelser, ferdigstille beredskaps- og kontinuitetsplaner eller oppdatere protokollen over behandlinger av personopplysninger. Av disse anbefalingene hadde 96 blitt fulgt opp (helt eller delvis). 27 anbefalinger hadde ikke blitt fulgt opp. For 16 anbefalinger mangler vi empiri til å avgjøre graden av oppfølging.

59 Forumene besto av medarbeidere med viktige roller i sikkerhetsorganiseringen (informasjonssikkerhetsleder, personvernombud, system-, tjeneste- eller prosesseiere).

60 Se https://norsis.no/nasjonal-sikkerhetsmaned/. Sist besøkt 19.03.2023.

61 Table-top (diskusjonsøvelser) var den vanligste øvelsesformen, men mange institusjoner oppga også at de hadde deltatt i sektorens IT-sikkerhetsøvelse (øvelse Morris i regi av Sikt).

Tekniske tiltak

Universitetene og høgskolene opplyste om at arbeidet med tekniske tiltak for å forebygge brudd på informasjonssikkerheten og krenkelser av personvernet hadde fortsatt i 2022. Viktige tiltak som ble nevnt var totrinnsinnlogging, styrking av interne sikkerhetsbarrierer i datanettverket, forbedret kontroll med tilgangen til og bruken av IT-systemer, og bedre sikring av reservekopier av data og programvare.

Det mest påfallende var likevel økningen i antallet tekniske tiltak som hadde til hensikt å oppdage og håndtere digitale sikkerhetshendelser. 18 av de 21 universitetene og høgskolene rapporterte om at de hadde iverksatt slike tiltak. Et av de viktigste gjaldt regelmessig sikkerhetstesting – sårbarhetsskann.[62] 12 institusjoner opplyste om at de jevnlig skannet eget datanettverk for å finne og utbedre sikkerhetshull i datamaskiner og programvare.

Dette var sikkerhetstester som kom i tillegg til Sikt sin obligatoriske testing (skanning) av de internetteksponerte delene av institusjonenes datanettverk. Enkelte institusjoner benyttet to-tre selvvalgte testverktøy (særlig OpenVAS[63] og Nessus[64]) som supplement til sårbarhetsskanningen fra Sikt.

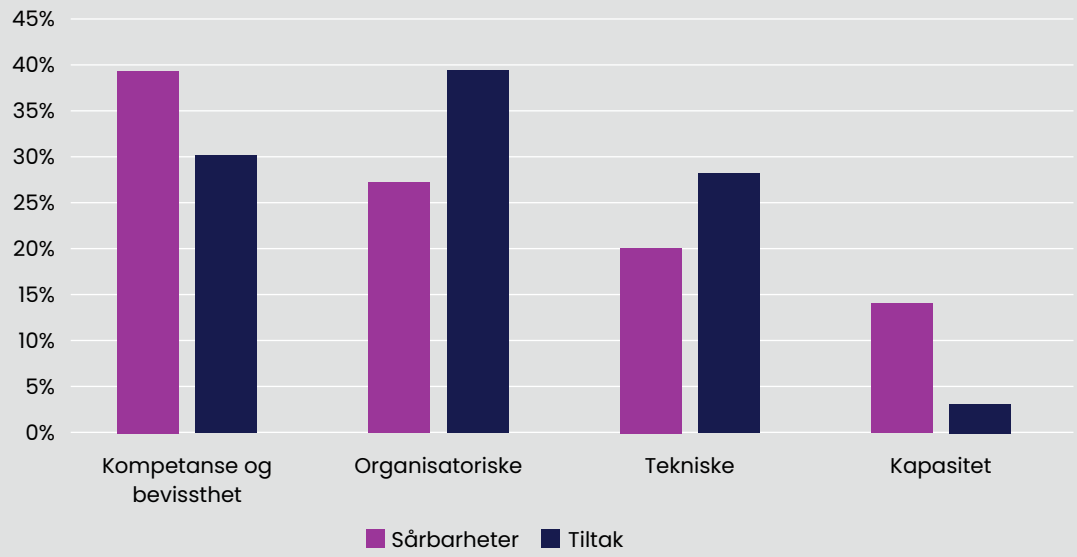
Det ble også rapportert om flere andre tekniske tiltak for å styrke evnen til å oppdage og håndtere digitale sikkerhetshendelser. Slike tiltak inkluderte bruk av ny sikkerhetsfunksjonalitet fra leverandører av skytjenester, innføring av nye brannmurløsninger, anskaffelse av programvare for analyse av datalogger, anvendelse av nye innbruddsensorer og videreutvikling av eksisterende digitale alarmsystemer.

62 Sårbarhetsskann gjennomføres for å avdekke og fikse sikkerhetshull i institusjonenes datanettverk.

63 Se https://www.openvas.org/. Sist besøkt 19.03.2023.

64 Se https://www.tenable.com/products/nessus. Sist besøkt 19.03.2023.

Figur 9: Samsvar mellom sårbarhetsprofil og tiltaksaktivitet, 2022



Samsvar mellom sårbarhetsprofil og tiltaksaktivitet?
I hvilken grad samsvarte tiltaksaktiviteten diskutert ovenfor med institusjonenes sårbarhetsprofil? Var det samsvar mellom det universitetene og høgskolene mente var de viktigste sårbarhetene og de tiltakene som ble iverksatt?

Figur 9 gir en oversikt over graden av samsvar mellom sårbarhetsprofilen og tiltaksaktivitet hos de 21 institusjonene i 2022.

I figuren har vi slått sammen sårbarhetskategoriene kompetanse og bevissthet. Dette fordi pedagogiske tiltak dekker begge. Det blir dermed enklere å vurdere hvorvidt det er samsvar mellom pedagogiske tiltak og de sårbarhetene som slike tiltak er ment å utbedre.

I figuren ser vi at det var et visst misforhold mellom sårbarhetsprofilen og tiltaksaktiviteten[65]. Det innebærer at fordelingen av tiltakene hos universitetene og høgskolene ikke fullt ut speiler de områdene (sårbarhetskategoriene) hvor institusjonene mente at de hadde størst behov for forbedringer.

Vi ser for eksempel at kompetanse og bevissthet ble vurdert å være de viktigste sårbarhetene i 2022. Det var likevel ikke her at tiltaksaktiviteten hadde vært størst – den hadde vært klart størst når det gjaldt organisatoriske tiltak.

Videre ser vi at selv om organisatoriske tiltak utgjorde den største tiltakskategorien, ble denne typen sårbarheter vurdert å være noe mindre viktig enn manglende kompetanse og bevissthet.

Samtidig ble det iverksatt flere tekniske tiltak enn hva institusjonenes sårbarhetsvurderinger strengt tatt skulle tilsi. Det motsatte er tilfelle for kapasitet. Her ble det rapportert om færre tiltak enn forventet sett i lys av betydningen som institusjonene mente at manglende personalressurser (årsverk) hadde for arbeidet med informasjonssikkerhet og personvern.

65 Figuren viser prosentandelen sårbarheter og tiltak som institusjonene rapporterte om innfor de ulike sårbarhets- og tiltakskategoriene. Ved å standardisere tallene på denne måten blir det enklere å vurdere om tiltaksaktiviteten samsvarer (eller ikke) med de sårbarhetene som det ble opplyst om. Kapasitet er her målt som økningen i antallet årsverk fra 2021 til 2022, hvor ett årsverk er regnet som ett tiltak.

Samlet vurdering og forbehold

Også etter fjorårets kartlegging så vi at det var et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak. Denne tendensen har fortsatt i 2022. Det indikerer at de tiltakene som institusjonene gjennomførte kunne vært enda mer treffsikre. Treffsikkerheten kan styrkes ved at tiltakene blir bedre tilpasset de sårbarhetene som universitetene og høgskolene mener påvirker deres arbeid med informasjonssikkerhet og personvern."

Det kan spesielt være behov for pedagogiske tiltak, det vil si tiltak som adresserer mangelen på kompetanse og bevissthet. Det samme synes å være tilfelle når det gjelder tiltak som imøtekommer behovet for «flere hender i arbeid» (kapasitet/årsverk).

Våre vurderinger av samsvaret mellom sårbarheter og tiltaksaktivitet har noen svakheter. Det skyldes at vi måler omfanget av tiltaksaktiviteten – antallet rapporterte tiltak innenfor hver tiltakskategori – og ikke kvaliteten eller effekten av dem. Det kan derfor tenkes at vurderingene ville sett litt annerledes ut dersom vi hadde hatt mer informasjon om kvaliteten og effekten av hvert enkelt av de 352 iverksatte tiltakene.

Forbedringer og status

Neste spørsmål er om tiltakene hadde påvirket etterlevelsen av kravene i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.[66] Hva var status for etterlevelse – i hvilken grad var etterlevelsen tilfredsstillende hos universitetene og høgskolene?

Før vi gjør opp status for 2022, vurderer vi i hvilken grad institusjonene hadde forbedret sin etterlevelse av departementets policy eller ikke. Deretter vurderer vi om eventuelle forbedringer hadde ført til tilfredsstillende etterlevelse eller om det var behov for ytterligere forbedringer.

Forbedret etterlevelse på enkeltområder

Figur 10 oppsummerer våre vurderinger av endringer i etterlevelsen av kravene i departementets policy fra 2021 til 2022. Vurderingene gjelder både informasjonssikkerhet og personvern.

Figuren viser hvor mange institusjoner som ikke hadde forbedret seg, forbedret seg i noen grad, eller klart forbedret seg.

Vår vurdering er at 16 av 21 universiteter og høgskoler hadde forbedret sin etterlevelse av departementets policy fra 2021 til 2022. Hos ni av de 16 institusjonene var forbedringene tydeligere enn hos de øvrige, mens syv av dem hadde forbedret seg i noen grad.

De fem siste institusjonene hadde verken forbedret eller svekket sin etterlevelse av kravene i policyen – de befant seg på omtrent samme nivå som i 2021. Ingen av institusjonene hadde svekket sin etterlevelse av policyen i løpet av fjoråret.

Vurdering av forbedring og status

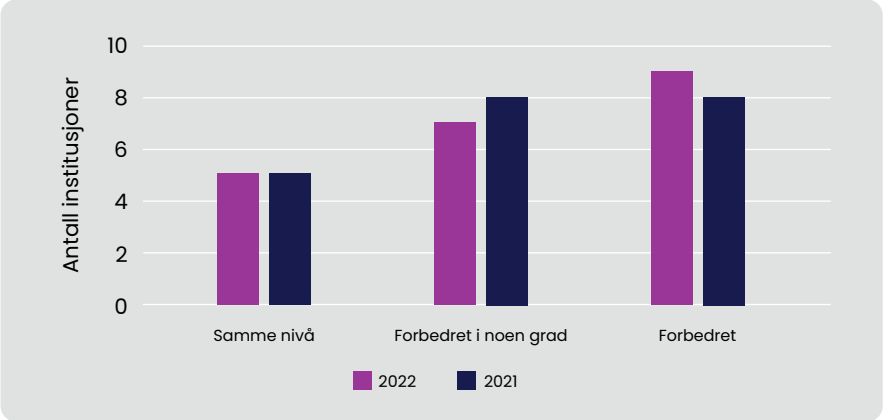
Vurderinger av forbedring og status når det gjelder etterlevelse av krav som departementets policy stiller til informasjonssikkerhet, er basert på følgende momenter: (i) tiltak for å forebygge, oppdage og håndtere trusler mot sikkerheten til informasjonsverdier, (ii) tiltak for å gjenopprette normal drift etter større sikkerhetsbrudd (beredskap/kontinuitet) og (iii) toppledelsen og styrets involvering i arbeidet med informasjonssikkerhet. Det legges i tillegg særlig vekt på hvor langt arbeidet med innføring av ledelsessystemer for informasjonssikkerhet var kommet.

Vurderinger av status og forbedring når det gjelder etterlevelse av krav som departementets policy stiller til personvern (GDPR), er basert på følgende momenter: (i) oversikt over behandlinger av personopplysninger (protokoller), (ii) rutiner for ivaretakelse av de registrertes rettigheter og (iii) tiltak for økt bevissthet og kompetanse om reglene i personopplysningsloven og personvernforordningen, og hvordan reglene kan etterleves. I tillegg legges det særlig vekt på hvor langt arbeidet med innføring av en internkontroll for GDPR var kommet (jf. artikkel 24 i personvernforordningen).[67]

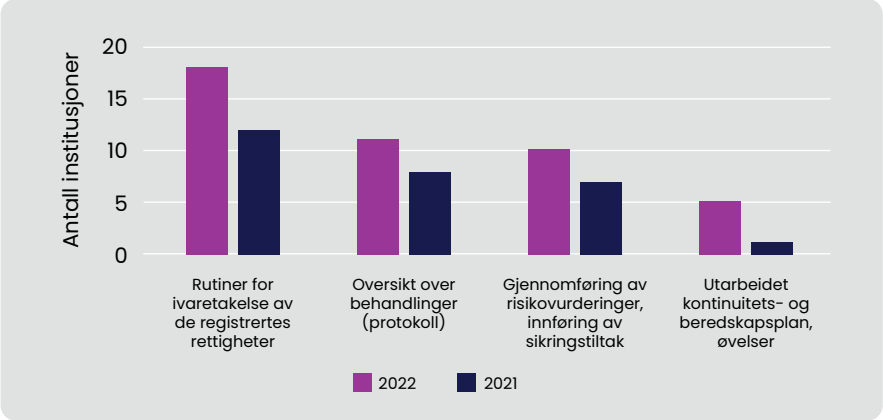
66 Se «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». https://www.hkdir.no/vaare-tenester/styring-av-informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning. Sist besøkt 13.03.2022.

67 Se også Datatilsynets veiledningssider om internkontroll. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/. Sist besøkt 13.03.2022.

Figur 10: Forbedringer i etterlevelse av policy, 2021-2022



Figur 11: De viktigste forbedringsområdene, 2021-2022



Forbedringstakten

Forbedringstakten var omtrent den samme i 2022 som året før. Forskjellen er at antallet institusjoner som tydelig hadde forbedret sin etterlevelse økte med én fra 2021 til 2022.

Figur 11 gir en mer detaljert oversikt over hvilke områder hvor forbedringene i etterlevelse hadde vært størst i 2021 og 2022.

Figuren viser at den største utviklingen har skjedd når det gjelder antallet institusjoner som har utarbeidet fullstendige rutiner for ivaretakelse av de registrertes personvernrettigheter. Dette antallet økte fra 12 institusjoner i 2021 til 18 i 2022.

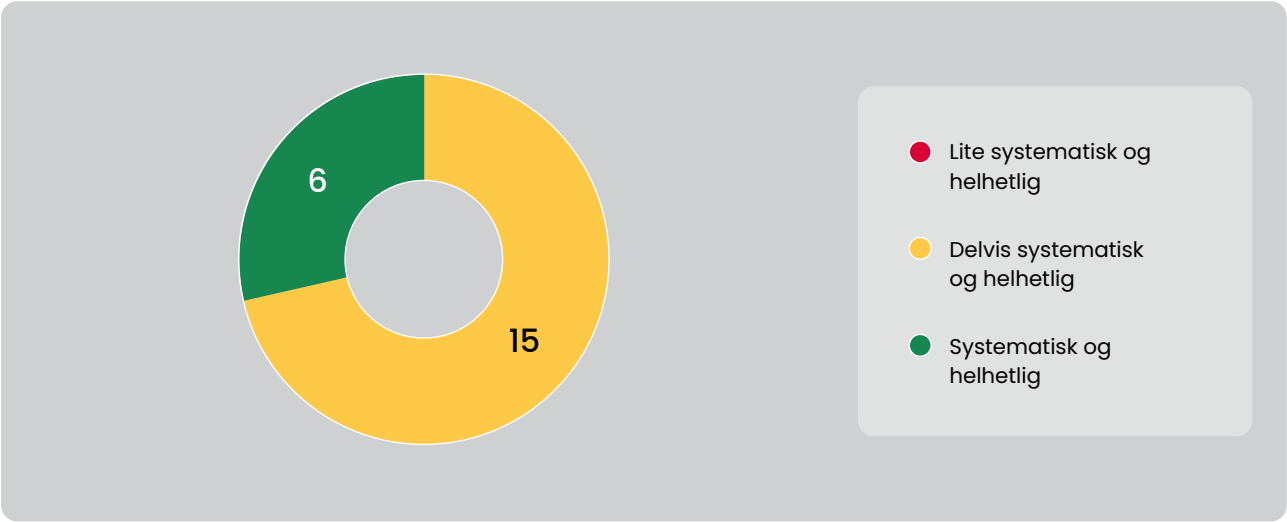
Videre viser figuren at antall institusjoner med tilfredsstillende oversikt over behandlinger av personopplysninger (protokoll), økte fra åtte i 2021 til 11 i 2022.

Tilsvarende økning ser vi med hensyn til kravene som gjelder risikostyring og innføring av sikringstiltak. Her økte antallet institusjoner som etterlevde disse kravene på tilfredsstillende måte fra sju i 2021 til 11 i 2022.

Også kravene til beredskaps- og kontinuitetsplaner på IT-området og kriseøvelser (håndtering av IT-sikkerhetshendelser), ble etterlevd i større grad i 2022 enn året før: fem institusjoner overholdt disse kravene i 2022 mot én i 2021.

For de andre kravene i policyen, for eksempel innføring og praktisering av ledelsessystemer for informasjonssikkerhet i alle deler av organisasjonen, var endringene mindre.

Figur 12: Etterlevelse av personvernkravene i policyen, 2022



Status – etterlevelse av kravene til personvern (GDPR)
Neste spørsmål er om forbedringene skissert ovenfor hadde ført til endringer i status for etterlevelsen av de særskilte personvernkravene i policyen. Dette gjelder primært punktene 6-10, men også 11-12 i policyen. Førte forbedringene til at flere universiteter og høgskoler enn tidligere etterlevde samtlige personvernkrav på en tilfredsstillende måte?

I figur 12 besvares dette spørsmålet.

Figuren viser at i 2022 hadde seks institusjoner etablert et systematisk og helhetlig arbeid som ivaretok personvernkravene i departementets policy på en tilfredsstillende måte. Disse institusjonene jobber langsiktig og planmessig med personvern, prinsippet om kontinuerlig forbedring er godt institusjonalisert, og arbeidet har tydelig støtte fra topplededelsen og styret.

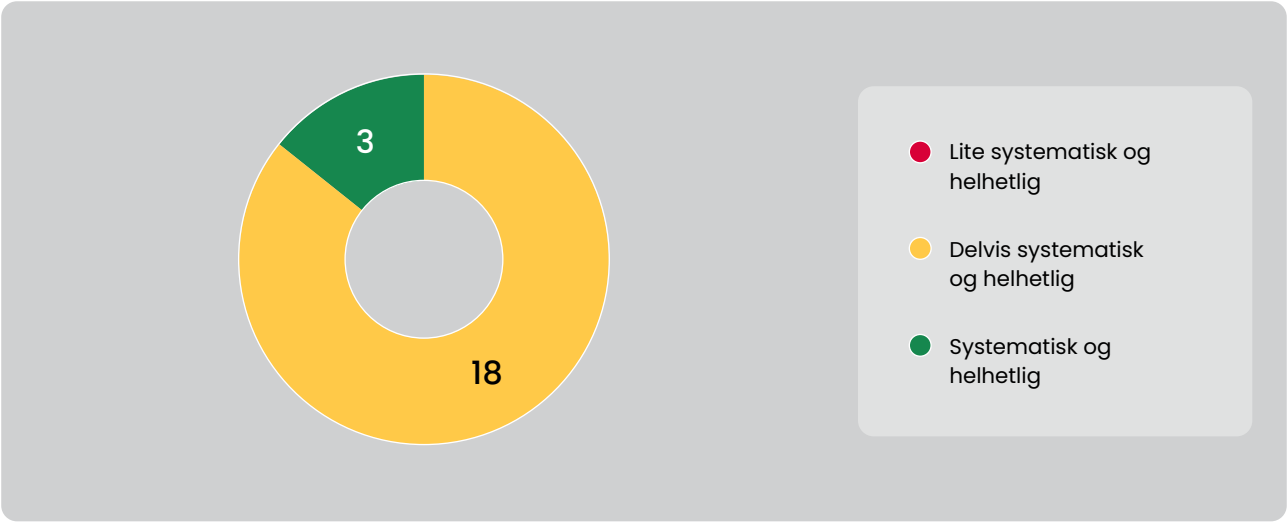
Antallet institusjoner som overholder personvernkravene i policyen var det samme i 2022 som i 2021. Forbedringene diskutert ovenfor medførte derfor ikke endringer i etterlevelsesstatus fra 2021 til 2022. Antallet institusjoner med et systematisk og helhetlig personvernarbeid har likevel doblet seg fra 2020 til 2022.

De resterende 15 institusjonene hadde kommet et stykke på vei med å tilfredsstille kravene i policyen: personvernarbeidet var delvis systematisk og helhetlig. Disse institusjonene rapporterte om enkelte avvik fra policyen som de hadde behov for å lukke. De viktigste policyavvikene gjaldt vanskeligheter med å bekjentgjøre og praktisere interne rutiner og retningslinjer for behandling av personopplysninger, spesielt på enhetsnivå. Disse avvikene skyldtes, ifølge institusjonene selv, hovedsakelig sårbarheter knyttet til kompetanse/bevissthet og organisatoriske mangler.

Flere av disse institusjonene hadde likevel forbedret arbeidet med personvern såpass mye i 2022 at de er klare «oppgraderingskandidater»: de befinner seg i «grenseområdet» mellom delvis tilfredsstillende og tilfredsstillende etterlevelse.

Ingen institusjoner ble vurdert til å jobbe lite systematisk og helhetlig – ad hoc og tilfeldig – med policyens personvernkrav. Heller ikke i 2021 fant vi institusjoner som i svært liten grad etterlevde kravene til personvern.

Figur 13: Etterlevelse av informasjonssikkerhetskravene i policyen, 2022



Status – etterlevelse av kravene til informasjonssikkerhet

I Figur 13 gis en oversikt over hvor mange institusjoner som etterlevde de særskilte kravene som policyen stiller til arbeidet med informasjons- og personopplysningssikkerhet. Dette gjelder primært punktene 1-5, men også 11-12 i policyen.

Figuren viser at i 2022 hadde tre institusjoner etablert et systematisk og helhetlig informasjonssikkerhetsarbeid som ivaretok de relevante kravene i policyen på en tilfredsstillende måte. Dette er det samme antallet som året før.

Dersom vi sammenlikner tallene i figur 13 med antallet institusjoner som etterlevde de særskilte personvernkravene, ser vi at tre færre institusjoner overholdt kravene til informasjonssikkerhet. Dette antyder at arbeidet med informasjonssikkerhet kan være noe mer krevende enn arbeidet med overholdelse av de særskilte personvernkravene.

De tre institusjonene som etterlevde kravene, hadde fortsatt enkelte mindre policyavvik. Vår vurdering er likevel at arbeidet omfattet alle deler av kjernevirksomheten, det er tydelig forankret hos toppledelsen og styret, og prinsippet om kontinuerlig forbedring er tilfredsstillende institusjonalisert.

De resterende 18 universitetene og høgskolene jobbet delvis systematisk og helhetlig med informasjonssikkerhet – det samme som i 2021. Det betyr at heller ikke når det gjaldt informasjonssikkerhet hadde forbedringene diskutert ovenfor vært store nok til at vi har kunnet oppgradere statusen til noen av disse institusjonene. Men også her er det flere institusjoner som er oppgraderingskandidater, det vil si at de befinner seg i «grenseområdet» mellom delvis tilfredsstillende og tilfredsstillende etterlevelse (se drøftelse nedenfor).

Det mest gjennomgående avviket hos disse 18 institusjonene var at ledelsessystemer for informasjonssikkerhet ikke var fullt innført og praktisert i alle deler av kjernevirksomheten. Spesielt avgjørende i denne forbindelse var behovet for å aktivere ledere og medarbeidere med sentrale roller i arbeidet med informasjonssikkerhet, for eksempel system- eller tjenesteeiere. Dette gjaldt i større grad på enhetsnivå enn i fellesadministrasjonen.

Ingen institusjoner ble vurdert til å jobbe lite systematisk og helhetlig – ad hoc og tilfeldig – med kravene til informasjonssikkerhet. Heller ikke i 2021 fant vi institusjoner som i svært liten grad etterlevde informasjonssikkerhetskravene.

Forventninger til 2023

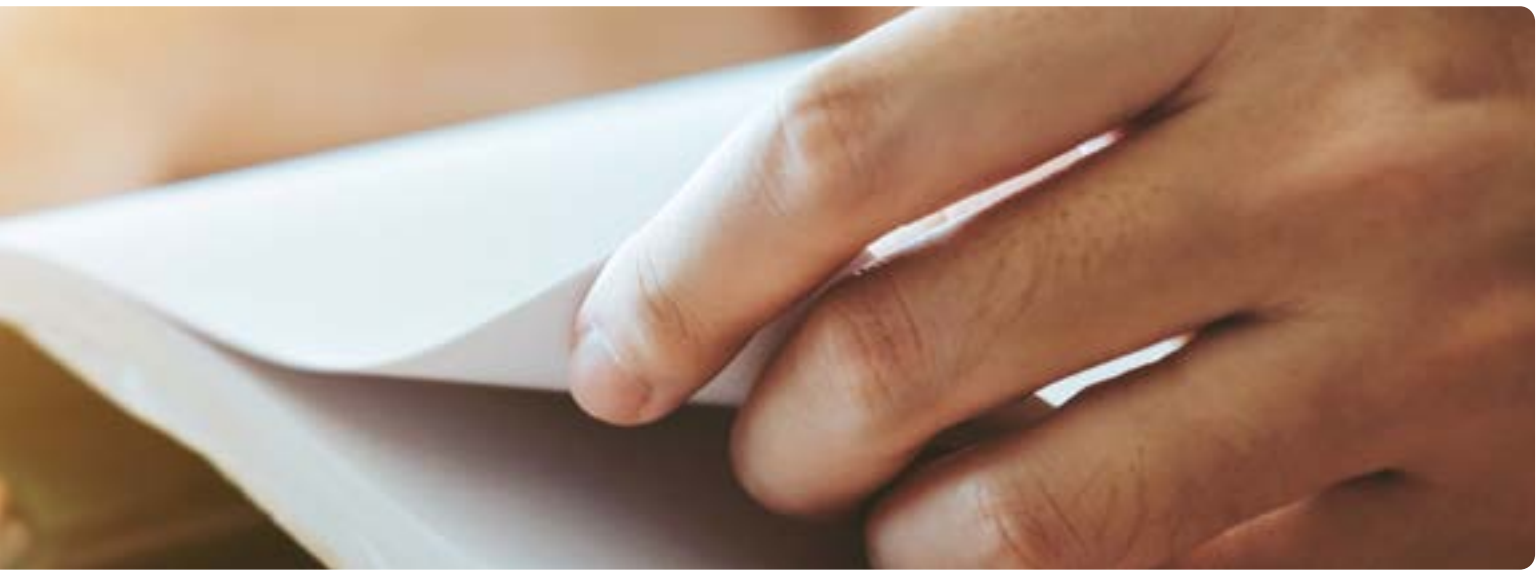
To institusjoner tilfredsstilte samtlige krav i departementets policy på tilfredsstillende vis. Det gjorde de også i 2021. Vi forventer at begge vil opprettholde og styrke sin policyetterlevelse i 2023.

Nedenfor vurderer vi sannsynligheten for at de øvrige institusjonene vil etterleve samtlige krav i policyen ved utgangen av 2023. Som i fjorårets risiko- og tilstandsvurdering, har vi delt de 19 universitetene og høgskolene inn i tre kategorier basert på hvor sannsynlig vi mener tilfredsstillende etterlevelse er.

Sannsynlighetskategoriene

- **Sannsynlig**: det er mer sannsynlig enn ikke at institusjonen vil kunne overholde kravene i policyen ved utgangen av 2023 (mer enn 50 prosent, men mindre enn 80 prosent sannsynlig).
- **Mulig**: det er mer usannsynlig enn sannsynlig at institusjonen vil kunne overholde kravene i policyen ved utgangen av 2023 (mer enn 30 prosent, men mindre enn 50 prosent sannsynlighet).
- **Lite sannsynlig**: det er liten grunn til å forvente at institusjonen vil kunne overholde kravene i policyen ved utgangen av 2023 (mindre enn 30 prosent sannsynlighet).

- **Etterlevelse sannsynlig**: Det er sannsynlig at seks institusjoner vil kunne etterleve samtlige krav i policyen ved utgangen av 2023. Forutsetningen for at institusjonene skal krysse grenselinjen, er at de har minst like stor fremgang i etterlevelsesarbeidet i inneværende år som de hadde i 2021 og 2022.
- **Etterlevelse mulig**: Det er mulig at seks andre institusjoner vil kunne etterleve samtlige krav i policyen ved utgangen av 2023. For disse institusjonene vil det kreve betydelig fremgang i etterlevelsesarbeidet. Vi regner det derfor som mindre sannsynlig at disse institusjonene vil etterleve policyen ved utgangen av 2023 enn hva tilfelle er for institusjonene i kategorien ovenfor.
- **Etterlevelse lite sannsynlig**: For de resterende sju institusjonene mener vi det er lite sannsynlig at de vil kunne etterleve samtlige krav i policyen ved utgangen av 2023. Vår vurdering er at disse institusjonene vil trenge noe lengre tid enn de øvrige på å oppnå tilfredsstillende etterlevelse.



Oppsummering og anbefalinger

I dette kapitlet har vi sett at universitetene og høgskolene oppga at de viktigste sårbarhetene i arbeidet med informasjonssikkerhet og personvern gjaldt kompetanse og organisatoriske mangler. Deretter fulgte tekniske sårbarheter, manglende kapasitet og bevissthet.

13 institusjoner hadde imidlertid styrket kapasiteten – årsverksinnsatsen – i 2022. Det samlede antall årsverk øremerket for arbeidet med informasjonssikkerhet og personvern økte fra i overkant av 100 i 2021 til ca. 111 i 2022.

I tillegg hadde universitetene og høgskolene gjennomført 352 andre typer informasjonssikkerhets- og personverntiltak. Her var organisatoriske tiltak den største tiltakskategorien. Deretter fulgte pedagogiske og tekniske tiltak. Det hadde blitt iverksatt klart færrest juridiske tiltak.

Også i 2022 var det et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak. Selv om kompetanse og bevissthet[68] ble vurdert å være de viktigste sårbarhetene i 2022, var tiltaksaktiviteten klart størst med hensyn til organisatoriske tiltak. Og mens organisatoriske tiltak utgjorde den største tiltakskategorien, ble denne sårbarheten vurdert å være noe mindre viktig enn kompetanse og bevissthet.

Dette indikerer at tiltakene som ble gjennomført i 2022 kunne vært enda mer treffsikre sett opp mot de rapporterte sårbarhetene. Styrket samsvar mellom rapporterte sårbarheter og iverksatte tiltak kan bidra til ytterligere å forbedre arbeidet med informasjonssikkerhet og personvern.

Universitetene og høgskolene hadde likevel styrket sin etterlevelse av kravene i departementets policy innenfor viktige enkeltområder. Det gjaldt spesielt rutiner for ivaretakelse av de registrertes rettigheter, oversikt over behandlinger av personopplysninger (protokoll), risikostyring av informasjonssikkerheten, beredskaps- og kontinuitetsplaner på IT-området og øvelser på håndtering av IT-sikkerhetshendelser. Disse forbedringene hadde imidlertid ikke ført til at flere institusjoner enn tidligere etterlevde samtlige 12 hovedkrav i policyen på en tilfredsstillende måte.

I 2023 mener vi det er sannsynlig at seks universiteter og høgskoler vil kunne etterleve kravene i policyen for informasjonssikkerhet og personvern. Det forutsetter at disse institusjonene fortsatt har god progresjon i arbeidet.

For de øvrige institusjonene er tilfredsstillende etterlevelse i løpet av 2023 mindre eller lite sannsynlig.

Med bakgrunn i drøftelsene i dette kapitlet, mener vi at sektortiltak som bidrar til å styrke kompetansen og bevissthetten om informasjonssikkerhet og personvern bør prioriteres. Slik vi ser det, er det innen disse områdene at sektortiltak trolig vil gjøre størst forskjell og bidra mest til å styrke arbeidet og forbedre policyetterlevelsen.

---

68 Som allerede nevnt, er kompetanse og bevissthet slått sammen for å sammenfalle med tiltakskategorien som avhjelper slike sårbarheter: pedagogiske tiltak.

Kapittel 4

Øvrige virksomheter – direktorater og selskaper

Kapittel 4

Øvrige virksomheter – direktorater og selskaper

Innledning

Sju øvrige virksomheter – direktorater og selskaper – er underlagt Kunnskapsdepartementet policy for informasjonssikkerhet og personvern. Det gjelder følgende virksomheter:

- Sikt – kunnskapssektorens tjenesteleverandør.
- Norges forskningsråd (NFR).
- Nasjonalt organ for kvalitet i utdanningen (NOKUT).
- Simula Research Laboratory.
- Norsk utenrikspolitisk institutt (NUPI).
- De nasjonale forskningsetiske komiteene (FEK).
- Universitetssenteret på Svalbard (UNIS).

Disse virksomhetene er såpass forskjellige fra de 21 universitetene og høgskolene, blant annet med hensyn til oppgaver, oppbygning og (til dels) størrelse, at de har litt andre utfordringer innen informasjonssikkerhet og personvern enn resten av sektoren. Vi har derfor valgt å behandle de sju siste virksomhetene i et eget kapittel.

I dette kapitlet følger først en oversikt over status for virksomhetenes arbeid med å identifisere de informasjonsverdier som omfattes av kravene i departementets policy for informasjonssikkerhet og personvern.

Så følger en oversikt over (i) brudd og hendelser på informasjonssikkerhets- og personvernområdet i 2022, (ii) sårbarheter i arbeidet med informasjonssikkerhet og personvern, og (iii) tiltak som ble iverksatt i 2022 for å utbedre sårbarhetene.

Til slutt gis en oversikt over status for etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

Spesielt om Sikt og HK-dir

Sikt ble opprettet 1. januar 2022, og det første kartleggingsmøtet med denne virksomheten ble avholdt i midten av februar i 2021. Etter som Sikt var nyopprettet på dette tidspunktet, var det ikke hensiktsmessig med en ordinær gjennomgang av deres arbeid med informasjonssikkerhet og personvern. Første ordinære kartlegging ble derfor gjennomført 9. februar i år.

Dette medfører at enkelte av funnene som diskuteres i dette kapitlet ikke direkte kan sammenliknes med tilsvarende funn i fjorårets rapport.

Direktoratet for høyere utdanning og kompetanse (HK-dir) omfattes av policyen for informasjonssikkerhet og personvern. Det er departementet som har ansvaret for styring av arbeidet med informasjonssikkerhet og personvern i HK-dir. HK-dir inngår derfor ikke i de årlige kartleggingene.

Oversikt over informasjonsverdier

De sju virksomhetene forvalter viktige informasjonsverdier på vegne av sektoren. Sikt driver for eksempel forskningsnettet i Norge og annen digital infrastruktur, blant annet tungregneanlegg.[69] Datterselskapet Sigma2 er en viktig aktør i denne forbindelse.

Enkelte av virksomhetene forvalter informasjonsverdier innenfor til dels sensitive kunnskapsområder. For Simula og NUPI dreier det seg blant annet om kryptologi, sikkerhets- og forsvarsstudier, og andre områder som er viktige for norsk utenriks- og sikkerhetspolitikk. UNIS gjennomfører forskning innenfor områder som biologi, geologi, geofysikk og arktisk teknologi.[70]

Størrelsen på virksomhetene gjør likevel at de forvalter færre informasjonsverdier – opplysninger, datamaskiner, programvare, osv. – enn universitetene og høgskolene. Samtidig er «verdilandskapet» mindre komplekst. Det innebærer for eksempel at omfanget av personopplysninger som behandles er begrenset sammenliknet med universitetene og høgskolene.

Årsrapportene til de sju virksomhetene for 2021 gir likevel indikasjoner på at avhengigheten av digital teknologi øker. Flere av virksomhetene uttrykker for eksempel at digitalisering er en viktig del av arbeidet med å utvikle og effektivisere arbeidsprosesser. Dette skjer blant annet ved anskaffelse av skylagringstjenester, modernisering av saksbehandlingssystemer, og bruk av roboter og kunstig intelligens.[71]

I årsrapportene fremheves også betydningen av digitalisering innen formidling og generelt informasjonsarbeid. Her handler det spesielt om nettbasert publisering, digitalisering av veiledningstilbud og annen utadrettet virksomhet.

Utviklingen som skisseres i virksomhetenes årsrapporter, indikerer at det blir stadig viktigere å ha god oversikt over datamaskiner, programvare og IT-tjenester – og hvilke opplysninger som behandles i IKT-løsningene – for å kunne ivareta informasjonssikkerheten og personvernet.

Behandlingsprotokoll

En dekkende og oppdatert behandlingsprotokoll gir en samlet oversikt over mange av de viktigste informasjonsverdiene som virksomhetene forvalter. I kapittel 1 så vi at personopplysningsloven og personvernforordningen (GDPR) krever at virksomhetene har en slik protokoll. Den skal blant annet gi en oversikt over hvilke typer personopplysninger som virksomheten behandler og hvem opplysningene gjelder.[72]

Figur 14 viser hvor mange av de sju virksomhetene som oppga at de enten har en fullstendig og oppdatert, delvis dekkende eller svært mangelfull behandlingsprotokoll.

Fire av de sju virksomhetene rapporterte om at behandlingsprotokollen var fullstendig og oppdatert. De tre siste oppga at protokollen ikke ga en fullgod oversikt over deres behandling av personopplysninger.

Ingen opplyste om at protokollen var svært mangelfull.

Dette er en klar forbedring sammenliknet med fjorårets kartlegging. Da mente to av de fem virksomhetene som ble kartlagt at de hadde en fullstendig og oppdatert protokoll. Tre virksomheter mente at protokollen var delvis dekkende. Hos den siste virksomheten vurderte vi statusen som svært mangelfull.

69 Se Sikt sin tjenesteoversikt. https://sikt.no/tjenesteoversikt. Sist besøkt 03.03.2023.

70 UNIS Strategy 2025. https://www.unis.no/wp-content/uploads/2019/04/UNIS_Strategy_2025_web.pdf. Sist besøkt 03.03.2023.

71 Se for eksempel NFR årsrapport 2021, side 12, https://www.forskningsradet.no/siteassets/publikasjoner/2022/forskningsradets-arsrapport-2021_2.pdf, eller NOKUT årsrapport 2021, side 16-17, https://www.nokut.no/siteassets/om-nokut/arsrapporter-og-tildelingsbrev/2021/nokut-arsrapport-for-2021.pdf. Sist besøkt 03.03.2023.

72 For nærmere informasjon om kravene til behandlingsprotokoll, se Datatilsynets veiledning på https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/. Sist besøkt 03.03.2023.

Andre informasjonsverdier
Samtlige virksomheter rapporterte om at de hadde kartlagt andre informasjonsverdier enn personopplysninger: datamaskiner, programvare og IT-tjenester. Hos enkelte av virksomhetene var kartlegginger delvis gjennomført ved hjelp av tekniske produkter som identifiserer hvilke datamaskiner som er tilkoblet datanettverket og programvaren som maskinene benytter.

På bakgrunn av kartleggingene var det utarbeidet system- eller tjenesteoversikter. Oversiktene inkluderte også bruk av skytjenester.

Fem av de sju virksomhetene mente at de hadde en relativt fullstendig og oppdatert oversikt over datamaskiner, programvare og IT-tjenester. Hos de to siste ble det enten oppgitt at de viktigste IT-tjenestene var kartlagt eller at det var behov for å detaljere den oversikten som var utarbeidet.

To virksomheter hadde gjennomført eller var i ferd med å gjennomføre kartlegging av informasjonsverdier som kunne være omfattet av sikkerhetsloven eller eksportkontrollreguleringer. Den ene virksomheten hadde konkludert med at de ikke forvalter verdier som er relevante i relasjon til sikkerhetsloven. Den andre hadde nedsatt en arbeidsgruppe som skulle kartlegge hvilke verdier som reguleres av eksportkontrollbegrensninger.

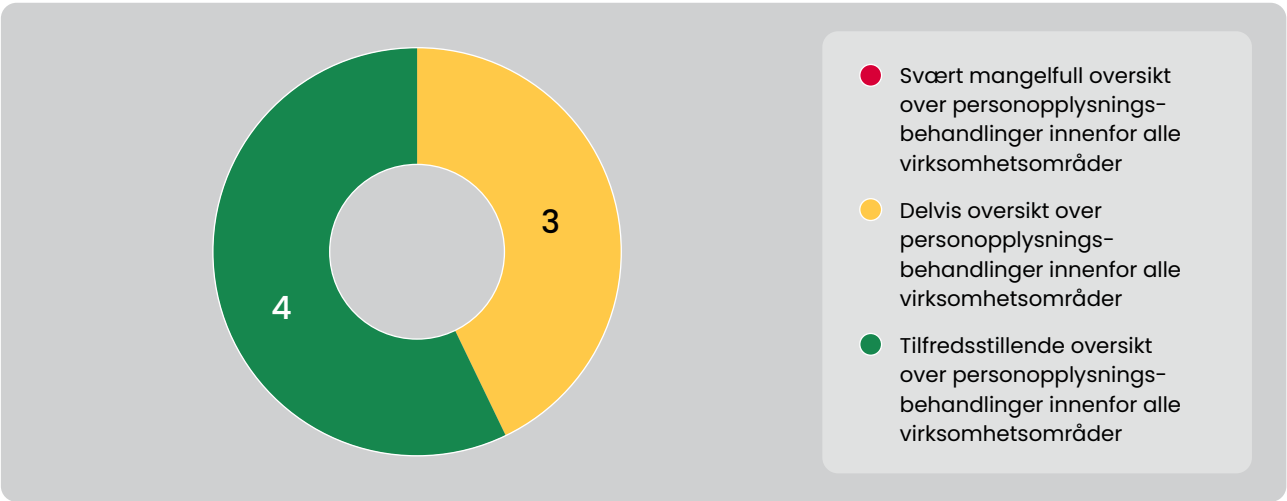
Ingen av de øvrige virksomhetene opplyste om at de hadde gjennomført eller planla å gjennomføre tilsvarende kartlegginger. Én av disse virksomhetene hadde jobbet med å øke bevisstheten om at de kan være mål for utenlandsk etterretningsvirksomhet (statlige hackergrupper).

Det ble likevel ikke oppgitt at det var gjennomført særskilte kartlegginger av «etterretningsrelevante» informasjonsverdier.

Oppsummert innebærer dette at de sju direktoratene og selskapene hadde bedre oversikt enn tidligere over hvilke opplysninger som skal beskyttes mot krenkelser av personvernet (personopplysninger). Tre virksomheter hadde behov for å forbedre sin behandlingsprotokoll. Disse virksomhetene jobber med å forbedre sine protokoller.

Virksomhetene har også styrket oversikten over andre typer informasjonsverdier, spesielt datamaskiner, programvare og IT-tjenester. Det samme gjaldt for informasjonsverdier undergitt sikkerhetsloven og eksportkontrollreguleringer.

Figur 14: Status for behandlingsprotokoll, 2022



Hendelser og avvik

Samlet ble det rapportert om 62 hendelser og brudd hos de sju virksomhetene. 51 av dem gjaldt uønskede informasjonssikkerhetshendelser, mens 11 gjaldt avvik fra interne rutiner for håndtering av personopplysninger.

To virksomheter hadde ikke registrert hendelser eller avvik i 2022.

62 registrerte hendelser og brudd er en økning sammenliknet med 2021. Da ble det rapportert om 23 hendelser og brudd. Økningen fra året før skyldes at fem virksomheter ble kartlagt med hensyn til hendelser og brudd i 2021 mot sju i 2022.

Dersom vi ser på de virksomhetene som ble kartlagt i perioden 2020-2022, opplyste disse virksomhetene om 10 hendelser og brudd i 2022 mot 23 i 2021 og 95 i 2020. Der vi har sammenliknbare tall, ser vi derfor en nedgang i det totale antallet hendelser og brudd over tid.

Hendelsesprofilen
De typene informasjonssikkerhetshendelser som ble registrert i denne delen av sektoren i 2022, gjaldt i all hovedsak de samme som det ble rapportert om i 2021: menneskelige eller tekniske feil og uhell. I tillegg ble det registrert enkelte forsøk på nettsvindel og datainntrenging (kompromittering av brukerkontoer).

Ingen av forsøkene hadde lyktes, blant annet på grunn av at det var innført totrinnsinnlogging.

Andre vanlige informasjonssikkerhetshendelser gjaldt ikke-planlagt nedetid på IT-tjenester (manglende tilgjengelighet) og tekniske sårbarheter (sikkerhetshull) i programvare. Det ble også rapportert om enkelte tilfeller med uønsket eksponering av personopplysninger og feil i styringen av tilganger til IT-løsninger.

Det ble heller ikke i 2022 registrert forsøk på datainntrenging hvor det var mistanke om involvering fra statlige eller statsstøttede hackergrupper (APT-grupper). Det samme gjaldt løsepengevirus, tjenestenektangrep og misbruk av lokale datamaskiner, for eksempel til utvinning av kryptovaluta.

Når det gjaldt avvik fra interne rutiner for behandling av personopplysninger, ble det opplyst om seks tilfeller hvor det manglet databehandleravtale med leverandører av IT-tjenester. Det ble også registrert enkelte tilfeller med manglende sletting av personopplysninger og feil registrering av slike opplysninger.

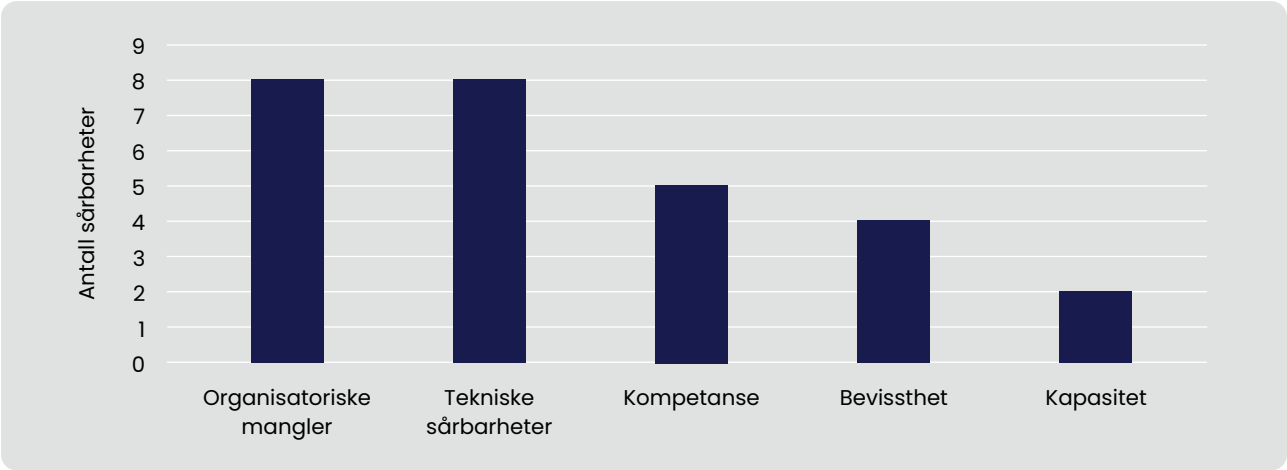
Skadevirkninger
Virksomhetene ble bedt om å vurdere hvilke skadevirkninger som hendelsene og avvikene hadde ført til. Ingen av virksomhetene mente at de hadde medført annet enn begrensede eller ingen skadevirkninger.

Manglende databehandleravtale med leverandører av IT-tjenester ble riktignok vurdert som avvik fra policy og regelverk som det var viktig å lukke. Det ble likevel oppgitt at disse avvikene ikke hadde ført til krenkelser av personvernet, for eksempel ved at personopplysninger ble misbrukt eller eksponert for uvedkommende.

Heller ikke hendelser som innebar brudd på konfidensialiteten til personopplysninger ble vurdert som alvorlige. Dette fordi det handlet om et fåtall alminnelige opplysninger som gjaldt et begrenset antall personer. Samtidig ble det raskt iverksatt tiltak for å rette feilene og hindre gjentakelse.

Ingen av bruddene på personopplysningssikkerheten ble vurdert å representere en så stor risiko for personvernet at de ble vurdert som meldepliktige til Datatilsynet.

Figur 15: Antall og typer sårbarheter, 2022



Sårbarheter

Som drøftet i kapittel 3, ligger sårbarheter vanligvis til grunn for brudd på informasjonssikkerheten, krenkelser av personvernet og avvik fra interne rutiner. Virksomhetene ble derfor spurt om hvilke sårbarheter de har behov for å utbedre for å styrke informasjonssikkerheten og personvernet.

Figur 15 gir en samlet oversikt over hovedkategorier av sårbarheter som virksomhetene rapporterte om.

Hver virksomhet oppga flere ulike typer sårbarheter. Stolpene i figuren viser hvor mange ganger de ulike sårbarhetskategoriene ble nevnt av de sju virksomhetene.

Figuren viser at organisatoriske mangler og tekniske sårbarheter ble vurdert som de viktigste sårbarhetene. Organisatoriske mangler dreide seg primært om uklare ansvars- og oppgavefordeling og manglende rutiner for sikker og lovlig behandling av personopplysninger.

Tekniske sårbarheter handlet i stor grad om sikkerhetshull i IT-løsninger, ustabile IT-tjenester og bruk av utdaterte dataprogrammer.

Når det gjaldt kompetansemangler, ble det vist til at ledere eller medarbeidere som var ment å spille sentrale roller i arbeidet med informasjonssikkerhet og personvern, spesielt system- eller tjenesteeiere, ikke hadde tilstrekkelig praktisk kunnskap eller erfaringer til å løse sine pålagte oppgaver på en hensiktsmessig måte.

Bevissthet, det vil si kjennskap til og oppmerksomhet om informasjonssikkerhets- og personvernutfordringer ble vurdert som noe mindre viktig enn de øvrige sårbarhetene. Det samme gjaldt kapasitetsutfordringer (årsverksinnsats).

Sårbarhetsprofilen i figuren avviker noe fra tilsvarende profil fra fjorårets kartlegging. De viktigste forskjellene er at organisatoriske mangler oppgis å være en viktigere sårbarhet i 2022 enn året før, og at det ble rapportert om kapasitetsmangler. Kapasitetsmangler ble ikke nevnt i 2021.

Kapasitetstiltak

I hvilken grad hadde de sju virksomhetene adressert kapasitetsutfordringene og styrket årsverksinnsatsen i 2022?

To virksomheter oppga at de hadde styrket årsverksinnsatsen noe sammenliknet med 2021. Hos fire virksomheter ble det ikke opplyst om endringer i årsverksinnsatsen.

Den siste virksomheten rapporterte om at årsverksinnsatsen ble redusert i 2022. Årsaken til reduksjonen ble oppgitt å være at det var mindre behov for ressurser til innføring av ledelsessystemet for informasjonssikkerhet og internkontrollen for personvern (GDPR) enn tidligere.

Samlet innebærer dette at det totale antallet årsverk i denne delen av UH-sektoren ikke hadde endret seg nevneverdig fra 2021 til 2022.

Andre viktige tiltak i 2022

Vi spurte de sju forvaltningsorganene og selskapene om hvor mange og hvilke andre tiltak de hadde iverksatt i 2022 for å utbedre sårbarheter og styrke arbeidet med informasjonssikkerhet og personvern.

Figur 16 gir en oversikt over antall og hovedtyper tiltak som virksomhetene opplyste om. Som for universitetene og høgskolene, deles tiltakene inn i fire kategorier: tekniske, organisatoriske, pedagogiske og juridiske.

Hva som inngår i de ulike tiltakskategoriene, er definert i kapittel 3.

Figuren viser at direktoratene og selskapene totalt rapporterte om 94 iverksatte tiltak. Dette er en økning sammenliknet med 2021. Da ble det rapporterte om 58 tiltak.

Under kartleggingen i fjor var det fem virksomheter som rapporterte om tiltak mot sju i år. Økningen i tiltaksaktiviteten kan derfor i noen grad skyldes at flere virksomheter rapporterte om dette i 2022. Forskjellen er likevel såpass stor at det likevel har vært en reell økning i 2022 sammenliknet med tidligere år.

Virksomhetene rapporterte om flest organisatoriske tiltak (37), mens pedagogiske tiltak var den nest største tiltakskategorien (27). Deretter fulgte tekniske tiltak (24). Den klart minste kategorien var juridiske tiltak (6).

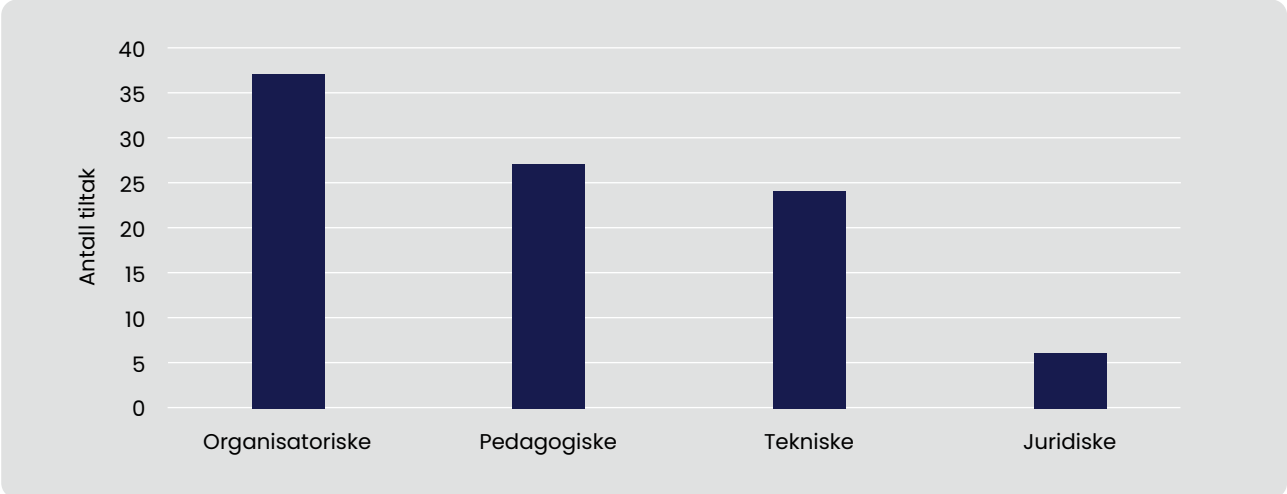
Dette er omtrent den samme fordelingen som i 2021. Den viktigste forskjellen er at i 2021 var tekniske tiltak den nest største tiltakskategorien, mens pedagogiske tiltak inntok tredjeplassen.

Vi ser også at det ikke er store variasjoner mellom de tre største tiltakskategoriene. Tiltaksaktiviteten fordeler seg derfor relativt jevnt mellom organisatoriske, tekniske og pedagogiske tiltak.

Tiltaksprofilen

Fire virksomheter hadde hovedsakelig iverksatt organisatoriske og pedagogiske tiltak. Pedagogiske tiltak handlet for eksempel om e-læringskurs, opplæring i informasjonssikkerhet og personvern og øvelser i håndtering av alvorlige sikkerhetsbrudd. Typiske organisatoriske tiltak gjaldt oppdatering av behandlingsprotokollen, forbedring av kontinuitetsplaner og utarbeidelse av rutiner for behandling

Figur 16: Antall og typer informasjonssikkerhets- og personverntiltak, 2022



(for eksempel sletting) av person-opplysninger.

Tre virksomheter hadde i større grad enn de øvrige iverksatt tekniske tiltak. Eksempler på dette inkluderte segmentering av datanettverk, innføring av totrinnsinnlogging på nye IT-tjenester, bruk av ny sikkerhetsfunksjonalitet i MS 365, testing av sikkerheten i datanettverket (sårbarhetsskanning) og lukket sikkerhetshull avdekket i tekniske sikkerhetstester.

Fem av de sju virksomhetene hadde styrket sin evne til å oppdage, varsle og håndtere digitale sikkerhetshendelser. To av disse virksomhetene hadde anskaffet ekstern leverandør av tekniske sikkerhetstjenester (SOC). En tredje var i ferd med å gjøre det samme.

I tillegg ble det opplyst om andre tiltak for å styrke oppdagelsesevnen, for eksempel regelmessige tester av den tekniske sikkerheten i IT-tjenester og datanettverk.

Flere virksomheter hadde også forenklet og forbedret rutiner og skjema for varsling av hendelser og avvik.

Sårbarheter og tiltak

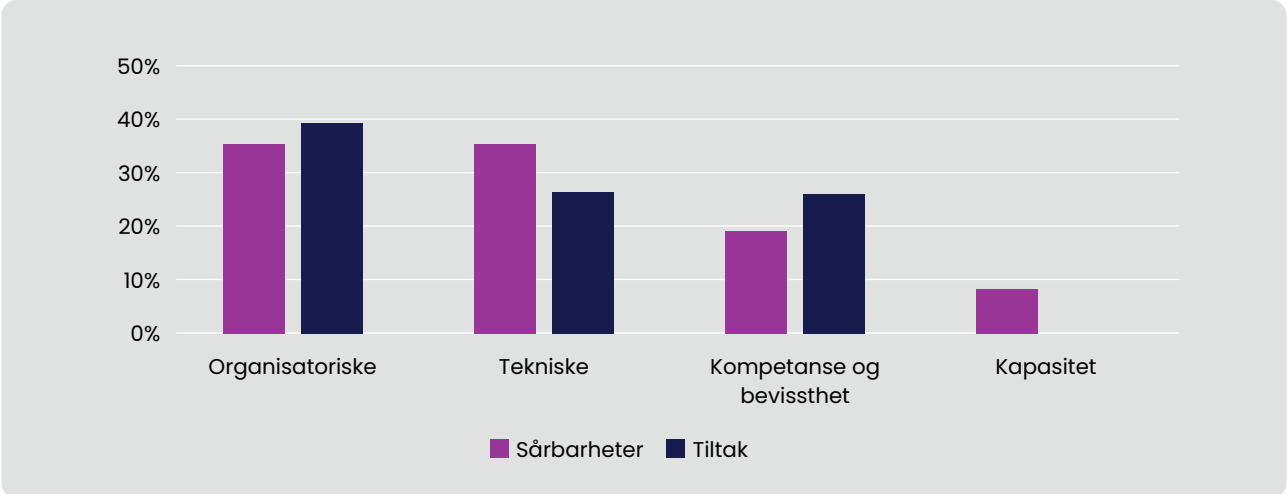
Neste spørsmål er i hvilken grad iverksatte tiltak var egnet til å utbedre de sårbarhetene som virksomhetene rapporterte om: ble det gjennomført tiltak der hvor virksomhetene mente at forbedringspotensialet var størst?

Figur 17[73] viser hvordan rapporterte tiltak fordeler seg på de ulike sårbarhetsområdene. Vi ser at det er et forholdsvis godt samsvar mellom iverksatte tiltak og rapporterte sårbarheter – flest tiltak iverksettes innenfor områder hvor utfordringene (sårbarhetene) vurderes å være størst.

Det er likevel viss en forskjell mellom tekniske tiltak og sårbarheter: tiltaksaktiviteten var noe lavere enn omfanget av rapporterte tekniske sårbarheter. Det motsatte var tilfelle når det gjelder kompetanse og bevissthet.

Disse resultatene indikerer at det fortsatt kan være rom for å gjøre tiltakene enda mer treffsikre sett opp mot virksomhetenes sårbarhetsprofil.

Figur 17: Forholdet mellom sårbarheter og tiltak, 2022



73 Figuren viser prosentandelen sårbarheter og tiltak som virksomhetene rapporterte om innfor de ulike sårbarhets- og tiltakskategoriene. Ved å standardisere tallene på denne måten blir det enklere å vurdere om tiltaksaktiviteten samsvarer (eller ikke) med de sårbarhetene som det ble opplyst om. Kapasitet er her målt i økningen av antall årsverk fra 2021 til 2022, hvor ett årsverk er regnet som ett tiltak.

Status – etterlevelse av kravene til personvern (GDPR)

Figur 18 nedenfor gir en oversikt over hvordan de sju virksomhetene etterlevde de særskilte kravene som departementets policy stiller til arbeidet med personvern (GDPR).

Dette gjelder primært punktene 6-10 og 11-12 i policyen. Figuren antyder derfor om tiltakene drøftet ovenfor hadde ført til forbedringer i policyetterlevelsen.

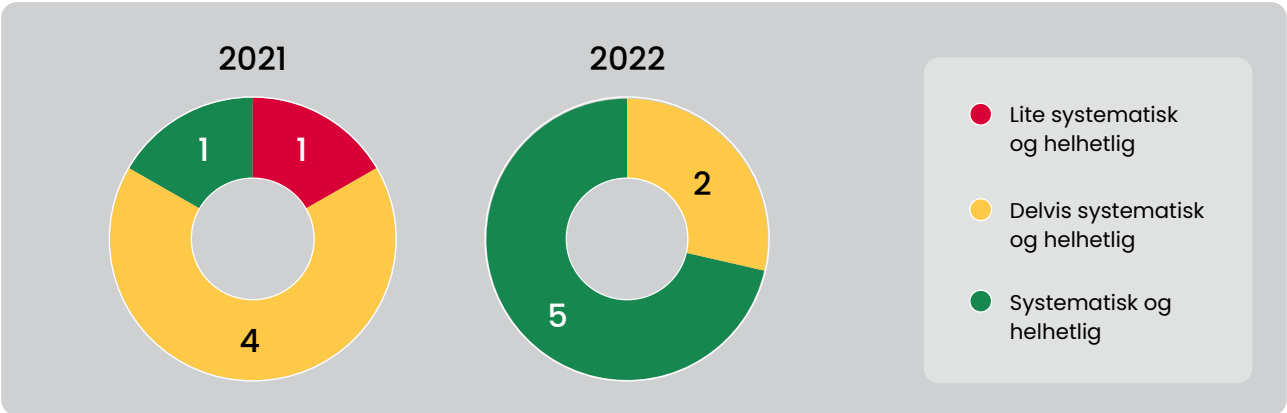
Statusvurderingen i figuren omfatter ikke kravene som stilles til sikring av personopplysninger. De inngår i vurderingen av status for arbeidet med informasjonssikkerhet, jf. figur 19.

Om statusvurderingene

Sammenlikning av status for 2022 og 2021, er noe haltende. Årsaken til dette er at antallet virksomheter som inngikk i statusvurderingene endret seg fra i fjor til i år. Fjorårets statusvurdering omfattet derfor seks virksomheter. Statusvurderingen for 2022 omfatter disse seks og én ny: Sikt.

Kriteriene for vurdering av status i figur 18 og 19 er de samme som for universitetene og høgskolene. Kriteriene er gjort rede for i kapittel tre.

Figur 18: Etterlevelse av krav til personvern, 2021 og 2022



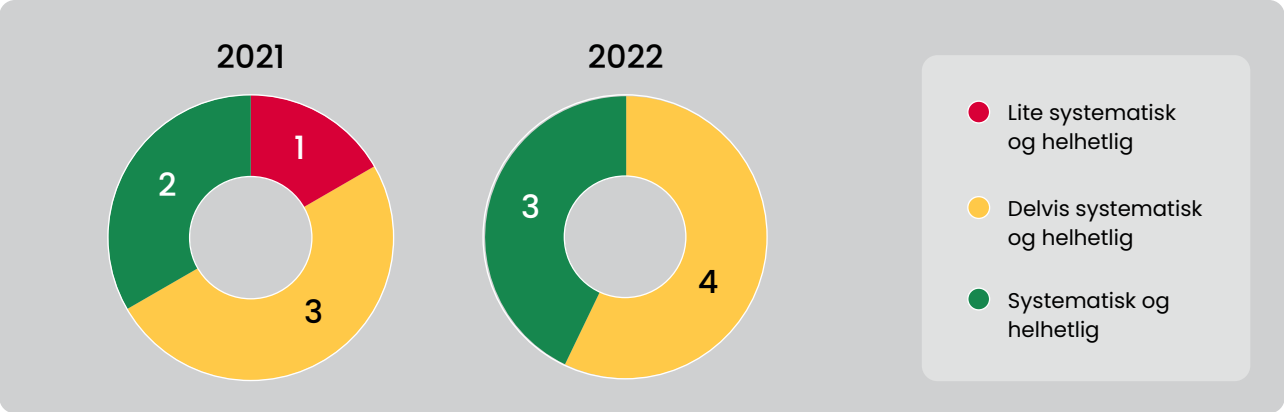
Figuren viser at mens én virksomhet ble vurdert å ha etablert et systematisk og helhetlig personvernarbeid i 2021, hadde fem virksomheter gjort det samme i 2022. Disse virksomhetene jobber langsiktig og planmessig med personvern (GDPR), prinsippet om kontinuerlig forbedring er tilfredsstillende institusjonalisert, og arbeidet har tydelig støtte fra toppledelsen og styret.

De to siste virksomhetene var i ferd med å tilfredsstille kravene i policyen: personvernarbeidet var delvis systematisk og helhetlig. Det betyr at disse virksomhetene hadde enkelte viktige avvik fra kravene i departementets policy. Begge bør imidlertid kunne bli «grønne» i løpet av 2023.

Status – etterlevelse av kravene til informasjonssikkerhet

Figur 19 gir en oversikt over hvordan de sju virksomhetene etterlevde kravene som departementets policy stiller til arbeidet med informasjons- og personopplysningssikkerhet. Dette gjelder primært krav i punktene 1-5 i policyen, men også punktene 11-12.

Figur 19: Status for etterlevelse av krav til informasjonssikkerhet, 2021 og 2022



Også når det gjelder kravene til informasjons- og personopplysnings-sikkerhet, ser vi en positiv utvikling fra 2021 til 2022. Endringene var likevel noe mindre enn med hensyn til personvernkravene i policyen.

I 2022 ble tre virksomheter vurdert å ha et systematisk og helhetlig arbeid med informasjons- og personopplysningssikkerhet mot to i 2021. Det innebærer at disse tre jobber langsiktig og planmessig med informasjonssikkerhet, prinsippet om kontinuerlig forbedring er institusjon-alisert, og arbeidet har støtte fra toppledelsen, eventuelt styret.

Samtidig hadde én virksomhet endret status fra «rød» til «gul». De fire «gule» virksomhetene i figuren hadde fortsatt enkelte viktige avvik fra policyens krav. Også for disse virksomhetene bør kunne oppnå tilfredsstillende etterlevelse i løpet av 2023.

Tre virksomheter etterlevde samtlige krav i policyen på tilfredsstillende vis i 2022. Dette er to flere enn i 2021. Vår vurdering er at det er sannsynlig at de øvrige fire virksomhetene kan oppnå det samme i 2023.

Oppfølging av anbefalinger

Forbedringene i status for etterlevelse av departementets policy, avspeiler seg i virksomhetenes oppfølginger av HK-dir sine skriftlige tilbakemeldinger (anbefalinger) om hvilke avvik fra policyen de har behov for å lukke. Av de til sammen 52 anbefalinger som virksomhetene mottok etter kartleggingen i fjor, hadde 42 av dem blitt fulgt opp i 2022. Åtte av anbefalingene hadde ikke blitt fulgt opp. For de to siste anbefalingene mangler vi tilstrekkelig informasjon til å vurdere graden av oppfølging.

Oppsummering og anbefalinger

De sju øvrige virksomhetene som kartlegges av HK-dir har et mindre omfattende og komplekst «verdilandskap» enn universitetene og høgskolene. Det avspeiler seg i at disse virksomhetene har relativt god oversikt over sine informasjonsverdier.

Der hvor vi har sammenliknbare tall over tid, ser vi en nedgang i antallet rapporterte brudd på informasjonssikkerheten og krenkelser av personvernet. I 2022 handlet slike saker i hovedsak om feil og uhell eller avvik fra egne rutiner. Det ble ikke rapportert om bekreftet eller mistenkt statlig hacking. Heller ikke tidligere har det vært et vesentlig problem i denne delen av sektoren.

De sju øvrige virksomhetene mente at organisatoriske mangler og tekniske sårbarheter var de viktigste utfordringene i 2022. Samtidig ble det iverksatt flest organisatoriske og pedagogiske tiltak. I 2022 var det likevel noe bedre samsvar mellom rapporterte sårbarheter og iverksatte tiltak i denne delen av UH-sektoren enn hva vi har sett tidligere. Det er imidlertid fortsatt rom for ytterligere å bedre samsvaret.

Status for etterlevelse av departementets policy for informasjonssikkerhet og personvern hadde forbedret seg fra 2021 til 2022. Forbedringene var størst med hensyn til de særskilte personvernkravene i policyen, men også når det gjaldt informasjons- og personopplysningssikkerhet hadde det skjedd viktige forbedringer.

Vi antar at etterlevelsen av kravene i policyen vil bli styrket ytterligere i løpet av inneværende år. Dette kan blant annet oppnås ved at misforholdet mellom rapporterte sårbarheter og iverksatte forbedringstiltak reduseres.

Vi ser ingen sterke grunner til å foreslå særskilte sektortiltak for de sju virksomhetene som er behandlet i dette kapitlet. Foreslåtte tiltak for universitets- og høgskoledelen av sektoren vil derfor også være relevante her.

Kapittel 5

Risiko, mål og anbefalinger

Kapittel 5

Risiko, mål og anbefalinger

Innledning

I fjorårets rapport vurderte vi risikoen for hendelser (risikoscenarier) som kan føre til at informasjonsverdier i sektoren går tapt, skades, misbrukes eller eksponeres for uvedkommende.[74] I dette kapitlet følger en revidert og oppdatert vurdering av disse risikoscenariene.

Det gis også en oppdatert vurdering av om målene for informasjonssikkerhet og personvern i strategien for digital omstilling i UH-sektoren[75] kan realiseres i løpet av strategiperioden. En forutsetning for å nå målene i strategien, er tilfredsstillende etterlevelse av departementets policy for informasjonssikkerhet og personvern.[76] Graden av policyetterlevelse gir derfor en god indikasjon på mulighetene for måloppnåelse.

Til slutt oppsummerer vi våre anbefalinger til sektortiltak som kan bidra til å styrke informasjonssikkerheten og personvernet hos virksomhetene som omfattes av departementets policy. Anbefalingene er skissert i tidligere kapitler.

---

74 Se «Risiko- og tilstandsvurdering 2022», kapittel 5. https://hkdir.no/rapportar/informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning. Sist besøkt 22.03.2023.

75 Strategi for digital omstilling i universitets- og høgskolesektoren 2021-2025, er tilgjengelig på https://www.regjeringen.no/contentassets/c151afba427f446b8aa44aa1a673e6d6/no/pdfs/kd-strategi-digital-omstilling.pdf. Sist besøkt 22.03.2023.

76 Policyen er kommunisert til sektoren i rundskriv F-04-20. Se https://www.regjeringen.no/no/dokumenter/f-04-20-policy-for-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning/id2769629/. Sist besøkt 22.03.2023.

Bakgrunnen for vurdering av risiko

Våre vurderinger av risiko for hendelser og muligheter for måloppnåelse tar utgangspunkt i viktige funn og konklusjoner diskutert i de foregående kapitlene. Vi mener følgende forhold er særlig relevante for vurdering av risiko og måloppnåelse:

- Sektoren har forbedret sin oversikt over informasjonsverdier – opplysninger, programvare, datamaskiner, nettverksutstyr, osv. – som skal beskyttes mot trusler og håndteres i henhold til rettslige krav. Hos universitetene og høgskolene var oversikten over personopplysninger i administrasjon og undervisning fortsatt noe mangelfull. Sektoren jobber med å få oversikter over informasjonsverdier som er undergitt eksportkontroll.

- Sektorens informasjonsverdier ble utsatt for færre brudd på informasjonssikkerheten og krenkelser av personvernet enn tidligere: ca. 30 prosent nedgang i antallet hendelser og brudd i 2022 hos universitetene og høgskolene. Hos de sju øvrige virksomhetene hadde det vært en mindre økning, men dette skyldes at flere virksomheter inngikk i årets kartlegging enn i 2021. Ingen av hendelsene medførte alvorlige skadevirkninger.

- Sektoren hadde forbedret sin evne til å oppdage, varsle og håndtere brudd på informasjonssikkerheten og krenkelser av personvernet, blant annet ved bruk av nye sikkerhetstjenester og forbedring av varslingsrutiner.

- Nettkriminelle grupper og tekniske eller menneskelige feil og uhell utgjorde de viktigste truslene. Rapporterte tilfeller av forsøk på statlig hacking var vesentlig redusert sammenliknet med 2021.

- Antallet meldinger til Datatilsynet om brudd på sikkerheten til personopplysninger gikk ned med drøyt 40 prosent hos universitetene og høgskolene i 2022. Universitetene og høgskolene rapporterte om ca. 22 prosent færre personvernsaker (brudd og avvik) sammenliknet med året før.

- Antallet årsverk øremerket for arbeidet med informasjonssikkerhet og personvern økte med drøyt 10, det vil si til omkring 128 årsverk, hos de 28 virksomhetene.

- Tiltaksaktiviteten var relativt høy også i 2022. Det ble iverksatt flest organisatoriske og pedagogiske tiltak. Fordelingen av tiltakene samsvarte ikke alltid like godt med de områdene (sårbarhetene) hvor de 28 virksomhetene selv mente at de hadde størst behov for forbedringer.

- Sektoren hadde styrket sin etterlevelse av kravene i departementets policy for informasjonssikkerhet og personvern. Dette var særlig tydelig hos de sju direktoratene og selskapene.

- Hos universitetene og høgskolene var styrkingen noe ujevnt fordelt mellom de ulike hovedkravene i policyen. Men også denne delen av sektoren hadde gjort fremskritt i sitt etterlevelsesarbeid i 2022, uten at flere institusjoner ble vurdert å overholde samtlige hovedkrav i policyen enn i 2021.

Spørsmålet er hvordan disse funnene og konklusjonene påvirker risikoen i sektoren for brudd på informasjons- og personopplysningssikkerheten?

Rammeverket for vurdering av risiko

Vi benytter det samme rammeverket for vurdering av risiko som i fjorårets risiko- og tilstandsvurdering. Her vurderes risikoscenarier – hendelser som fører til brudd på informasjons- og personopplysningssikkerheten – langs to dimensjoner: (i) sannsynligheten for at brudd kan skje og (ii) mulige skadevirkninger dersom brudd skulle skje.

Sannsynlighet operasjonaliseres som forventet hendelsesfrekvens – hvor ofte vi antar at bestemte brudd kan skje. Skadevirkningene er sammensatte og kan ramme ulike aktører og interesser, for eksempel utførelsen av kjerneoppgaver, enkeltpersoner eller grupper (ansatte, studenter, forskningsdeltakere, osv.) og nasjonale interesser.

I tekstboksen nedenfor gis en kort forklaring til hvordan vi har operasjonalisert sannsynlighet og skadevirkninger.

En nærmere fremstilling av rammeverket for vurdering av risiko – og verdiene for sannsynlighet og skadevirkninger – finnes i vedlegg 3.

Sannsynlighet og skadevirkninger

Vi benytter fire sannsynlighetsverdier. Disse varierer mellom ekstremverdiene «svært sannsynlig» (det forventes at hendelsen kan skje flere ganger hver måned) og «svært lite sannsynlig» (det forventes at hendelsen kan skje sjeldnere enn hvert femte år).

Vi benytter følgende verdier for skadevirkning (konsekvensverdier):

- **Personvernkrenkelser**: eksempler på krenkelser ved brudd på sikkerheten til personopplysninger inkluderer at uvedkommende får tilgang til opplysningene, den registrerte får ikke tilgang til egne opplysninger, opplysningene endres eller slettes slik at de blir feil eller misvisende, opplysningene anvendes til formål som den registrerte ikke kjenner til, opplysningene er utilgjengelige for rettmessige brukere.
- **Tjenesteavbrudd**: kjerneoppgaver utføres ikke på grunn av manglende tilgang til informasjonsverdier (IT-tjenester eller data/opplysninger).
- **Økonomi**: eksempler på økonomiske kostander er overtidsarbeid ved hendelseshåndtering, innleie av ekstern assistanse i forbindelse med hendelseshåndtering og gjenoppretting av normal drift; gjenskaffe tapte data/opplysninger; gjenkjøp av IT-utstyr; overtredelsesgebyr fra Datatilsynet.
- **Omdømme og tillit**: eksempler på omdømmeskade og tillitstap er misnøye blant egne brukere; oppslag i riksmedia som kan svekke allmennhetens tillit til sektoren; offentlig kritikk av sektorens arbeid (for eksempel fra Datatilsynet eller Riksrevisjonen); brudd og hendelser som får politiske følger (spørsmål til og kritikk av politisk ledelse, osv.).
- **Nasjonale interesser**: eksempler på denne typen skader er uautorisert tilgang til forskningsdata/-resultater innen områder som har betydning for nasjonale interesser; brudd på internasjonale forpliktelser, for eksempel ulovlig kunnskapsoverføring.

Risikoscenarier og risikonivå

Risikoscenariene vi vurderer, er brudd på informasjons- og personopplysningssikkerheten som virksomhetene i UH-sektoren rapporterte om eller som de uttrykte bekymring for.

Nedenfor vurderer vi risiko for hver enkelt av de ulike risikoscenariene.

Som tidligere år, var nettfiske og kompromittering av brukerkontoer de vanligste metodene som trusselaktører benyttet i forsøkene på å bryte informasjons- og personopplysningssikkerheten til virksomhetene i UH-sektoren.

Maskinlæring og språkmodeller

Informasjonssikkerhet og personvern ved bruk av maskinlæring, spesielt språkmodeller som ChatGPT[77] og Bard[78], var ikke problemstillinger som ble nevnt under årets kartlegging. Men ChatGPT – og i det siste GPT4 – har ført til diskusjoner i sektoren om hva denne typen tjenester kan benyttes til. Eksamensfusk, det vil si at chatbot-tjenester som kan gjøre fusk enklere å gjennomføre og vanskeligere å oppdage, har vært særlig mye debattert.[79]

I årets risikovurdering har vi likevel ikke lagt spesielt vekt på betydningen av maskinlæring og språkmodeller for informasjons- og personopplysningssikkerheten i UH-sektoren. Vi erkjenner imidlertid at denne teknologien reiser flere sikkerhetsmessige problemstillinger som sektoren må ta stilling til og håndtere fremover.[80] Det er derfor trolig at dette vil være viktige momenter i HK-dir sine fremtidige vurderinger av risiko på sektornivå.

Scenario 1: løsepengevirusangrep[81] – høy risiko

Alle virksomheter kan bli utsatt for løsepengevirusangrep, og flere norske virksomheter i ulike bransjer og sektorer har opplevd større hendelser av denne typen de siste årene.[82] I 2022 ble det rapport om flere sannsynlige forsøk på løsepengevirusangrep i UH-sektoren.[83] Forsøkene ble vanligvis oppdaget tidlig og avverget.

I ett tilfelle lyktes likevel angriperen med å kryptere innholdet på en lokal datamaskin, men informasjonen på maskinen kunne gjenopprettes fra sikkerhetskopi. Resten av datanettverket ble ikke berørt (se kapittel 2).

Virksomhetene i UH-sektoren har iverksatt tiltak som reduserer sannsynligheten for at større løsepengevirusangrep skal lykkes, det vil si at hele eller store deler av det lokale datanettverket settes ut av spill. Det inkluderer blant annet totrinnsinnlogging, segmentering av datanettverk og testing av sikkerheten for å avdekke og fikse tekniske sårbarheter (se særlig kapittel 3 og 4). Samtidig har flere virksomheter gjennomført tiltak for å kunne gjenopprette kryptert informasjon (nye back-up-løsninger).

77 https://openai.com/blog/chatgpt. Sist besøkt 22.05.2023.

78 https://bard.google.com/?hl=en. Sist besøkt 22.05.2023.

79 Se for eksempel https://khrono.no/emne/chatgpt. Sist besøkt 22.05.2023.

80 For en oversikt over viktige problemstillinger, se for eksempel Standford Center for Security and Emerging Technology (2023): «Adversarial Machine Learning and Cybersecurity. Risks, Challenges and Legal Implications». https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2023-04/adversarial_machine_learning_and_cybersecurity_v7_pdf_1.pdf. Sist besøkt 22.05.2023. Se også det nasjonale cybersikkerhetssenteret i Storbritannia (NCSC) sine temasider om kunstig intelligens: https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=artificial%20intelligence&sort=date%2Bdesc. Sist besøkt 22.05.2023.

81 Løsepengevirus er skadelige programvare som kan gjøre alle datamaskiner i et datanettverk ubrukbare (innholdet på maskinene krypteres). Offret blir bedt om å betale en løsepengesum til angriperen, vanligvis en nettkriminell gruppe. Dersom utbetaling skjer, lover angriperne at de vil sørge for at datamaskinene – og arbeidsprosessene som er avhengig av dem – igjen skal fungere.

82 Se for eksempel «Risiko- og tilstandsvurdering 2022», kapittel 2. https://hkdir.no/rapportar/informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning. Sist besøkt 23.03.2023. Se også kapittel 2 i denne rapporten.

83 Omfanget av denne typen trussel-aktivitet er fortsatt stort internasjonalt, se for eksempel rapport fra sikkerhetsselskapet Sophos: «The State of Ransomware 2023». https://www.sophos.com/en-us/whitepaper/state-of-ransomware. Sist besøkt 21.05.2023.

Vår vurdering av risikoen for løsepengevirusangrep er likevel den samme som tidligere, det vil si at risikoen fortsatt er høy. Dette fordi skadevirkningene av vellykkede løsepengevirus kan bli svært store og sammensatte. Det kan blant annet dreie seg om omfattende tjenesteavbrudd – kjerneoppgaver blir umulig å utføre for en kortere eller lengre periode. Videre kan angriperne stjele informasjon fra virksomhetene, typisk personopplysninger, og true med å offentliggjøre dem dersom løsepenger ikke betales.

De økonomiske tapene i form av oppryddingskostnader og tjenesteavbrudd (oppgaver som ikke utføres) kan også bli høye.[84] Det samme gjelder andre typer økonomiske tap, for eksempel knyttet til permanent tap av viktige forskningsdata eller andre typer data. I enkelte tilfeller kan skadene være irreversible.

Vi antar dessuten at større løsepengevirusangrep vil medføre medieoppslag som påvirker omdømme og tilliten til enkeltinstitusjoner, eventuelt til sektoren som sådan.

Scenario 2: statlig kunnskapsspionasje –høy til lav risiko

I 2021 ble det rapportert om trusselaktivitet rettet mot datanettverkene til en rekke universiteter og høgskoler, trolig for å finne tekniske sårbarheter, hvor statlige hackergrupper ble mistenkt å stå bak. Det ble også opplyst om enkelte forsøk på datainntrenging fra slike grupper.

I 2022 var antallet rapporter om bekreftet eller mistenkt statlig trusselaktivitet betydelig redusert (se kapittel 2). Det var bare hos én virksomhet at det ble rapportert om nye hendelser hvor det var mistanke om statlig involvering. Virksomheter som tidligere år har registrert mistenkte eller bekreftede forsøk på statlig datainntrenging, rapporterte ikke om dette i 2022.

Flere av tiltakene drøftet i kapittel 3 og 4, spesielt innføring av totrinnsinnlogging og sikkerhetstesting (sårbarhetsskanning), kan bidra til å redusere sannsynligheten for at datainntrenging fra statlige hackergrupper vil lykkes. Enkelte av tiltakene kan også redusere skadevirkningene av vellykkede forsøk, for eksempel nettverkssegmentering og forbedret evne til raskt å oppdage kunnskapstyveri.

Vi mener likevel at risikoen for statlige hackerangrep fortsatt er høy i deler av UH-sektoren. Det samme bemerkes av EOS-tjenestene i deres årlige risiko- og trusselvurderinger. EOS-tjenestene fremhever at enkelte forsknings- og kunnskapsområder kan være særlig utsatt for denne typen trusselaktivitet.[85] Videre viser EOS-tjenestene til at Ukraina-krigen innebærer at etterretningstrusselen er forhøyet, inkludert i UH-sektoren.

Som for løsepengevirusangrep, legger vi til grunn at skadevirkningene av statlige hackerangrep kan bli betydelige. Også dette taler for at risikoen fortsatt er høy i deler av sektoren. De mest alvorlige skadevirkningene vil trolig handle om nasjonale interesser, for eksempel kompromittering av kunnskap undergitt eksportkontroll eller andre internasjonale reguleringer (sanksjonsforskrifter). Slike hendelser kan også skade omdømme og tillit til enkeltinstitusjoner og sektoren som sådan. For berørte virksomheter kan opprydningskostnadene bli store.

Som bemerket i fjorårets rapport, er det trolig at risikoen for statlig hacking – etterretning og kunnskapsspionasje – er ujevnt fordelt i sektoren. Vi mener derfor at risikoen for slike hendelser er relativt lav hos flere av høgskolene. Dette er virksomheter med en faglig profil som i liten grad samsvarer med kunnskapsområder som EOS-tjenestene mener kan være gjenstand for utenlandsk etterretning. Vi er heller ikke kjent med at disse virksomhetene har forskningsaktiviteter innenfor områder som er undergitt eksport- eller andre spredningsbegrensninger.

84 Ifølge IBM, var den gjennomsnittlige kostnaden ved vellykkede løsepengevirusangrep i 2022 i underkant av 50 millioner kroner (4.54 millioner dollar). «Cost of Data Breach Report 2022», side 6. https://www.ibm.com/reports/data-breach. Sist besøkt 21.05.2023.

85 I kapittel 2 har vi sett at det kan gjelde forskningsmiljøer innenfor fagområder som undervanns- og dypvannsteknologi, kontrollsystemer, maskinlæring, datasikkerhet, nanoteknologi, satellitt- og missilteknologi og teknologi tilpasset arktiske forhold. Også forskning knyttet til nordområdene kan være av interesse for statlige trussel-aktører.

Scenario 3: utilsiktede feil og uhell – middels risiko
I 2022 som tidligere år, ble det rapportert om forholdsvis mange innsidehendelser: brudd eller krenkelser som skyldes utilsiktede menneskelige eller tekniske feil og uhell (ikke fremprovosert av trussel-aktører). Selv om antallet brudd på personopplysningssikkerheten som ble meldt til Datatilsynet var vesentlig redusert, utgjorde utilsiktede feil og uhell en høy andel av disse bruddene (se kapittel 2).

Virksomhetene hadde imidlertid iverksatt tiltak i 2022 som reduserer sannsynligheten for utilsiktede feil og uhell. I kapittel 3 og 4 har vi for eksempel sett at pedagogiske tiltak – opplæring, kompetanseheving og bevisstgjøring – var en viktig tiltakskategori. Dette er tiltak som blant annet hadde til hensikt å sørge for sikker håndtering av personopplysninger og andre viktige informasjonsverdier.

I tillegg hadde rutiner og systemer for varsling av utilsiktede brudd og krenkelser blitt forbedret. Dette kan redusere skadevirkningene ved at slike hendelser varsles og håndteres raskere enn tidligere.

Skadevirkningene av utilsiktede feil og uhell var heller ikke i 2022 svært alvorlige. Det handlet primært om noe tapt arbeidstid ved kortere avbrudd i eksterne tjenesteleveranser og enkelte personvernkrenkelser. Det siste dreide seg i hovedsak om at ansatte hadde fått tilgang til personopplysninger de ikke hadde tjenstlige behov for, for eksempel ved feilsending av epost. Det var likevel mindre krenkelser – feil og uhell som rammet få personer.

Vår vurdering er derfor at risikoen for brudd og krenkelser som følge av utilsiktede feil og uhell er litt lavere enn tidligere, primært fordi forekomsten av denne typen er noe mindre enn før. Antallet hendelser med skadevirkninger – målt som brudd meldt til Datatilsynet – er også redusert. Vi mener likevel at slike hendelser kan i verstefall medføre vesentlige krenkelser av personvernet.

Scenario 4: direktør- og fakturasvindel – lav risiko
Heller ikke i 2022 ble det rapportert om mange og store direktør- eller fakturasvindelsaker i UH-sektoren. Den mest alvorlige hendelsen gjaldt urettmessig utbetaling av en månedslønn (dekanlønn). Ellers ble det rapportert om et par tilfeller hvor ansatte hadde blitt lurt til å kjøpe gavekort.

Sannsynligheten for vellykkede nettsvindelforsøk fremstår som lavere enn tidligere, blant annet fordi det rapporteres om økt bevissthet om direktør- og fakturasvindel, særlig blant økonomimedarbeiderne. I tillegg har mer effektive løsninger for deteksjon og sperring av skadelig epost bidratt til at sannsynligheten for direktør- og fakturasvindel trolig er redusert.

Samtidig har skadevirkningene av vellykket direktør- eller fakturasvindel vanligvis ikke vært veldig alvorlige i UH-sektoren.[86] Likevel er det viktig å være oppmerksom på at nettsvindel, inkludert direktør- og fakturasvindel, er en profitabel form for kriminalitet internasjonalt.[87]

Vår vurdering er derfor at sannsynligheten for at det utbetales store beløp som følge av direktør- eller fakturasvindel, er relativt liten. Samtidig utsettes virksomhetene for kontinuerlige forsøk på direktør- og fakturasvindel. Dermed er det fortsatt behov for årvåkenhet i sektoren når det gjelder nettsvindel generelt og direktør- eller fakturasvindel spesielt.

Scenario 5: tjenestenekt (DDoS[88]) – middels risiko
I 2022 ble det rapportert om ett større tjenestenektangrep i UH-sektoren. Tidligere år har det ikke vært rapportert om store tjenestenektangrep, og sektorens responsmiljø hos Sikt har i 2020 og 2021 registrert få tjenestenektangrep i forskningsnettet.

Ukraina-krigen førte imidlertid til at flere offentlige virksomheter i Norge har vært utsatt for slike angrep i 2022. Tjenestenektangrepet nevnt ovenfor hadde også trolig sin bakgrunn i denne konflikten.

Skadevirkningene av tjenestenektangrep kan variere noe, for eksempel at hjemmesiden er midlertidig nede eller at eksamen må utsettes fordi

86 Det har likevel vært ett tilfelle i sektoren de siste årete hvor et tosifret antall millioner ble utbetalt til en nettkriminell aktør (fakturasvindel). I slike tilfeller er de økonomiske tapene merkbare. Samtidig kan medieoppslag skade omdømmet til den aktuelle virksomheten.

87 Se for eksempel Federal Bureau of Investigation: Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Sist besøkt 23.03.2023.

88 DDoS-angrep innebærer at trussel-aktører sender så mye datatrafikk mot utvalgte datamaskiner (webtjenester) at de ikke greier å håndtere trafikkmengden. Dermed blir maskinene (tjenestene) utilgjengelige for legitime brukere.

den digitale eksamensløsningen er utilgjengelig. Vi er ikke kjent med at tjenestenektangrep har ført til skadevirkninger av betydning i UH-sektoren de siste fem årene.

Vi mener likevel at risikoen for tjenestenektangrep mot virksomheter i UH-sektoren bør forhøyes – fra lav til middels. Dette begrunner vi med at sannsynligheten for tjenestenekt-angrep kan være noe høyere enn tidligere, særlig på grunn av krigen i Ukraina (hevnaksjoner fra russiske trussel-aktører mot vestlige land som støtter Ukraina). Vi har ikke grunnlag for å mene at skadevirkningene vil bli mer alvorlige enn før.

Scenario 6: misbruk av lokale dataressurser – middels risiko

I 2022 ble det i liten grad rapportert om at trussel-aktører hadde kompromittert lokale datamaskiner for å utvinne kryptovaluta eller gjennomføre dataangrep mot andre virksomheter. Tidligere år har rapporter om denne typen hendelser ikke vært uvanlige i UH-sektoren. I noen av tilfellene hadde trussel-aktører hatt tilgang til lokale datamaskiner i mange måneder før det ble oppdaget og stoppet.

Flere av tiltakene drøftet i kapittel 3 og 4 har bidratt til at sannsynligheten for disse formene for misbruk av lokale dataressurser trolig er noe redusert. Innføring av totrinnsinnlogging har for eksempel ført til en nedgang i antallet kompromitterte brukerkontoer. Dermed har det blitt vanskeligere for trussel-aktører å få tilgang til virk-somhetenes datamaskiner. Bruk av ny sikkerhetsfunksjonalitet som stopper nettfiskeforsøk og jevnlig testing av datasikkerheten (sårbarhetsskanning) har bidratt til det samme.

Misbruk av dataressurser trenger ikke å medføre alvorlige skadevirkninger for virksomheter som utsettes for det. I tilfeller hvor forskningsinfrastruk-turer har blitt benyttet til utvinning av kryptovaluta, kan prosesseringen av forskningsdata ha tatt noe lengre tid enn ellers. Strømregningen til virksomheten kan også ha økt noe.

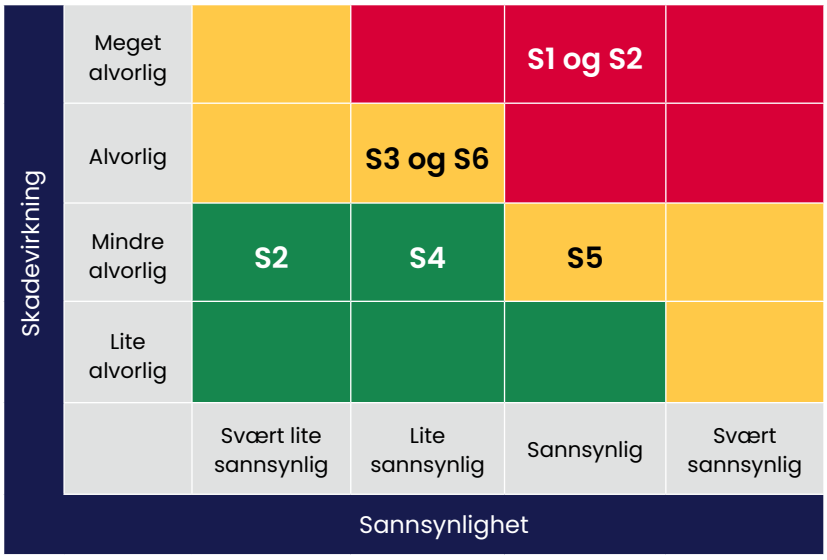
I tilfeller hvor trussel-aktører har anvendt lokale digitale ressurser i operasjoner rettet mot andre virksomheter, har det skjedd en form for risikooverføring – de største potensielle skadevirkningene rammer andre virksomheter enn den som i utgangspunktet ble kompromittert. De reelle virkningene av slike hendel-ser kan derfor være uoversiktlige og sammensatte.

Vi mener derfor at risikoen for misbruk av lokale dataressurser til kriminelle eller statlige formål, er middels. Sannsynligheten for dette er noe redusert de siste årene, men dersom lokale dataressurser misbrukes kan skadevirkningene ramme relativt bredt, også utenfor UH-sektoren (risikooverføring).

Risikomatrisen

Risikoen for de seks scenariene oppsummeres i risikomaterien nedenfor. Scenariene benevnes S1 – S6:

- S1 = løsepengevirus.
- S2 = statlig kunnskapsspionasje.[89]
- S3 = utilsiktede feil og uhell.
- S4 = direktør- og fakturasvindel.
- S5 = tjenestenekt (DDoS).
- S6 = misbruk av lokale dataressur-ser (utvinning av kryptovaluta og dataangrep mot tredjeparter).



89 Risikoscenariet (kunnskapsspionasje) er markert i to ulike celler i risikomatrisen nedenfor. Dette for å tydeliggjøre at risikoen vurderes å være ujevnt fordelt i sektoren.

Muligheter for måloppnåelse

Neste spørsmål er hvordan funnene i denne rapporten påvirker mulighetene for at informasjonssikkerhets- og personvernmålene i sektorens strategi for digital omstilling[90] kan realiseres?

Vurdering av måloppnåelse
Vi har ikke funnet grunnlag for å endre våre vurderinger av sannsynligheten for måloppnåelse sammenliknet med fjorårets risiko- og tilstandsvurdering.

Vår vurdering av måloppnåelse er derfor følgende:

- Alle de sju direktoratene og selskapene vil trolig kunne oppnå strategimålene om informasjonssikkerhet og personvern.
- Målene i strategien vil trolig kunne nås hos 13 av de 21 universitetene og høgskolene.
- Det er mer usikkert om de siste åtte universitetene og høgskolene vil gjøre det samme. Vi regner det likevel som realistisk at flertallet av disse institusjonene vil kunne oppnå målene.

Målene i strategien for digital omstilling

I strategien for digital omstilling omtales informasjonssikkerhet og personvern som én av seks forutsetninger for digitalisering. Det innebærer at arbeidet med informasjonssikkerhet og personvern skal sørge for at utdanning, forskning, formidling og administrasjon gjennomføres på en sikker og tillitsvekkende måte.

Videre sies det at forvaltningen av data i sektoren stiller store krav til forsvarlig behandling av personopplysninger og god informasjonssikkerhet.[91] Ansatte og studenter må derfor ha god kunnskap om informasjonssikkerhet og personvern.[92]

Det sies også at informasjonssikkerhet og personvern må prioriteres høyt i forskningsinfrastrukturer og ved deling av forskningsdata.[93]

Målene i strategien stiller ikke andre krav til informasjonssikkerhet og personvern enn hva som følger av departementets policy for informasjonssikkerhet og personvern.

Usikkerheten handler dels om at enkelte av høgskolene oppgir å mangle kapasitet til å forbedre arbeidet med informasjonssikkerhet og personvern ytterligere. Avhengighet av få ansatte kan i tillegg sette arbeidet tilbake dersom disse prioriterer andre oppgaver. Dels handler det om at enkelte større institusjoner oppgir at det vil ta to-tre år å etablere et systematisk og helhetlig informasjonssikkerhets- og personvernarbeid i hele organisasjonen.

90 «Strategi for digital omstilling i universitets- og høgskolesektoren, 2021-2025». https://www.regjeringen.no/no/dokumenter/strategi-for-digital-omstilling-i-universitets-og-hoyskolesektoren/id2870981/. Sist besøkt 23.03.2023.

91 Ibid., side 22.

92 Ibid., side 26-29 og 32.

93 Ibid., side 19.

Risikohåndtering – forslag til sektortiltak

Mot denne bakgrunn mener vi at arbeidet med informasjonssikkerhet og personvern i sektoren fortsatt bør styrkes. Dette er nødvendig for å utbedre sårbarheter, redusere risiko, styrke policyetterlevelse og bidra til måloppnåelse.

Nedenfor revideres og oppdateres fjorårets anbefalinger i lys av funnene og konklusjonene diskutert i de tidligere kapitlene. Tiltakene er kort skissert i oppsummeringene til tidligere kapitler.

Verdikartlegging og kartleggingsverktøy
Sektoren har fortsatt utfordringer med å få oversikt over enkelte av informasjonsverdiene som de forvalter, inkludert behandlinger av personopplysninger og verdier undergitt eksportkontroll.

Vi anbefaler derfor at sektoren tilbys råd og veiledning om hvordan kartlegging av verdier best kan gjennomføres i praksis, spesielt hvilke arbeidsverktøy som kan benyttes.

Oppdagelse og håndtering av hendelser
Sektorens evne til raskt å oppdage informasjonssikkerhetshendelser og å begrense skadevirkningene av dem, er styrket i 2022. Det er likevel behov for at oppdagelses- og håndteringskapasiteten forbedres i takt med endringer i trusselbildet.

Vi anbefaler derfor at informasjons- og opplæringstilbudet til sektorens hendelseshåndteringsteam (IRT) fortsatt styrkes.

I tillegg anbefaler vi følgende tiltak:

- videreutvikling av analyse- og responskapasitet hos Sikt (eduCSC),
- videreutvikling av dagens sikkerhetstester som Sikt gjennomfører (styrket sårbarhetsstyring),
- forbedre veilednings- og kurstilbudet i sektoren med hensyn til deteksjon og håndtering av IT-sikkerhetshendelser,
- styrke bistanden til sektoren når det gjelder utvikling av beredskaps- og kontinuitetsplaner på IT-området.

Opplæring og kompetanseheving
Manglende kompetanse og bevissthet om krav til og gjennomføring av arbeidet med informasjonssikkerhet og personvern, er viktige sårbarheter i sektoren. Kompetanse har vist seg utfordrende å skaffe gjennom rekruttering og nyansettelser.

Vi anbefaler derfor fortsatt satsing på kompetansehevende tiltak og utvikling av opplæringstilbudet i sektoren. Det gjelder særlig følgende tiltak:

- styrke veiledningen om og bistanden til innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR),
- tilby rådgiving om organisering og styring av arbeidet med informasjonssikkerhet og personvern som er tilpasset den enkelte virksomhet,
- etablere et tilbud om revisjoner av den enkelte virksomhet sitt arbeid med informasjonssikkerhet og personvern,
- videreutvikle sektorens møteplasser for informasjonsutveksling og erfaringsdeling (CISO- og personvernombudsforum).

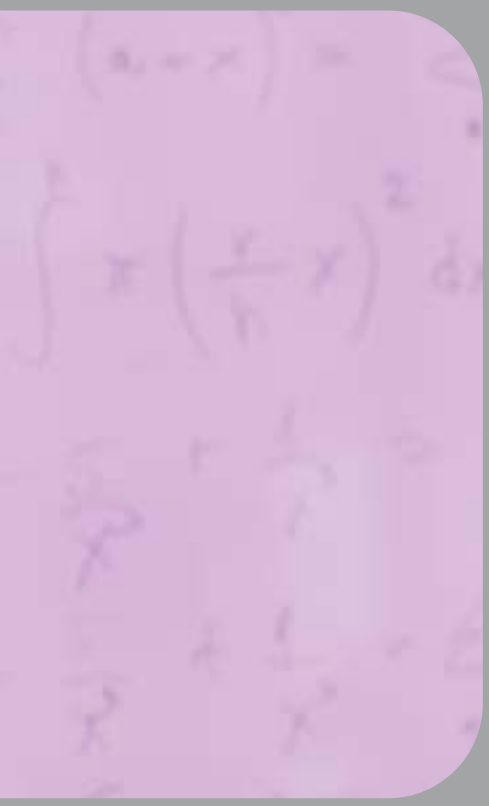
Krav til fellestjenester
Enkelte virksomheter i sektoren anskaffer og forvalter viktige IT-tjenester som benyttes av de øvrige virksomhetene (kunder). Det er imidlertid den enkelte kunde som har det rettslige hovedansvaret for informasjonssikkerheten og personvernet i disse tjenestene. Det betyr at dersom det tilbys fellestjenester hvor kravene til informasjonssikkerhet og personvern ikke er godt nok ivaretatt, overføres risikoen som dette innebærer til den enkelte kunde.

Vi anbefaler derfor at det stilles tydelige forventninger til virksomheter som tilbyr fellestjenester om at krav til informasjonssikkerhet og personvern er ivaretatt (så langt som praktisk mulig) før tjenestene tas i bruk i sektoren.

Scenarier med høy risiko
I risikoscenario S1 – S2 vurderes risikoen for brudd på informasjons- og personopplysningssikkerheten som høy (løsepengevirus og statlig kunnskapsspionasje).

Vi anbefaler at sektortiltakene diskutert ovenfor innrettes slik at risikoen for disse scenariene reduseres. Reduksjon av risikoen for løsepengevirus og statlig kunnskapsspionasje bør derfor være sentrale tema i kompetansehevende aktiviteter, og i rådgivings- og veiledningsarbeidet til Sikt (eduCSC).

Vedlegg



VEDLEGG

Vedlegg 1:

Datagrunnlaget og arbeidet med rapporten

Rapporten bygger primært på informasjon innhentet gjennom kartleggingsmøter i sektoren. Slike møter ble gjennomført med hver av de 21 statlig eide universitetene og høgskolene, og de sju øvrige forvaltningsorganer og selskaper som omfattes av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i UH-sektoren.

Kartleggingsmøtene med til sammen 28 virksomheter ble gjennomført i perioden 7. november 2022 til 13. februar 2023.

Forberedelse og kontakt
Virksomhetene mottok brev fra HK-dir om kartlegging. Brevene til 13 første virksomhetene ble sendt ut i oktober 2022. Brevene til de siste 15 virksomhetene ble sendt ut i november 2023.

Et sett med spørsmål om arbeidet med informasjonssikkerhet og personvern (kartleggingsskjema) var vedlagt brevene (kartleggingsskjemaet finnes i vedlegg 2). Hensikten med møtene var å få svar på spørsmålene i skjemaet.

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

HK-dir stilte med to eller tre deltakere.

Gjennomføring og datainnsamling
Alle kartleggingsmøter ble avholdt som videokonferanser, og det var satt av 1,5 time til besvarelse av spørsmålene i kartleggingsskjemaet.

Hos enkelte institusjoner og virksomheter tok gjennomgangen av spørsmålene i skjemaet noe lengre tid enn berammet.

Fra tre av universitetene mottok HK-dir skriftlige besvarelser på spørsmålene. De skriftlige svarene ble gjennomgått under møtet med disse institusjonene.

Hos de øvrige virksomhetene ble svarene på spørsmålene i skjemaet gitt muntlig i møtet. Svarene ble fortløpende notert av deltakerne fra HK-dir.

Etterarbeid og tilbakemeldinger
I etterkant av møtene utarbeidet HK-dir et kartleggingsreferat som oppsummerte virksomhetenes svar. Referatene ble sendt tilbake til den enkelte virksomhet for kommentarer og kvalitetssikring. Vi mottak tilbakemeldinger – korreksjoner og utfyllende kommentarer – fra 21 virksomheter.

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

De 13 institusjonene og virksomhetene som det ble gjennomført kartleggingsmøter med i november og desember 2022, mottok sine anbefalingsbrev like før jul eller i januar 2023. De øvrige 15 virksomhetene mottok sine brev i april og mai 2023.

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

- statistikk om IT-sikkerhetshendelser i forskningsnettet fra «Cybersikkerhetssenteret for forskning og utdanning» (eduCSC) hos Sikt,
- årsrapporter fra virksomhetene for 2021,
- rapporter om arbeidet med informasjonssikkerhet og personvern behandlet i styremøter,
- risiko- eller trusselvurderinger fra nasjonale myndigheter,
- informasjon om arbeidet med informasjonssikkerhet og personvern publisert på virksomhetenes hjemmesider,
- risiko- eller trusselvurderinger fra internasjonale aktører,
- forskningslitteratur innen informasjonssikkerhet og personvern.

Metodiske begrensninger
Den primære datakilden var svarene som virksomhetene ga på spørsmålene i kartleggingsskjemaet. 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.

Det ble ikke bedt om tilgang til annen skriftlig dokumentasjon, for eksempel risikovurderinger, kontinuitetsplaner eller rutiner for sikker og lovlig behandling av personopplysninger.

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

Informasjonssikkerhets- og personverntiltak som virksomhetene opplyste om, ble ikke kontrollert eller testet. Rapporten gir derfor ikke innsikt i om iverksatte tiltak virker som forutsatt. Opplysninger om tekniske eller andre typer sårbarheter og mangler ble heller ikke undersøkt nærmere.

VEDLEGG

Vedlegg 2:

Kartleggingsskjemaet som ble benyttet

1. Hvor store ressurser (årsverk) er øremerket (helt eller delvis) til arbeidet med informasjonssikkerhet og personvern hos dere?
   - Eventuelle endringer siden fjorårets kartlegging.

2. I hvilken grad har dere tilfredsstillende oversikt over de informasjonsverdiene – data, programvare, brukerenheter, skytjenester, osv. – som dere forvalter?
   - Eventuelle data/informasjon som det er særlig viktig å beskytte/forvalte på sikker og lovlig måte.

3. Hvilke brudd på informasjonssikkerheten, inkludert personopplysningssikkerheten, og avvik fra egne sikkerhetsrutiner har dere registrert i 2022?
   - Anslagsvis antall og hovedtyper sikkerhetsbrudd eller rutineavvik.
   - Noen eksempler på mulige typer sikkerhetsbrudd og rutineavvik: løsepengevirus, direktør- eller fakturasvindel, tjenestenektangrep, brukerkontoer på avveie, informasjonstyveri, misbruk av dataressurser, brudd på rutiner/retningslinjer for tildeling eller avslutning av brukertilganger, misbruk av brukertilganger.

4. Hvilke andre typer personvernhendelser og rutineavvik (enn brudd på personopplysningssikkerheten) har dere registrert i 2022?
   - Anslagsvis antall og hovedtyper personvernhendelser eller rutineavvik.
   - Noen eksempler på typer hendelser/avvik: manglende vurdering av behandlingsgrunnlag, brudd på sletterutiner, opplysninger oppbevares lengre enn nødvendig, vanskelig å ivareta rettigheter (innsyn, retting, sletting, osv.) eller mangelfull behandlingsprotokoll.

5. Hvilke sårbarheter kan føre til brudd på informasjonssikkerheten og uønskede personvernhendelser hos dere?
   - Noen eksempler på sårbarheter: utdatert programvare, manglende rutiner for sikkerhetsoppdatering, mangelfull brukerkompetanse/bevissthet, begrensede ressurser (tid, bemanning og økonomi), uklar ansvars- eller oppgavefordeling.

6. Hvordan vil dere beskrive status for etterlevelse av personopplysningsloven/GDPR i virksomheten?
   - Nye personverntiltak/-initiativ som eventuelt ble gjennomført i 2022.
   - Om behandlingsprotokollen er relativt komplett/fullstendig.
   - Eventuelle områder i virksomheten hvor dere mener at arbeidet med etterlevelse av personopplysningsloven/GDPR bør styrkes.

7. Hvordan vil dere beskrive status for innføring og praktisering av ledelsessystemet for informasjonssikkerhet i virksomheten?
   - Eventuelle tiltak/initiativ for å styrke praktiseringen av ledelsessystemet i 2022.
   - Eventuelle endringer i status for arbeidet med informasjonssikkerhet og ledelsessystemet siden forrige kartlegging.
   - Eventuelle områder i virksomheten hvor dere mener at ledelsessystemet er mangelfullt innført og praktisert.

8. Hvordan vil dere beskrive risikostyringen innen informasjonssikkerhet. I hvilken grad ble det gjennomført risikovurderinger i 2022 og ble vurderingene fulgt opp med nødvendige sikringstiltak?

9. Hvilke initiativ/tiltak (om noen) ble gjennomført i 2022 for å oppdage og håndtere uønskede informasjonssikkerhets- og personvernhendelser?
   - Noen eksempler på ordninger eller tiltak: styrket hendelseshåndteringsteamet (IRT), rutiner for håndtering av sikkerhetshendelser/-avvik, anskaffet nytt avviksmeldingssystem, rutiner for varsling av Datatilsynet/de registrerte, sikkerhetsovervåking/-monitorering.

10. I hvilken grad har dere kriseplaner for håndtering av alvorlige informasjonssikkerhets- og personvernhendelser (beredskap og kontinuitet)? Ble det øvd på håndtering av slike hendelser i 2022?
    - Eksempler på tiltak/initiativ innen beredskap og kontinuitet: kartlagt kritiske IT-løsninger og avhengigheter, fastsatt krav til gjenopprettingstid/datatap, etablert tiltakskort for IKT-sikkerhetshendelser eller utarbeidet planer for opprettholdelse av kritiske oppgaver ved langvarige bortfall av viktige IT-løsninger.

11. Hvilke hovedtema/-problemstillinger ble diskutert på ledelsens gjennomgang i 2022?
    - Viktige initiativ/forbedringstiltak innen informasjonssikkerhet og personvern som planlegges gjennomført i 2023.
    - Styrets kontroll med virksomhetens arbeid innen informasjonssikkerhet og personvern.

Vedlegg 3:

Rammeverket som ble benyttet ved vurdering av risiko

Sannsynlighetsverdier (hendelsesfrekvens)

Svært sannsynlig:	Det forventes at hendelsen kan skje flere ganger hver måned.
Sannsynlig:	Det forventes at hendelsen kan skje hvert år.
Lite sannsynlig:	Det forventes at hendelsen kan skje sjeldnere enn hvert år, men oftere enn hvert femte år.
Svært lite sannsynlig:	Det forventes at hendelsen kan skje sjeldnere enn hvert femte år.

Konsekvensverdier (skadevirkninger)

Lite alvorlig: hendelser med ubetydelige skadevirkninger.
Eksempler på hendelser med ubetydelige skadevirkninger fordelt på utvalgte skadekategorier:

- **Personvernkrenkelser:** korte avbrudd i den registrertes tilgang til egne personopplysninger; enkelte mindre viktige opplysninger er misvisende; intern bruker har tilgang til et fåtall alminnelige opplysninger etter at behovet for tilgang har opphørt.
- **Tjenesteavbrudd:** korte perioder med ustabil tilgang til enkelte tjenester eller til mindre mengder data/opplysninger.
- **Økonomisk tap:** noe ekstraarbeid i forbindelse med hendelseshåndtering.
- **Tap av omdømme og tillit:** noe misnøye blant enkelte interne brukere med det lokale arbeidet med digitalisering, informasjonssikkerhet og personvern.
- **Skader nasjonale interesser:** N/A.

Mindre alvorlig: hendelser med en viss skadevirkning.
Eksempler på hendelser med en viss skadevirkning fordelt på utvalgte skadekategorier:

- **Personvernkrenkelser:** uautorisert eksponering av mindre mengder alminnelige personopplysninger; enkelte opplysninger mangler eller er feil; opplysningene er utilgjengelige for den registrerte opp mot fem dager.
- **Tjenesteavbrudd:** stans i levering av ikke-kritiske tjenester, eventuelt manglende tilgang til lite tidskritiske data/opplysninger, i mindre enn 24 timer.
- **Økonomisk tap:** enkeltpersoner (ansatte eller studenter) utbetaler mindre beløp til nettkriminelle som følge av direktørsvindel eller nettfiske.

- **Tap av omdømme og tillit:** misnøye blant viktige interne brukergrupper med det lokale arbeidet med digitalisering, informasjonssikkerhet og personvern.
- **Skader nasjonale interesser:** uautorisert tilgang til forskningsdata/-resultater innen områder som kan ha en viss betydning for ivaretakelse av nasjonale interesser.

Alvorlig: hendelser med merkbare skadevirkninger.
Eksempler på hendelser med merkbare skadevirkninger fordelt på utvalgte skadekategorier:
- **Personvernkrenkelser:** uautorisert eksponering av større mengder alminnelige personopplysninger; viktige opplysninger mangler eller er feil; opplysningene er utilgjengelige for den registrerte opp mot én måned.
- **Tjenesteavbrudd:** stans i levering av virksomhetskritiske tjenester eller manglende tilgang til tidskritiske data/opplysninger i 1-7 døgn, eventuelt kortere stans i levering av eller ustabil tilgang til tidskritiske tjenester (for eksempel i forbindelse med eksamensavvikling).
- **Økonomisk tap:** utbetaling av et større beløp til nettkriminelle som følge av fakturasvindel; Datatilsynet ilegger et større overtredelsesgebyr på grunn av omfattende regelavvik; mye overtidsarbeid i forbindelse med hendelseshåndtering og gjenoppretting.
- **Tap av omdømme og tillit:** oppslag i lokal-/regionalmedia som er egnet til å svekke allmennhetens tillit til den aktuelle virksomhetens arbeid med digitalisering, informasjonssikkerhet og personvern; offentlig kritikk av virksomhetens arbeid (for eksempel fra Datatilsynet eller Riksrevisjonen); kompromitterte brukerkontoer eller IoT-utstyr benyttes i dataangrep mot virksomheter i egen eller andre sektorer.
- **Skader nasjonale interesser:** uautorisert tilgang til forskningsdata/-resultater innen områder som har betydning for ivaretakelse av nasjonale interesser, eller brudd på internasjonale forpliktelser, for eksempel ulovlig kunnskapsoverføring (flerbruksteknologi).

Meget alvorlig: hendelser med betydelige skadevirkninger.
Eksempler på hendelser med betydelige skadevirkninger fordelt på utvalgte skadekategorier:
- **Personvernkrenkelser:** uautorisert eksponering av større mengder særlige kategorier personopplysninger; mange viktige opplysninger mangler eller er feil; viktige personopplysninger er utilgjengelige for den registrerte lengre enn én måned.
- **Tjenesteavbrudd:** stans i levering av virksomhetskritiske tjenester, eventuelt manglende tilgang til viktige og tidskritiske data/opplysninger, i mer enn én uke.
- **Økonomisk tap:** mye overtidsarbeid over en lang periode og innleie av ekstern assistanse i forbindelse med hendelseshåndtering og gjenoppretting; tap av viktige forskningsdata med høy gjenskaffelseskostnad; tap av uerstattelige data; gjenkjøp av store mengder IT-utstyr.
- **Tap av omdømme og tillit:** oppslag i riksmedia som i betydelig grad er egnet til å svekke allmennhetens tillit til arbeidet med digitalisering, informasjonssikkerhet og personvern i UH-sektoren; sterk offentlig kritikk av sektorens arbeid (for eksempel fra Datatilsynet eller Riksrevisjonen); uønskede hendelser i sektoren får rikspolitiske følger.
- **Skader nasjonale interesser:** uautorisert tilgang til forskningsdata/-resultater innen områder som er av særlig betydning for ivaretakelse av nasjonale interesser, eller større brudd på internasjonale forpliktelser, for eksempel ulovlig kunnskapsoverføring (flerbruksteknologi).

VEDLEGG

Risikonivåer og oppfølging

Høy risiko:

Hendelser som medfører uakseptabel risiko:

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

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

Middels risiko:

Hendelser som medfører behov for nærmere vurdering:

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

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

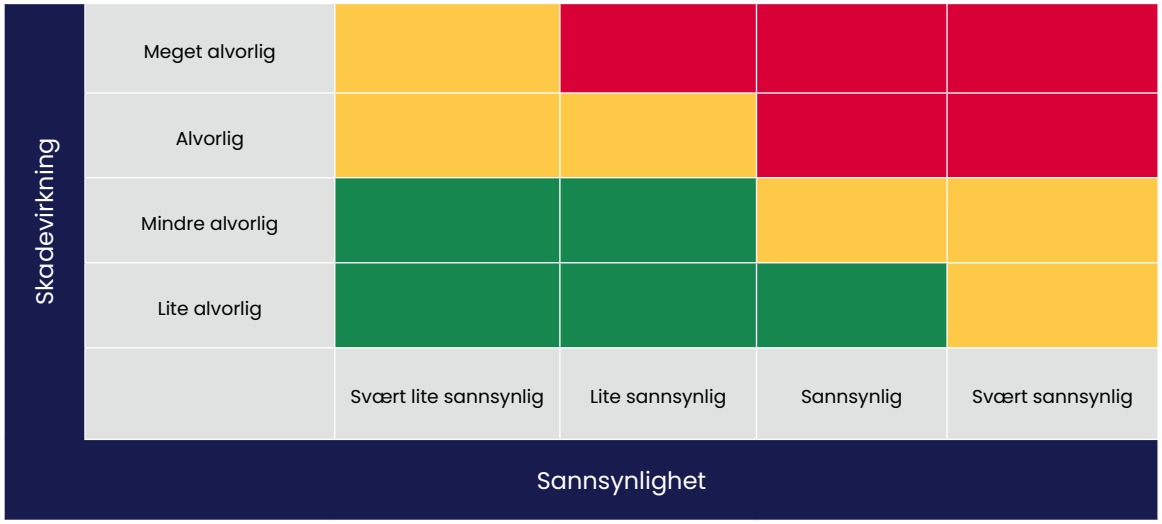
Lav risiko:

Risikoen aksepteres:

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

Oppfølging: N/A.

Risikomatrise:



Om vurdering av konsekvens

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

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

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

Rapportnummer: **4/23**
ISSN: **2703-9102**