Direktoratet for høyere utdanning og kompetanse

Risiko- og tilstandsvurdering 2024

Informasjonssikkerhet og personvern i høyere utdanning og forskning

Rapportnummer: **4/2024**
ISSN: **2703-9102**

Redaktør:
Kristin Selvaag

Forfattere:
André Gaustad (Prosjektleder)
Mathias Gullbrekken Sandnes

Grafisk utforming:
Elisabeth Guillot

Sammendrag

Denne risiko- og tilstandsrapporten presenterer resultatene fra 2023-kartleggingen av arbeidet med informasjonssikkerhet og personvern hos de 28 virksomhetene 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.

Vi vurderer også risikoen for brudd på informasjons- og personopplysningssikkerheten, det vil si uønskede hendelser som kan føre til at sektorens informasjonsverdier – opplysninger, datamaskiner og programvare – skades, ødelegges, eksponeres for uvedkommende eller er utilgjengelige.

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

Til slutt peker vi på områder hvor det er behov for å styrke arbeidet med informasjonssikkerhet og personvern i sektoren.

Arbeidet med rapporten, det vil si metodikk og datagrunnlag, gjøres rede for i vedlegg 1-2.

I det følgende oppsummeres de viktigste funnene i denne rapporten og våre anbefalinger til sektortiltak.

[1] Dette gjelder de 21 statlige universitetene og høgskolene, og følgende forvaltningsorganer og selskaper: Sikt, NFR, NOKUT, Simula, NUPI, FEK og UNIS.

Forbedringer og policyetterlevelse – viktige funn

- Antallet årsverk øremerket for arbeidet med informasjonssikkerhet og personvern økte i 2023.
- Alle de 28 virksomhetene gjennomførte flere hensiktsmessige tiltak i 2023, men det var noe lavere tiltaksaktivitet enn i 2022. Det ble iverksatt flest organisatoriske og tekniske tiltak. I sum samsvarte iverksatte tiltak bedre med de rapporterte sårbarhetene enn i foregående kartlegging.
- Tiltakene medførte at 16 av de 21 universitetene og høgskolene (institusjoner) hadde forbedret sin etterlevelse av kunnskapsdepartementets policy for informasjonssikkerhet og personvern i 2023. De fem siste institusjonene 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 av universitetene og høgskolene etterlevde de særskilte kravene til informasjonssikkerhet. De øvrige institusjonene hadde fortsatt avvik fra kravene i departementets policy.
- Det er sannsynlig eller mulig at fem nye universiteter og høgskoler vil kunne etterleve samtlige krav i policyen i løpet av 2024. Det forutsetter imidlertid at disse virksomhetene prioriterer å lukke viktige avvik fra kravene i departementets policy.
- Fem av de sju øvrige virksomhetene underlagt departementets styringsmodell (forvaltningsorganer og selskaper) etterlevde policyens særskilte krav til personvern (behandling av personopplysninger) i 2023. Tre av de sju gjorde det samme når det gjaldt kravene til informasjonssikkerhet.

Trusselbildet og risiko – viktige funn

- Institusjonene og virksomhetene rapporterte om færre brudd på informasjonssikkerheten enn tidligere år. Når det gjelder krenkelser av personvernet ble det rapportert om en økning i antall avvik og hendelser.
- Hos universitetene og høgskolene ble det rapportert om en nedgang i registrerte hendelser og brudd på informasjonssikkerheten på omkring 35 prosent sammenlignet med året før. Hos de sju øvrige virksomhetene var nedgangen på om lag 50 prosent. Ingen av hendelsene medførte alvorlige skadevirkninger.
- Nettkriminalitet (nettfiske og kompromitterte brukerkontoer), og tekniske eller menneskelige feil og uhell utgjorde flesteparten av hendelsene. Det var ingen rapporterte tilfeller av forsøk på statlig hacking (trolige forsøk på kunnskapsspionasje).
- Antallet brudd på personopplysningssikkerheten som universitetene og høgskolene meldte til Datatilsynet gikk opp i 2023. Meldte brudd gjaldt hovedsakelig små mengder personopplysninger som omhandlet et lite antall enkeltpersoner. Hos de sju øvrige virksomhetene ble det varslet om to slike brudd.
- 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 institusjoner og virksomheter hvor det behandles informasjonsverdier som er av interesse for utenlandsk etterretning; lav hos institusjoner og virksomheter i sektoren som i liten grad behandler slike verdier.
- Risikoen for brudd som følge av utilsiktede feil og uhell, og direktør og fakturasvindel, vurderes som middels.
- Risikoen for tjenestenektangrep (DDoS) vurderes som lav.

Muligheter for måloppnåelse

- Totalt åtte av institusjonene i sektoren kan oppnå målene om informasjonssikkerhet og personvern i «Strategi for digital omstilling i universitets- og høyskolesektoren, 2021-2025».
- For de øvrige universitetene og høgskolene er det noe mer usikkert om målene i strategien kan nås før strategiperiodens utløp.

Risikohåndtering – behov for sektortiltak

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 ser behov for tiltak på følgende områder:

1. Etablering og oppdatering av behandlingsprotokoll for personopplysninger i administrasjon og undervisning.
2. Etablering og vedlikehold av oversikter over andre informasjonsverdier enn personopplysninger.
3. Styrking av evnen til å oppdage og registrere informasjonssikkerhetsbrudd og -hendelser.
4. Styrke samhandling og kompetansedeling om informasjonssikkerhet og personvern mellom organisatoriske enheter hos institusjonene.
5. Periodiske dybdeundersøkelser av institusjonenes arbeid med informasjonssikkerhet og personvern.

HK-dir utarbeider også i år brev til den enkelte institusjon og virksomhet med anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern.

Innhold

Innledning 6
Policy, styringsdokument og strategi 7
Informasjonsverdier, trusler og sårbarheter 8
Risiko, etterlevelse og anbefalinger 8
Om begrensninger 9
Et bedre informasjonsgrunnlag 9
Vedlegg 10

Kapittel 1: Informasjonsverdier og digitale ressurser 11
Kort om digitalisering og verdivekst 11
Inventarkontroll – oversikt over informasjonsverdier 14
Andre informasjonsverdier enn personopplysninger 15
Oppsummering og anbefalinger 18

Kapittel 2: Universiteter og høgskoler – brudd og hendelser 20
Innledning 20
EOS-tjenestene – Statlig etterretningsvirksomhet mot UH-sektoren 21
Utsatte teknologi- og forskningsområder 22
Nettkriminelle trusselaktører 22
Endringer i trusselbildet – mindre aktivitet, mer alvorlige trusler 23
Informasjonssikkerhet – brudd og hendelser i 2023 24
Fortsatt nedgang i rapporterte hendelser og brudd 25
Varierende oppdagelsesevne 25
Typer hendelser og skadevirkninger 26
Hendelser og sårbarheter registrert hos Sikt 27
Personvern – brudd og hendelser i 2023 29
Oppsummering og behov for tiltak 31

Kapittel 3: Universiteter og høgskoler – sårbarheter, forbedringer og status 33
Innledning 33
Rapporterte sårbarheter i 2023 34
Sårbarhetsprofilen – endringer fra i fjor 35
Iverksatte tiltak i 2023 36
Andre viktige tiltak i 2023 37
Samsvar mellom sårbarhetsprofil og tiltaksaktivitet? 41
Samlet vurdering og forbehold 42
Forbedringer og status 43
Forbedringstakt 44
Status – etterlevelse av kravene til personvern (GDPR) 45
Status – etterlevelse av kravene til informasjonssikkerhet 46
Oppfølging av anbefalinger 47
Forventninger til 2024 49
Oppsummering og behov for tiltak 50

Kapittel 4: Øvrige virksomheter – forvaltningsorganer og selskaper 51
Innledning 51

Oversikt over informasjonsverdier 51
Hendelser og avvik 53
Sårbarheter 54
Sårbarheter og tiltak 57
Forbedringer og status – etterlevelse av kravene i departementets policy 58
Forbedringer i arbeidet med informasjonssikkerhet og personvern 2023 61
Forventninger til 2024 62
Oppsummering og anbefalinger 63

Kapittel 5: Risiko, mål og anbefalinger 64
Innledning 64
Bakgrunnen for vurdering av risiko 64
Rammeverket for vurdering av risiko 65
Risiko i sektoren 66
Risikoscenarier og risikonivå 67
Risikomatrisen 70
Muligheter for måloppnåelse 71
Vurdering av måloppnåelse 71
Risikohåndtering – behov for sektortiltak 72

Vedlegg 1: Datagrunnlaget og arbeidet med rapporten 74

Vedlegg 2: Kartleggingsskjemaet som ble benyttet 76

Vedlegg 3: Rammeverket som ble benyttet ved vurdering av risiko 78

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 2023.

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 de 28 universiteter, høgskoler og øvrige virksomheter som omfattes av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[2]

Dernest å vurdere følgende forhold:

- etterlevelsen i sektoren av kravene i departementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning»,[3]
- 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.

Til slutt viser vi behov for tiltak på sektornivå som kan bidra til å styrke arbeidet med informasjonssikkerhet og personvern hos de 28 virksomhetene.

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.

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. 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 et virkemiddel for å ivareta personvernet når det behandles opplysninger om den enkelte, men er også nyttig for andre formål. Eksempler på andre formål inkluderer effektiv forvaltning, forsvarlig saksbehandling, tilfredsstillende økonomistyring og beskyttelse av offentlige eller kommersielle interesser.

[2] 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 22.03.2024.
[3] Policyen er fastsatt av Kunnskapsdepartementet i rundskriv F-04-20, og er gjort gjeldende fra 1. oktober 2020.

Policy, styringsdokument og strategi

Kravene til informasjonssikkerhet og personvern i sektoren fremgår av «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».[4] 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».[5]

Videre inneholder «Strategi for digital omstilling i universitets- og høgskolesektoren, 2021-2025» enkelte målformuleringer gjeldende informasjonssikkerhet og personvern.[6] Her fremheves informasjonssikkerhet og personvern som forutsetninger for arbeidet med digital omstilling.

Departementets policy for informasjonssikkerhet og personvern operasjonaliserer hva som kreves for at målene i strategien skal kunne nås.

[4] 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 22.03.2024.
[5] 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 22.03.2024.
[6] Se https://www.regjeringen.no/no/dokumenter/strategi-for-digital-omstilling-i-universitets-og-hoyskolesektoren/id2870981/. Sist besøkt 22.03.2024.

Informasjonsverdier, trusler og sårbarheter

Drøftelsene i denne rapporten av viktige funn og konklusjoner fra årets kartlegging, 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 som anvendes 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 institusjonene og 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 skal forebygge, oppdage og håndtere. Eksempler på trusler er nettkriminelle grupper og statlige hackere som opererer på internettet.

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 som kan føre til brudd på informasjonssikkerheten og personvernet – 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 hendelser som kan føre til 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 strategien 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 inneholder nærmere beskrivelser av arbeidet med informasjonssikkerhet og personvern. Det er heller ikke gjennomført kontroller eller tester av rapporterte initiativ og forbedringstiltak. Kvalitetssikring av det lokale arbeidet med informasjonssikkerhet og personvern – og iverksatte forbedringstiltak – må skje gjennom sikkerhetstester og etterlevelsesrevisjoner.

Hensikten med undersøkelsen har vært å kartlegge:

- systematikken i arbeidet med informasjonssikkerhet og personvern hos den enkelte virksomhet,
- trusler og sårbarheter som påvirker sektorens evne til å ivareta informasjonssikkerheten og personvernet, og
- viktige endringer og forbedringstiltak som er iverksatt for å utbedre sårbarhetene og håndtere truslene.

Et bedre informasjonsgrunnlag

Nytt av året er at årets tilstands- og risikorapport har et bedre informasjonsgrunnlag enn tidligere utgaver. Dette skyldes til dels at HK-dir oppsummerte utviklingen fra 2018 til 2022 i UH-sektorens arbeid med informasjonssikkerhet og personvern i en egen temarapport i januar 2024.[7] Temarapporten har styrket muligheten for sammenligning av funn, vurderinger, og utvikling i arbeidet med informasjonssikkerhet og personvern i UH-sektoren over flere år. Informasjonsgrunnlaget er videre styrket av funn i HK-dir sin kartlegging av UH-sektorens arbeid med digital omstilling, spesielt funn om sektorens kapasitet og ressurser har vært viktige i våre vurderinger.[8]

Den viktigste endringen er imidlertid at Riksrevisjonen i januar 2024 publiserte sin rapport om informasjonssikkerhet i forskning innenfor kunnskapssektoren.[9] Revisjonen av 10 forskningsinstitusjoner har gitt HK-dir ny og viktig informasjon om sektorens arbeid med informasjonssikkerhet og personvern.

Funnene fra rapportene benyttes i våre vurderinger av de underlagte virksomhetenes muligheter for måloppnåelse i kapittel 3 og 4, og risikovurderingene våre i kapittel 5.

[7] Rapporten «Informasjonssikkerhet og personvern i et femårsperspektiv» er tilgjengelig på: HK-dir | HK-dir (hkdir.no), sist besøkt 23.05.2024.
[8] Rapporten om digital omstilling i UH-sektoren er tilgjengelig på: HK-dir | HK-dir (hkdir.no), sist besøkt 16.05.2024.
[9] Riksrevisjonens rapport er tilgjengelig på: Sensitive forskningsdata kan komme på avveie (riksrevisjonen.no), sist besøkt 22.05.2024.

Om Riksrevisjonens rapport

Riksrevisjonen gjennomførte i perioden 2022-2023 omfattende undersøkelser hos åtte universiteter og høgskoler, og to andre virksomheter underlagt departementet.[10] Disse ble utvalgt fordi de har et stort omfang av viktige og sensitive forskningsdata, i tillegg til at Riksrevisjonen vektla variasjon i utvalget etter kriterier som størrelse og faglig profil.

Alle de 10 forskningsinstitusjonene ble undersøkt på de samme områdene gjennom dokumentstudier, tekniske utdrag fra IT-systemer, og intervjuer. Hos tre institusjoner ble det gjennomført dybdeundersøkelser med mer omfattende intervjuer, utdrag fra IT-systemer, og penetrasjonstester.

Det ble funnet alvorlige tekniske sikkerhetshull og sårbarheter hos alle de reviderte virksomhetene. I tillegg ble det pekt på en rekke organisatoriske svakheter, spesielt i gjennomføringen av det praktiske arbeidet med informasjonssikkerhet. Riksrevisjonens overordnede vurdering var at:

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

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.

[10] Disse var Nord, NIH, NTNU, NUPI, UiB, UiO, UiS, USN, UiT, og UNIS. Offentlig versjon av rapporten er tilgjengelig på Dokument 3:11 (2023–2024) (riksrevisjonen.no). Sist besøkt 26.03.2024.

Kapittel 1: Informasjonsverdier og digitale ressurser

Hensikten med å etterleve kravene i departementets policy om informasjonssikkerhet og personvern er å sikre viktige informasjonsverdier, og sikre forsvarlig og lovlig håndtering av personopplysninger. For å kunne etterleve kravene, må virksomhetene som omfattes av styringsmodellen vite hvilke informasjonsverdier policyen omfatter.

Virksomhetene som er underlagt departementets styringsmodell forvalter viktige informasjonsverdier som forskningsdata og personopplysninger ved bruk av datamaskiner, programvare og nettverksutstyr. Sektorens evne til å utføre sine kjerneoppgaver kan skades dersom disse verdiene ødelegges, mistes, eksponeres for uvedkommende, eller håndteres på ulovlig vis.

Også enkeltpersoner og tredjeparter kan henholdsvis få sine personopplysninger misbrukt, og informasjonsverdier kompromitterte dersom UH-sektoren ikke lykkes med å tilstrekkelig sikre sine IT-systemer og tjenester.

I dette kapittelet ser vi nærmere på de informasjonsverdiene som arbeidet med informasjonssikkerhet og personvern har til hensikt å ivareta. Formålet med kapitlet er todelt:

(i) å gi en skjematisk oversikt over «verdilandskapet» hos de statlige universitetene og høgskolene

(ii) 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 4.

Nedenfor følger først en 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 de informasjonsverdiene som digitaliseringen både endrer og skaper. Vi ser også på institusjonenes arbeid med oversikt over informasjonsverdier (kunnskap) som omfattes av regler om internasjonal kunnskapsoverføring og eksportkontroll.

Kort om digitalisering og verdivekst

I tidligere risiko- og tilstandsvurderinger har vi fremhevet at verdivekst og økt tempo i digitaliseringen medfører et større omfang av informasjonsverdier som skal sikres. I tillegg har vi pekt på at virksomhetene i sektoren blir stadig mer avhengig av digital teknologi for å utføre sine kjerneoppgaver.

Økt omfang av verdier og avhengighet til digital teknologi gjør at konsekvensene av informasjonssikkerhetshendelser mot sektorens digitale systemer og løsninger kan bli mer omfattende enn tidligere. HK-dir sin kartlegging av arbeidet med digital omstilling hos institusjonene viser at denne utviklingen har fortsatt i 2023.[11]

Kartleggingen av digital omstilling viser at institusjonene har en «tradisjonell tilnærming til digitalisering» – de satset på nye digitale verktøy for blant annet videoundervisning, digitale vurderingsformer, og digitale læringsverktøy. Verktøy-tilveksten var tydeligst på administrasjons- og undervisningssiden, men det var også et

[11] Rapporten «Digital omstilling i UH-sektoren status, muligheter og utfordringer 2023» er tilgjengelig på HK-dir | HK-dir (hkdir.no). Sist besøkt 04.03.2024.

betydelig aktivitetsnivå innen forskning og tilgang på forskningsdata. Ved innføring av nye digitale verktøy øker kompleksiteten i å holde oversikt over egne informasjonsverdier.

Videre fant kartleggingen at mange av institusjonenes tiltak innen digitalisering dreide seg om innføring av administrative fellesløsninger i sektoren, og organisatoriske endringer for å kunne ta imot de samme løsningene.[12] De seks institusjonene som ble intervjuet i kartleggingen problematiserte at flere tjenester vil kreve innføring i egen organisasjon samtidig, og at det samlede ressurskravet til mottakerne er for omfattende.

I tillegg ble institusjonene bedt om å vurdere i hvilken grad aktiviteter innen utdanning, forskning, formidling, og administrasjon gjennomføres på en måte som ivaretar hensynet til informasjonssikkerhet og personvern. Én institusjon svarte «i svært stor grad», 17 «i ganske stor grad» og tre «i hverken stor eller liten grad». Det påpekes i rapporten at dette sannsynligvis er en noe positiv fremstilling av status for arbeidet med informasjonssikkerhet og personvern. Samtidig indikerer svarene fra institusjonene at det er generelt høy bevissthet om arbeidet med informasjonssikkerhet og personvern i sektoren.

Kartleggingen av digital omstilling viser for det første at verdilandskapet blir mer omfattende og komplekst enn tidligere. For det andre viser kartleggingen at kapasiteten og ressursene til å drifte, vedlikeholde, og dermed sikre digitale systemer er under press i sektoren. Denne kombinasjonen kan bidra til å redusere fremgangen i institusjonenes arbeid med å etterleve kravene i departementets policy. Det er derfor positivt at resultatene fra spørsmålet om informasjonssikkerhet og personvern i kartleggingen indikerer at institusjonene har disse forvaltningsområdene høyt på agendaen.

[12] Se for eksempel Nasjonalt vitenarkiv (NVA) (sikt.no). Sist besøkt 08.03.2024.

«Verdilandskapet» – hovedtyper informasjonsverdier

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

1. **Studieadministrasjon**. Informasjon som typisk behandles i studieadministrative 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 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 vil typisk ha betydning for departementets krav til rapportering.

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

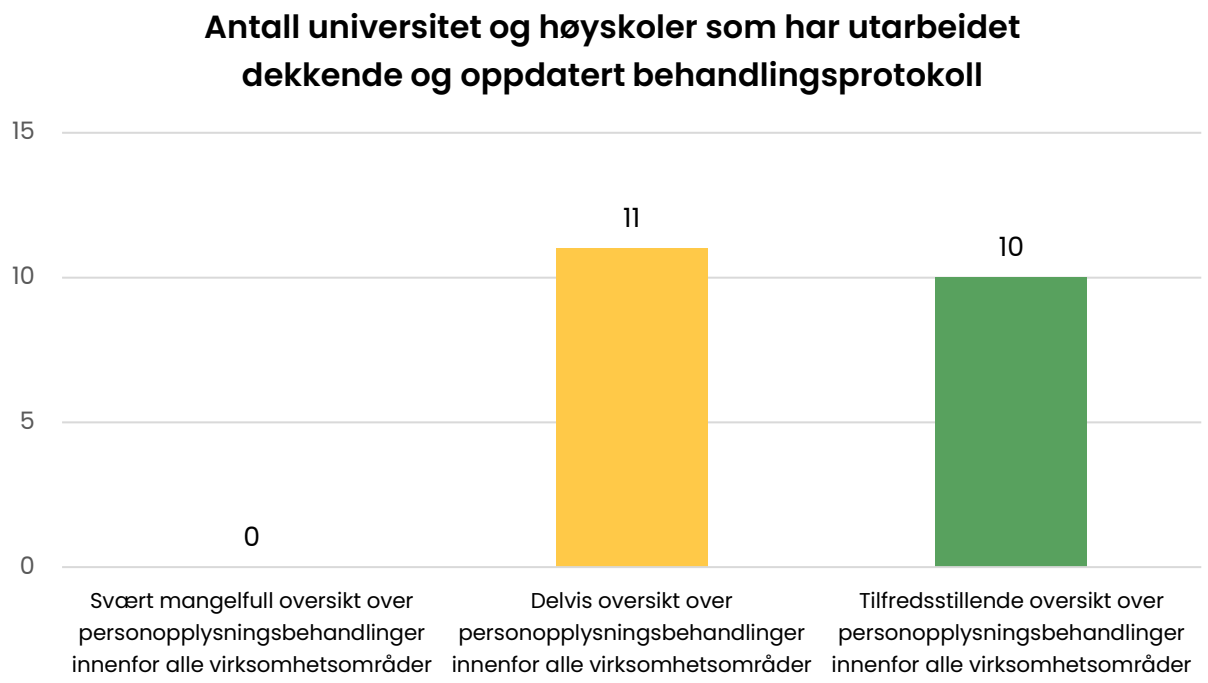
Inventarkontroll – oversikt over informasjonsverdier

Institusjonene ble spurt i møte med HK-dir om de har utarbeidet dekkende og oppdaterte oversikter over sine informasjonsverdier som omfattes av departementets policy. Vi la vekt på om de hadde oversikt over hvilke personopplysninger de behandler, men vi spurte også om oversikter over andre typer informasjonsverdier. Eksempler på andre informasjonsverdier er datamaskiner, programvare, og forskningsdata som institusjonene er pålagt å beskytte i henhold til departementets policy.

Behandlingsprotokoll for personopplysninger – 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.[13]

Figur 1 viser hvor mange universiteter og høgskoler som i 2023 oppga at de hadde utarbeidet en dekkende og oppdatert behandlingsprotokoll – og hvor mange som mente at de ikke hadde det.



Figur 1 - Status for behandlingsprotokoll 2023, universiteter og høgskoler

Figuren viser at 10 av de 21 universitetene og høgskolene opplyste om at behandlingsprotokollen var fullstendig og oppdatert. Dette er samme status som i 2022, og det var de samme institusjonene som hadde tilfredsstillende oversikt begge årene.

[13] 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 05.03.2024.

Det betyr at også i 2023 var det 11 universiteter og høgskoler som mente at behandlingsprotokollen ikke var dekkende innenfor alle virksomhetsområder, eller at den ikke var oppdatert. Manglende oppdatering innebar at oversikten i protokollen ikke hadde holdt tritt med institusjonenes digitalisering.

Det er fortsatt de mindre institusjonene som dominerer utvalget som oppga at de hadde en fullstendig og oppdatert behandlingsprotokoll. Dette kan ha sammenheng med at de største institusjonene har en større utfordring enn de mindre med å følge opp protokollføring hos et stort antall fakulteter, institutter, forskningssentre, og støttemiljøer.

Sikts personverntjenester og andre protokolløsninger

Hos alle universitetene og høgskolene var det etablert en egen behandlingsprotokoll for forskning. Denne protokollen ble ført gjennom meldeskjema for personopplysninger hos Sikts personverntjenester for forskning.[14] I institusjonsportalenen får universitetene og høgskolene oversikt over behandlinger av personopplysninger i forsknings- og studentprosjekter som er registrert via meldeskjema for personopplysninger. Prosjektene følges også opp av Sikt underveis i registeringen og ved prosjektslutt, spesielt at opplysninger enten er anonymisert eller slettet.

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

Innenfor de øvrige virksomhetsområdene, spesielt undervisning og administrasjon, tilbys det ikke en tilsvarende fellestjeneste som den levert av Sikt sine personverntjenester. Institusjonene må derfor finne sine egne protokolløsninger, vanligvis i form av excel-ark eller kommersielt tilgjengelige protokollverktøy.

Andre informasjonsverdier enn personopplysninger

I forsknings- og utviklingsaktiviteter behandler universitetene og høgskolene en rekke andre informasjonsverdier enn personopplysninger. Eksempler på slike verdier er forskning om nanoteknologi, kryptografi, romfart og satellitteknologi, undervannsteknologi, osv., men også blant annet vær- og klimadata, maritime data og geologiske data.

Som vi kommer tilbake til i kapittel 2, er enkelte teknologi- og forskningsområder viktige å beskytte av hensyn til eksportkontrollregelverket og internasjonale sanksjoner. I våre årlige kartlegginger har vi, blant annet på grunn av slike hensyn, vært opptatt av om institusjonene har oversikt over informasjonsverdier i forskning og utvikling som ikke er personopplysninger.

Kartlegging og klassifisering av andre informasjonsverdier

Utviklingen på dette området i 2023 er i stor grad en fortsettelse av de påbegynte prosessene som ble rapportert om i forrige kartlegging: I 2022 hadde åtte institusjoner gjennomført eller var i ferd med å gjennomføre kartlegginger av sine informasjonsverdier. Flere av prosjektene inkluderte personopplysninger, for eksempel tiltak rettet mot behandlingsprotokoll for personopplysninger. Likevel opplyste samtlige institusjoner om at kartleggingsprosjektene også omfattet andre informasjonsverdier som forskningsdata eller utstyr og systemer som benyttes til forskning.

[14] Vi har tidligere omtalt meldeskjema for personopplysninger og institusjonsprotalen som «meldingsarkivet». Institusjonsportalen, meldeskjema, og øvrige personverntjenester som Sikt tilbyr, er tilgjengelig her: https://sikt.no/tjenester/personverntjenester-forskning. Sist besøkt 07.03.2024.

I 2023 hadde 10 institusjoner startet eller gjennomført slike verdikartlegginger av informasjonsverdier. Fem institusjoner opplyste om kartlegginger av informasjonsverdier som er underlagt eksportkontrollforskriften og sikkerhetsloven. I tillegg hadde syv institusjoner lagt planer for å starte opp nye kartlegginger av informasjonsverdier i 2024.

De øvrige fem institusjonene opplyste ikke om planer om å starte opp, eller gjennomførte verdikartlegginger i 2023. Disse institusjonene arbeidet med å gjennomføre anbefalinger fra gjennomførte revisjoner, eller tidligere kartlegginger av informasjonsverdier.

Når det gjelder hvordan universitetene og høgskolene klassifiserer sine informasjonsverdier med hensyn til viktighet eller kritikalitet, påvirkes dette av om informasjonsverdiene er omfattet av juridiske krav til håndtering og sikring. Det er opp til den enkelte institusjon å vurdere viktigheten av andre typer informasjonsverdier enn de som er undergitt rettslig regulering. Det er vanlig at slike vurderinger skjer på en relativt ensartet måte, det vil si med utgangspunkt i et felles rammeverk for verdiklassifisering.[15]

Fra kartleggingen i 2023 har vi inntrykk av at vurderinger av viktighet (kritikalitet) for andre informasjonsverdier enn personopplysninger kan variere noe mellom institusjoner. Dette er samme inntrykk vi hadde etter kartleggingen i 2022. Flere av institusjonene rapporterte imidlertid om forbedringer i lagrings- og klassifiseringsguider, bevissthet om krav til sikring av informasjon blant ansatte og studenter, og økt bruk av tjenester som tilbyr sikre soner for sensitive data.

[15] Det vanligste klassifiseringsrammeverket blant institusjonene er varianter av Uninetts fagspesifikasjon (UFS) 136. Sikt sendte i desember 2023 ut «Sektorstandard for klassifisering av informasjon» som bygger videre på UFS. Sektorstandarden er tilgjengelig på Sektorstandard_klassifisering_av_informasjon (1).pdf (sikt.no). Sist besøkt 07.03.2024.

Maskinlæring og språkmodeller

Som en del av årets kartlegging ble institusjonene og virksomhetene spurt om hvilke konsekvenser KI-utbredelsen hadde hatt i deres organisasjon.

Svarene viser at sektoren har en rekke ulike KI-tjenester i bruk, og det var 13 av institusjonene og virksomhetene som oppga å ha etablert et tilbud om tilgang til språkmodeller i deres organisasjon. Ytterligere fire oppga å være i en utprøvingsfase. Blant språkmodellene var "Bing Chat Enterprise" den mest utbredte.

Ved 16 av institusjonene og virksomhetene var det iverksatt aktiviteter knyttet til KI-kompetanse. Blant annet ble det publisert informasjon på nettsider, opplæringsaktiviteter, etablert ulike former for arbeids- og ressursgrupper, og flere institusjoner oppga å ha samarbeid med andre virksomheter.

Videre var det 16 institusjoner og virksomheter som enten hadde etablert retningslinjer, eller var i ferd med å etablere slike. I møtene med HK-dir var flere institusjoner opptatt av eksamensreglementet. I denne sammenhengen ble det reist bekymringer for personvernet og mangel på databehandleravtaler med leverandører av språkmodellene. Enkelte av institusjonene hadde tydelige krav om hvilke data som kunne benyttes i språkmodellene, og koblet dette opp mot eksisterende reglement for lagring og klassifisering av data.

Når det gjaldt behov for overordnede retningslinjer eller avklaringer på sektornivå, uttrykte 15 av institusjonene og virksomhetene behov for felles regelverk eller retningslinjer i sektoren. Eksempelvis gjaldt dette felles avklaringer om databruk og retningslinjer for sikker bruk.

Inventarkontroll – datamaskiner, programvare og IT-tjenester

Kartleggingene av institusjonenes informasjonsverdier skal lede til forbedret inventarkontroll – bedre oversikt over datamaskiner og programvare på eget datanettverk, og hvilke IT-tjenester som brukes av medarbeidere og studenter.

I 2023 rapporterte alle institusjonene om forbedringer i sin inventarkontroll med tanke på digitale ressurser og utstyr. Inventarkontrollen var hovedsakelig ivaretatt av IT-avdelingene i sektoren, typisk i form av system- og tjenesteregister, programvarekataloger, og register over sluttbrukerutstyr som datamaskiner og mobiltelefoner. Samtidig pekte alle institusjonene på varierende forbedringspotensial i sine oversikter over informasjonsverdier, som blant annet behovet for de overnevnte kartleggingene.

Det ble også i 2023 rapportert om utfordringer knyttet til «skygge-IT». Dette er IT-tjenester som ansatte og/eller studenter tar i bruk uten formell godkjenning, og uten at institusjonen er kjent med bruken. For eksempel kan bruken av skygge-IT gjøre det vanskeligere å oppdage og utbedre avvik fra institusjonenes rutiner for behandlinger av personopplysninger.

Institusjonene som rapporterte om utfordringene knyttet til «skygge-IT», hadde iverksatt tiltak for å redusere omfanget i 2023. Tiltakene besto blant annet av regelverkinnstramminger om hvilke skytjenester og utstyr som studenter og ansatte kan bruke, applikasjonsregistre, og informasjon om retningslinjer for bruk og oppsett av egne IT-systemer.

Trenden fra 2022 ser derfor ut til å ha fortsatt i 2023 – problematikken med bruk av «skygge-IT» fremsto som noe redusert sammenliknet med hva som tidligere har blitt rapportert.

Internasjonal kunnskapsoverføring og eksportkontroll

Institusjonene skal ha oversikter over forskningsdata på enhetsnivå (fakulteter, institutter, osv.) som omfattes av regler for internasjonal kunnskapsoverføring – eksportkontroll. Regelverket innebærer at institusjonene må søke Utenriksdepartementet om lisens for overføring av kunnskap som har eller kan brukes til militære formål.[16] Dette skal sikre at internasjonal kunnskapsoverføring skjer i tråd med norske sikkerhets- og forsvarsinteresser, og ivaretar Norges internasjonale forpliktelser.[17]

I 2022 rapporterte ni institusjoner om at de hadde gjennomført tiltak eller kartlegginger for å få oversikt over forskningsdata som omfattes av reglene om internasjonal kunnskapsoverføring. Som nevnt ovenfor, hadde fem institusjoner fortsatt med kartlegging av slike verdier i 2023.

Vårt hovedinntrykk er derfor at arbeidet med eksportkontroll har styrket seg noe i 2023 i forhold til 2022.

Oppsummering og anbefalinger

En forutsetning 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 universitets- og høgskoledelen av sektoren har enkelte mangler når det gjelder oversikt over sine informasjonsverdier. Det skyldes i noen grad verdivekst i form av økt digitalisering, men også at ressursene til å forvalte og sikre verdiene er under press i sektoren.

Registreringen av personopplysninger i forskning virker å være institusjonalisert på et tilfredsstillende nivå i sektoren ved bruk av Sikts personverntjenester. Behandlingsprotokoll for personopplysninger i administrasjon og undervisning ser fortsatt ut til være utfordrende for om lag halvparten av institusjonene.

Likevel er det grunn til å anta at sektoren er på riktig kurs i arbeidet med å etablere tilfredsstillende oversikt over egne informasjonsverdier. Funnene fra kartleggingen av digital omstilling viser at informasjonssikkerhet og personvern er et prioritert forvaltningsområde for institusjonene.

---

[16] Se «Retningslinjer for kontroll med kunnskapsoverføring» (UD). https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/. Sist besøkt 08.03.2024.

[17] 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 08.03.2024. Jf. også «Panorama 2021-2027», side 12. https://www.regjeringen.no/contentassets/13e7862e6c064321af97fe0c58a8f7cb/f-4462-b_panorama_strategi.pdf. Sist besøkt 22.03.2024. 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 Retningslinjer for ansvarlig internasjonalt samarbeid | HK-dir (hkdir.no). Sist besøkt 22.03.2023.

Dette inntrykket er videre forsterket av at flere institusjoner i 2023 prioriterte kartlegging av andre informasjonsverdier enn personopplysninger, eller oppfølging av tidligere kartlegginger med tiltak. I tillegg har institusjonene fortsatt å forbedre sitt arbeid med å redusere bruken av skygge-IT.

Med bakgrunn i funnene diskutert i dette kapitlet, mener vi at sektoren har behov for tiltak spesielt på to områder:

(i) Etablering og oppdatering av behandlingsprotokoll for personopplysninger i administrasjon og undervisning. 11 av 21 institusjoner har fortsatt viktige avvik fra departementets policy på dette området.

(ii) Etablering og vedlikehold av oversikter over andre informasjonsverdier enn personopplysninger. Institusjoner som har informasjonsverdier underlagt eksportkontroll har særlig behov for å prioritere arbeidet med oversikt og sikring av disse informasjonsverdiene.

Institusjonene rapporterer i hovedsak om praktiske utfordringer med å føre og oppdatere behandlingsprotokoller for personopplysninger i administrasjon og undervisning. I forskningsdelen av virksomhetene er disse problemstillingene langt mindre sentrale, og virker å være institusjonalisert. Hovedforskjellen mellom disse områdene er at det finnes et sektortilbud for behandling av personopplysninger i forskning som benyttes av nesten alle institusjonene gjennom Sikts personverntjenester.

Vi mener derfor at et tilsvarende tilbud eller tjeneste for behandlinger av personopplysninger i administrasjon og undervisning vil kunne styrke arbeidet med føring av behandlingsprotokoll hos de 11 institusjonene som har mangler på dette området.

Når det gjelder verdioversikter, er vårt inntrykk at institusjonene også her mangler arbeidsverktøy som er tilpasset utdanningssektoren for å lage og vedlikeholde verdioversikter. Selv om også dette behovet kan løses ved en fellestjeneste levert av Sikt, mener vi at det er mer hensiktsmessig at institusjonene selv finner løsninger for verdioversikter som er tilpasset deres egen virksomhet.

Vi legger vekt på at institusjonene rapporterte om at mottakskapasiteten for fellesløsninger er under press i tilstandskartleggingen av digital omstilling i vår vurdering. I tillegg registrerer vi at det er ulike behov for slike oversikter i sektoren, og at det derfor vil være mer utfordrende å lage en fellestjeneste som kan møte de ulike behovene blant høgskolene og universitetene.

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 2023? 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.

Definisjoner – brudd og hendelser

Med **brudd** menes at informasjonsverdier faktisk ble utsatt for uautorisert tilgang, skade, ødeleggelse, endring, sletting eller ble utilgjengelige. 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 det har vært fare for uautorisert tilgang, skade, ødeleggelse, endring, sletting eller utilgjengelighet, men hvor dette likevel ikke har skjedd. Forsøk på datainntrenging eller dataangrep er eksempler på hendelser. Hendelser omfatter også ulovlig behandling av personopplysninger eller behandlinger i strid med interne rutiner, men hvor det ikke ble rapportert om krenkelser av personvernet.

Brudd og hendelser kan forårsakes av utilsiktede og tilsiktede handlinger. Når det gjelder tilsiktede brudd på informasjonssikkerheten (inkludert personopplysningssikkerheten) kan det dreie seg om sikkerhetstruende handlinger fra nettkriminelle grupper og statlige hackere (APT[18]). De utilsiktede bruddene på informasjonssikkerheten eller krenkelser av personvernet kan skyldes tekniske eller menneskelige feil og uhell.

I det følgende gis først en kort oversikt over trusselbildet mot UH-sektoren, hovedsakelig med grunnlag i 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 2023, og endringer sammenliknet med 2022.

Til slutt gis en oversikt over personvernbrudd og -hendelser og avvik som universitetene og høgskolene rapporterte om.

[18] 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, with potentially destructive consequences". https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. Sist besøkt 05.03.2024. Det kan for eksempel dreie seg om statlige eller statsstøttede hackergrupper, men også om nettkriminelle grupper. 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.

EOS-tjenestene – Statlig etterretningsvirksomhet mot UH-sektoren

EOS-tjenestene har over flere år vurdert statlig etterretningsvirksomhet som en viktig trussel mot norske interesser og virksomheter, inkludert virksomheter i UH-sektoren.[19] Dette budskapet forsterkes i tjenestenes vurderinger for 2024 med bakgrunn i den pågående krigen i Ukraina, men også eskalering av konflikter i Midtøsten. Russland og Kina er også i 2024 de viktigste landene som vil gjennomføre etterretningsaktivitet mot Norge. I tillegg forventes det at land som Iran og Nord-Korea vil gjennomføre cyberoperasjoner mot norske virksomheter.

Russland vil særlig ha behov for vestlig teknologi, kunnskap, og kompetanse med sivil og militær nytteverdi for å understøtte sin krigføring i Ukraina. Norske forsknings- og utdanningsinstitusjoner med relevante forskningsverdier er derfor fortsatt i målbildet for russiske etterretningstjenester. Nordområdene står ifølge E-tjenesten i en særstilling for Russland, men er også i økende grad interessant for Kina.[20] PST forventer at etterretningstrusselen fra Kina vil tilta i de kommende årene.[21]

EOS-tjenestene mener at disse landene vil kunne benytte seg av cyberoperasjoner, innsidevirksomhet, påvirkningsoperasjoner, forsøke å plante illegalister[22], og rekruttering av norske borgere for å nå sine etterretningsmål. Trusselaktørene vil utnytte både kjente og nye sårbarheter, og tilpasser sine fremgangsmåter etter hvor de antar målene deres er sårbare. For eksempel har NSM merket seg at økt bruk av mobiltelefon til databehandling har medført flere tilfeller av målrettet nettfiske (spear phishing)[23] rettet mot ansatte i forskning og forsvarsindustrien i 2023.[24]

Ifølge PST, er forsknings- og utdanningssektoren blant hovedmålene for cyberoperasjoner fra fremmede stater. Hovedhensikten med cyberoperasjonene er fortsatt informasjonsinnhenting, men de blir også i økende grad brukt for å skape usikkerhet i samfunnet, for eksempel gjennom tjenestenektangrep (DDoS).[25]

Samtidig har cyberdomenet utviklet seg som rekrutteringsarena for fremmede lands etterretningstjenester, ifølge PST. [26] I 2023 har digital rekrutering av norske borgere til tjeneste for fremmede lands etterretningstjenester skjedd i større grad enn tidligere. Denne trusselen er relevant for UH-institusjoner med studenter eller forskere fra land med autoritære regimer.[27]

Videre opplyser PST om at cyber-trusselen er økende som følge av stadig tettere samarbeid mellom statlige og kriminelle aktører. Samarbeidet gjør at stater som selv ikke har kapasitet og kompetanse til å gjennomføre cyberoperasjoner, kan anskaffe dette gjennom kriminelle aktører. I tillegg har Iran og Nord-Korea økt sin kapasitet

---

[19] Vi sikter til de nasjonale risiko- og trusselvurderingene fra NSM, PST, og E-tjenesten. Rapportene for 2024 er tilgjengelige på henholdsvis: Risiko 2024.pdf (nsm.no), Nasjonal trusselvurdering 2024 (pst.no), Fokus 2024 (etterretningstjenesten.no). Sist besøkt 23.05.2024.
[20] Se «Fokus 2024», side 13.
[21] Se «Nasjonal trusselvurdering 2024», side 5-6. Rapporten er tilgjengelig på Nasjonal trusselvurdering 2024 (pst.no). Sist besøkt 23.05.2024.
[22] PST definerer en illegalist som «en person som framstår som en vanlig borger, mens vedkommende egentlig jobber for utenlandsk etterretning». Se Spion-ekspert: Illegalister vil knytte så nære bånd til kollegaer som mulig (khrono.no), sist besøkt 16.05.2024.
[23] Datatilsynet beskriver målrettet nettfiske (spear phishing) som «er gjerne rettet mot en konkret virksomhet, eller enkeltpersoner i virksomheten […], Disse phishing-forsøkene kan være sofistikerte og vanskelig å oppdage». Se Phishing - hvordan beskytte virksomheten | Datatilsynet, sist besøkt 16.05.2024.
[24] Se «Risiko 2024», side 14.
[25] Se «Nasjonal trusselvurdering 2024», side 16-19.
[26] Se «Nasjonal trusselvurdering 2024», side 20.
[27] Se «Nasjonal trusselvurdering 2024», side 26.

til å gjennomføre cyberoperasjoner de siste årene. Denne utviklingen gjør cyber-trusselen fra statlige trusselaktører mer uforutsigbar enn tidligere.

Utsatte teknologi- og forskningsområder

EOS-tjenestene peker også i årets risiko- og trusselvurderinger på en rekke teknologi og forskningsområder som er av særlig interesse for stater som Kina og Russland. Sistnevnte er som følge av sanksjoner spesielt avskåret og isolert fra de tradisjonelle anskaffelsesmetodene av teknologi og kunnskap. UH-sektorens informasjonsverdier kan imidlertid fortsatt være tilgjengelig gjennom studentutveksling og forskningssamarbeid for Kina. PST peker på at utenlandske forskere inviteres til talentprogrammer og forskningsparker i Kina med formål om å utnytte deres kompetanse til å styrke egen militær kapasitet.[28]

Tabellen nedenfor viser hvilke fremvoksende teknologier og forskningsområder som PST opplyser om at er av særlig interesse for fremmede stater i sin åpne trusselvurdering for 2024. Institusjoner og virksomheter i UH-sektoren med informasjonsverdier innen disse forsknings- og teknologiområdene kan derfor være attraktive mål for etterretningsoperasjoner fra statlige trusselaktører.

Fremvoksende teknologier

- Kunstig intelligens
- Maritim autonomi
- Bioteknologi
- Kvantedatamaskiner

Forskningsområder av særlig interesse for fremmede stater

- Nanoteknologi
- Metallurgi
- Kryptografi
- Robotikk og autonomi
- Kjemi
- Mikroelektroniske systemer
- Akustikk
- Kjernefysikk og cybersikkerhet

Nettkriminelle trusselaktører

Vi har tidligere anslått at ca. 80 prosent av rapporterte informasjonssikkerhetshendelser i UH-sektoren i perioden 2018-2022 ble utført av nettkriminelle trusselaktører.[29] Nettkriminelle grupper er derfor en sentral trussel mot UH-sektorens verdier.

Nettkriminelle aktører har typisk økonomisk gevinst som motivasjon for sine forsøk på datainnbrudd, og skiller seg slik fra de statlige aktørene som antas å primært være ute etter kunnskap, for eksempel forskningsdata. Samtidig kan målsetningene være flere for enkelte cyberangrep, blant annet fordi nettkriminelle kan samarbeide med statlige trusselaktører.

[28] Se «Nasjonal trusselvurdering 2024», side 24.
[29] Se «Informasjonssikkerhet og personvern i et femårsperspektiv: Utvikling i UH-sektoren 2018-2022», side 20. Rapporten er tilgjengelig på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 12.03.2024.

Ifølge politiet, var majoriteten av de cyberrettede kriminelle lovbruddene som de registrerte i 2023 både opportunistiske og profittmotiverte. [30] Dette er i tråd med internasjonale studier. Verizon rapporterte for eksempel i 2022 og 2023 henholdsvis at 95 og 92 prosent av informasjonssikkerhetsbrudd i utdanningssektoren internasjonalt var økonomisk motivert.[31]

I 2023 registrerer vi at politiet vurderer trusselen fra nettkriminelle som økende på grunn av økt kompetanse og skadepotensial. I tillegg har markedet for kjøp og leie av verktøy og tjenester til kriminelle formål vokst, og de nettkriminelle aktørene viser stor evne og vilje til innovasjon i utvikling av sine verktøy. For eksempel mener politiet at utviklingen av kunstig intelligens vil gi stadig mer troverdige «deepfakes»[32], som kan benyttes til blant annet bedrageri og svindel.

Politiet opplyser også om at «hacktivister»[33] i økende grad søker å samarbeide. Dette gjør at slike grupper samlet kan øke sin kompetanse og kapasitet til å gjennomføre mer komplekse og skadelige handlinger som datainnbrudd. Slike grupper har ofte benyttet seg av tjenestenektangrep (DDoS) for å fremme sin politiske agenda, og kan operere i samarbeid med, eller på vegne av fremmede stater.[34]

Endringer i trusselbildet – mindre aktivitet, mer alvorlige trusler

Norske universiteter og høgskoler står også i 2024 ovenfor et krevende trusselbilde. Likevel er det indikasjoner på at mengden sikkerhetstruende aktivitet mot sektoren er redusert i 2023 i forhold til 2020 og 2021. Et slikt tegn er at NSM peker på forskning og utvikling som en sektor med redusert trusselaktivitet i forhold til tidligere. [35] Vår statistikk om brudd og hendelser i UH-sektoren fra fjorårets og årets kartlegging tyder på det samme. Vi kommer tilbake til statistikken nedenfor.

Dette betyr imidlertid ikke at UH-sektoren nødvendigvis har relativt lav trusselaktivitet i forhold til andre sektorer. I NSMs oversikt over cyberhendelser per samfunnssektor siden sommeren 2022, er UH-sektoren på samme nivå som forsvarssektoren (11 prosent).[35] Dette er betydelig høyere enn for eksempel justis- og beredskapssektoren (3 prosent), og finanssektoren (5 prosent).

Samtidig er det utviklingstrekk som tyder på at forsøkene på svindel, datainnbrudd, osv., blir stadig mer krevende å forebygge, oppdage, og håndtere for institusjonene. En viktig bidragsyter til denne utviklingen er at trusselaktørene ser ut til å fokusere mer på sosial manipulering som angrepsmetode sammenlignet med 2022. Verizon peker på at sosial manipulering erstattet «brute force» teknikker[36] på topp tre listen over de vanligste angrepsmetodene som

[30] Se «Politiets trusselvurdering 2024», side 10-11, og 13. Rapporten er tilgjengelig på Politiets trusselvurdering 2024. Sist besøkt 12.03.2024.
[31] Se Verizon: «2022 Data Breach Investigations Report», side 57-58. 2022-data-breach-investigations-report-dbir.pdf (verizon.com). Sist besøkt 12.03.2024. Se også «Data Breach Investigations Report 2023» side 54. Rapporten er tilgjengelig på DBIR Report 2023 - Summary of Findings | Verizon Business. Sist besøkt 12.03.2024.
[32] Deepfakes er et samlebegrep på bilder, video og lyd som er fremstilt ved hjelp av kunstig intelligens. Se side 13 i «Politiets trusselvurdering 2024.»
[33] Samlebetegnelse for politisk motiverte kriminelle grupperinger som opererer på internett. Definisjon hentet fra «Politiets trusselvurdering 2024», side 34.
[34] Et godt eksempel på en slik gruppe er KillNet som har en kjent tilknytning til Russland. For mer om KillNett og samarbeid mellom «hactivistgrupper» se «KillNet Showcases New Capabilities While Repeating Older Tactics», tilgjengelig på KillNet Showcases New Capabilities While Repeating Older Tactics | Mandiant. Sist besøkt 12.03.2024.
[35] Se «Nasjonalt digitalt risikobilde 2023», side 12-13. Rapporten er tilgjengelig på Nasjonalt digitalt risikobilde 2023.pdf (nsm.no). Sist besøkt 12.03.2024.
[36] «Brute force» teknikker er metoder hvor en angriper forsøker å oppdage angrepsmålets passord. Dette gjøres fortrinnsvis gjennom prøving og feiling, for eksempel ved bruk av programvare som gjetter kombinasjoner av brukernavn og passord. Se What is a Brute-Force Attack & Tips for Prevention | Verizon Business, sist besøkt 21.05.2024.

forårsaket brudd på informasjonssikkerheten i utdanningssektoren internasjonalt. [37] Også Google Cloud predikerer større utfordringer med å håndtere sosial manipulering i 2024 enn tidligere.[38]

De øvrige to angrepsmetodene i Verizons rapport var datainnbrudd, for eksempel gjennom utnyttelse av nulldagssårbarheter eller løsepengevirus. Den siste angrepsmetoden var utnyttelse av menneskelige og tekniske feil i IT-systemer. Til sammen utgjorde disse angrepsmetodene 76 prosent av de registrerte hendelsene i utdanningssektoren internasjonalt.

NSM har pekt på at sosial manipulering har blitt en mer alvorlig trussel mot norske virksomheter enn tidligere, blant annet fordi kvaliteten på målrettede svindel-eposter har nådd et urovekkende høyt nivå.[35] I likhet med PST og politiet, mener NSM at utviklingen i kunstig intelligens vil bidra til at svindel, desinformasjon, og spionasje vil foregå på nye og mer komplekse måter i fremtiden. I tillegg har også andre metoder som sårbarhetsskanning, løsepengevirus, og tjenestenektangrep blitt proffere.

Grunnen til at denne utviklingen øker vanskelighetsgraden for sikkerhetsorganisasjonene i UH-sektoren, er at sosial manipulering som angrepsmetode omgår flere av de viktigste tekniske sikkerhetstiltakene ved å rette seg mot mennesker fremfor IT-systemer. Denne angrepsmetoden kan være effektiv i UH-sektoren blant annet på grunn av at institusjonene har et høyt antall brukere, og det er utstrakt bruk av samarbeid på tvers av landegrenser, i tillegg til at sektoren vektlegger åpenhet.

Vi mener derfor at den skjerpede etterretningstrusselen fra fremmede stater og en økt profesjonalisering av angrepsmetoder hos nettkriminelle aktører, tilsier at det er blitt mer krevende å sikre sektorens informasjonsverdier enn tidligere. Samtidig er det positivt for sektoren at trusselaktiviteten ser ut til å ha blitt mindre enn tidligere.

Informasjonssikkerhet – brudd og hendelser i 2023

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 hadde registrert forsøk på brudd på informasjons- og personopplysningssikkerheten i 2023. I 2022 rapporterte institusjonene samlet om ca. 1450 brudd og hendelser, noe som var en nedgang på 30 prosent fra 2021. I 2023 har nedgangen fortsatt med 35 prosent: institusjonene rapporterte om ca. 950 hendelser og brudd.

[37] Se Verizon: «Data Breach Investigations Report 2023» side 54. Rapporten er tilgjengelig på DBIR Report 2023 - Summary of Findings | Verizon Business. Sist besøkt 12.03.2024.
[38] Se «Google Cloud Cybersecurity Forecast 2024», s 3-4 og 17. Rapporten er tilgjengelig på Google Cloud Cybersecurity Forecast 2024 | Mandiant. Sist besøkt 02.04.2024.

Om rapporteringen

I begge kartleggingene for 2022 og 2023 ble institusjonene bedt om å gi 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 skulle forstås: hvilke brudd eller hendelser er det snakk om? Likevel gir presentasjonen nedenfor et rimelig dekkende bilde av sektortilstanden, slik den ble rapportert til HK-dir.

Totaltallet på omkring 950 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».

Totaltallet på ca. 950 inkluderer brudd og hendelser som gjelder sikkerheten til personopplysninger (personopplysningssikkerhet). Det inkluderer imidlertid ikke andre typer personvernhendelser eller -avvik, for eksempel manglende sletting av personopplysninger eller mangelfulle vurderinger av det rettslige grunnlaget for bruk av personopplysninger. Omfanget av slike hendelser og avvik drøftes senere i kapitlet.

Fortsatt nedgang i rapporterte hendelser og brudd

Som tidligere år, var det de største institusjonene som rapporterte om flest hendelser og brudd. De fem institusjonene som meldte inn flest brudd og hendelser sto til sammen for 88 prosent av totalen i denne delen av sektoren.

Enkelte institusjoner rapporterte om flere registrerte sikkerhetssaker – blant annet innmeldte saker, varsler, eller oppfølgning av alarmer – enn tidligere. Likevel rapporterte disse institusjonene om færre hendelser og brudd enn tidligere, blant annet på grunn av endringer i det forebyggende sikkerhetsarbeidet som førte til økt registrering og håndtering på et tidligere tidspunkt.

Fire av institusjonene rapporterte om en økning i antall brudd og hendelser på mellom 15 og 49 prosent sammenlignet med fjoråret. Alle fire mente at økningen først og fremst skyldtes økt oppdagelses- og rapporteringsevne i egen organisasjon.

Hos de øvrige institusjonene ble det opplyst om relativt få hendelser og brudd, og det er små variasjoner mellom dem. Dette samsvarer med hva disse institusjonene har rapportert om tidligere.

Det kan fremstå som paradoksalt at både en nedgang i antall hendelser totalt, og en økning i registrerte hendelser lokalt vurderes som positivt. Årsaken til dette er at nedgangen er registrert av institusjoner med god deteksjonsevne, mens økningen er registrert hos institusjoner med et forbedringspotensial på dette området. Disse to trekkene indikerer at sektoren som helhet er utsatt for mindre trusselaktivitet enn tidligere, samtidig som at enkelte institusjoner har forbedret sin deteksjonsevne. Vi kommer tilbake til dette nedenfor.

Varierende oppdagelsesevne

Som i 2022, handlet det store flertallet av rapporterte hendelser og brudd i sektoren også i 2023 om IT-sikkerhet, spesielt nettbaserte hendelser (digital sikkerhet). De resterende tilfellene gjaldt andre typer brudd og hendelser, spesielt menneskelige feil og uhell.

Ettersom forhold knyttet til digital sikkerhet utgjorde den klart største hendelseskategorien, vil evnen til å oppdage denne typen hendelser og brudd påvirke rapporteringen. Desto bedre evne institusjonene har til å identifisere sikkerhetstruende aktivitet rettet mot egne dataressurser, jo flere hendelser og brudd vil bli registrert.

Variasjoner i antallet rapporterte hendelser og brudd kan indikere hvilke institusjoner som har best evne til å oppdage, analysere og håndtere ulike typer dataangrep og forsøk på datainntrenging. Det at mange av institusjonene rapporterer om få eller ingen brudd og hendelser, kan tyde på at oppdagelsesevnen i store deler av sektoren er lav. Dette inntrykket er forsterket av Riksrevisjonens rapport, hvor inntrengingstester hos tre forskningsinstitusjoner ga full kontroll over IT-infrastruktur hos to av dem.[39] I tillegg viser Riksrevisjonens undersøkelser at de reviderte virksomhetene hadde varierende grad av oversikter over hendelser.[40]

Samtidig vil antallet rapporterte brudd og hendelser påvirkes av andre forhold enn evnen til å oppdage og registrere dem. For eksempel er det mulig at de største institusjonene utsettes for flere forsøk på hendelser og brudd, blant annet fordi de er mer synlig på grunn av større offentlig profil enn mindre høgskoler. Det virker også å være varierende klassifiseringer og terskler for statistikkføring av avvik, brudd, og hendelser blant institusjonene. Dette kan påvirke antallet brudd og hendelser som rapporteres til HK-dir.

Typer hendelser og skadevirkninger

Nedenfor ser vi nærmere på hvilke typer hendelser og brudd som universitetene og høgskolene rapporterte om i 2023, og i hvilken grad de førte til skadevirkninger.

Det ble registrert enkelte alvorlige hendelser i 2023. Det ble registrert tre mulige løsepengevirusangrep, to ved bruk av en modifisert versjon av Cobalt Strike[41] og ett ved bruk av Rasberry Robin-skadevare.[42] En institusjon rapporterte om et avansert forsøk på datainnbrudd, hvor trusselaktøren forsøkte å omgå totrinnsinnloggingen. Ingen av disse hendelsene fikk skadevirkninger utover merarbeid for IT-avdelingene og utbytting av utstyr for institusjonene som ble utsatt for angrepene.

En institusjon rapporterte om at flere av de alvorlige sikkerhetssakene i 2023 dreide seg om datainnbrudd på IT-systemer og tjenester utenfor sentral IT-drift. Dette var typisk systemer som forskere og studenter selv satte opp, men heller ikke disse innbruddene medførte alvorlige skadevirkninger for institusjonen. Motivene bak disse angrepene var ikke kjent, og de ble derfor ikke kategorisert som løsepengevirusangrep.

Når det gjelder mindre alvorlige brudd og hendelser, dreide de fleste seg om nettkriminalitet. Disse bruddene og hendelsene handlet stort sett om kompromitterte brukerkontoer, og forsøk på faktura- og direktørsvindel. Den nest største hendelseskategorien var tekniske og menneskelige feil og uhell. Funnene sammenfaller med hva vi har funnet i tidligere kartlegginger, og med internasjonale trender i utdanningssektoren.[31]

Skadevirkningene av disse bruddene og hendelsene var relativt små: blant annet førte et par vellykkede svindelforsøk til kjøp av gavekort for noen tusen kroner, en kompromittert brukerkonto kan ha medført at

[39] Se Riksrevisjonens rapport «Informasjonssikkerhet i forskning innenfor kunnskapssektoren Offentlig versjon av Dokument 3:11 (2023–2024)», s. 10.
[40] Se Riksrevisjonens rapport «Informasjonssikkerhet i forskning innenfor kunnskapssektoren Offentlig versjon av Dokument 3:11 (2023–2024)», s. 89-91.
[41] For mer informasjon om Cobalt Strike se Cobalt Strike | Defining Cobalt Strike Components & BEACON (mandiant.com). Sist besøkt 13.03.2024.
[42] For mer informasjon se CTI Roundup: Raspberry Robin, USB Malware Update, and Ransomware Victims on the Rise | Tanium. Sist besøkt 09.04.2024.

personopplysninger til eieren av brukerkontoen ble hentet ut, og enkelte feil og uhell førte til korte tjenesteavbrudd for IT-systemer hos noen institusjoner.

Den tydeligste endringen fra fjorårets kartlegging er at omtrent to tredjedeler av institusjonene rapporterer om en økning i målrettede forsøk på nettfiske, og/eller bedre kvalitet forsøkene. Forbedringene var tydelige både i innhold og i målrettingen mot utvalgte medarbeidere. Innholdet hadde for eksempel bedre språk og kunne bruke informasjon fra institusjonenes nettsider. Målrettingen var forbedret ved at forsøkene rettet seg mot enkeltpersoner med beslutningsmyndighet, eller økonomiavdelinger. Dette sammenfaller med utviklingen som NSM og politiet beskriver i sine risiko- og trusselvurderinger.

APT-hendelser – statlig og statsstøttet hacking

Universitetene og høgskolene ble spurt om de hadde registrert bekreftede eller mistenkte APT-hendelser – datatyveri eller kunnskapsspionasje utført av statlige eller statsstøttede hackergrupper (nettkriminelle grupper som utfører oppdrag for statlige myndigheter).[43]

I 2023 hadde ingen institusjoner registrert bekreftet eller mistenkt APT-aktivitet. Enkelte institusjoner hadde merket seg mistenkelig aktivitet som påloggingsforsøk fra utlandet, rekognosering av nettverk, og til dels avanserte angrepsmetoder mot egne datamaskiner, men mente likevel å ikke ha grunn til å mistenke at en statlig eller statsstøttet aktør hadde vært involvert.

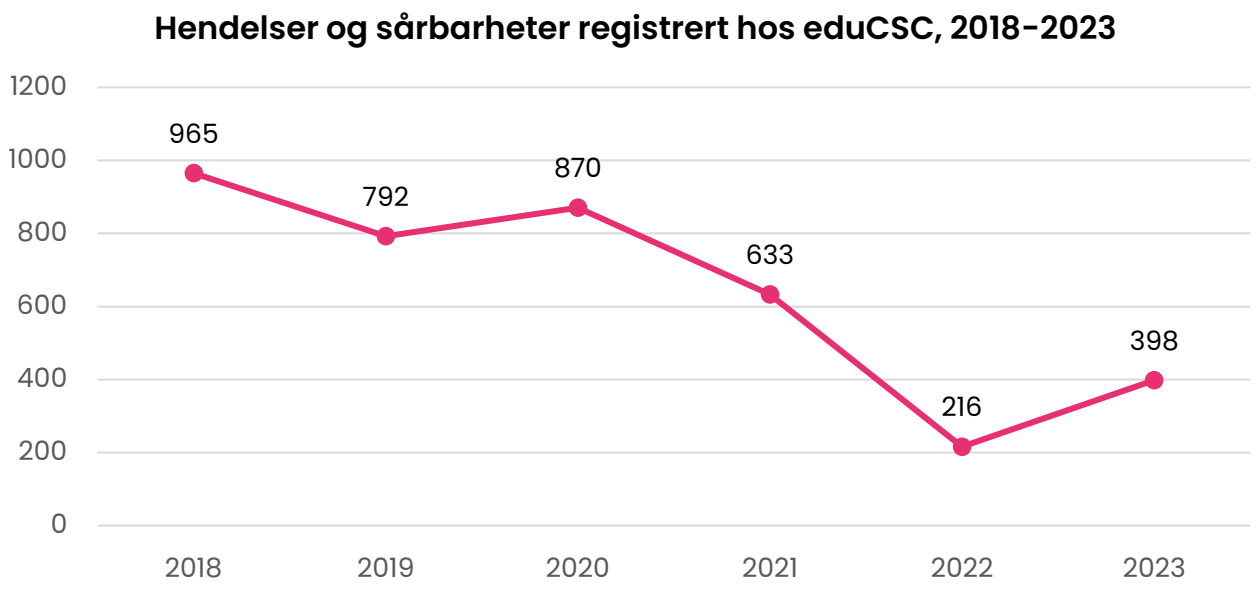
Til sammenligning ble det rapportert om fire brudd og hendelser som kunne tilskrives eller mistenkes at APT-aktører sto bak i 2022. I 2021 rapporterte seks institusjoner om bekreftede, og åtte institusjoner om mistenkte APT-hendelser. Det ser derfor ut til å ha vært en nedadgående utvikling i mistenkt og bekreftet aktivitet fra slike aktører i UH-sektoren de to siste årene.

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.

I 2023 rapporterte sektorens responsmiljø om 398 digitale sikkerhetshendelser og sårbarheter. Dette er en økning på 182 hendelser og sårbarheter sammenlignet med 2022. Tallene gjelder i utgangspunktet for alle de 140 kundene til eduCSC, men det er de 57 kundene som er tilknyttet forskningsnettet som står for mesteparten av rapporteringen. De 21 statlige universitetene og høgskolene, og seks av de syv øvrige virksomhetene som HK-dir kartlegger inngår blant disse 57 virksomhetene.

[43] 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.



Figur 2 - Hendelser og sårbarheter registrert hos eduCSC, 2018-2023

Figuren viser at reduksjonen i antallet registrerte hendelser og sårbarheter har vært betydelig siden toppåret i 2018. Likevel har det vært en økning mellom 2022 og 2023. Hovedårsaken til dette var ifølge eduCSC en økning i antall varsler om nye sårbarheter i IT-systemer og tjenester.

De viktigste sakskategoriene fra eduCSC hadde derfor endret seg noe fra 2022. Det var fortsatt sårbare IT-systemer som utgjorde den største sakskategorien, henholdsvis 48 og 62 prosent i 2022 og 2023. Den nest største kategorien i 2022 var forsøk på datainntrenging (8 prosent), mens i 2023 hadde nulldagssårbarheter[44] overtatt andreplassen (6 prosent). Datainntrenging utgjorde 3 prosent av hendelsene som var registrert hos eduCSC i 2023.

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 inkludert dem i sin årsstatistikk.

I tillegg mente eduCSC at hendelser, brudd og sårbarheter oftere enn tidligere ble formidlet via sektorens varslingskanal – IRT-chat. De ble ikke registrert i statistikken til eduCSC. Dette var fortsatt tilfellet i 2023.

Disse endringene kunne likevel forklare hele nedgangen fra 2021 til 2022. eduCSC fremhevet derfor at det hadde vært en reell reduksjon i antallet hendelser, brudd og sårbarheter i 2022, og en reell økning i 2023.

[44] NSM beskriver en nulldagssårbarhet som «En nulldagssårbarhet utgjør en mulighet for en trusselaktør til å utnytte en sårbarhet som produsenten og brukerne ikke er kjent med. Denne type sårbarheter er vanskelig å beskytte seg mot». For eksempel og mer informasjon, se Nulldagssårbarhet i Ivanti Endpoint Manager (MobileIron Core) – Nasjonal sikkerhetsmyndighet (nsm.no), sist besøkt 21.05.2024.

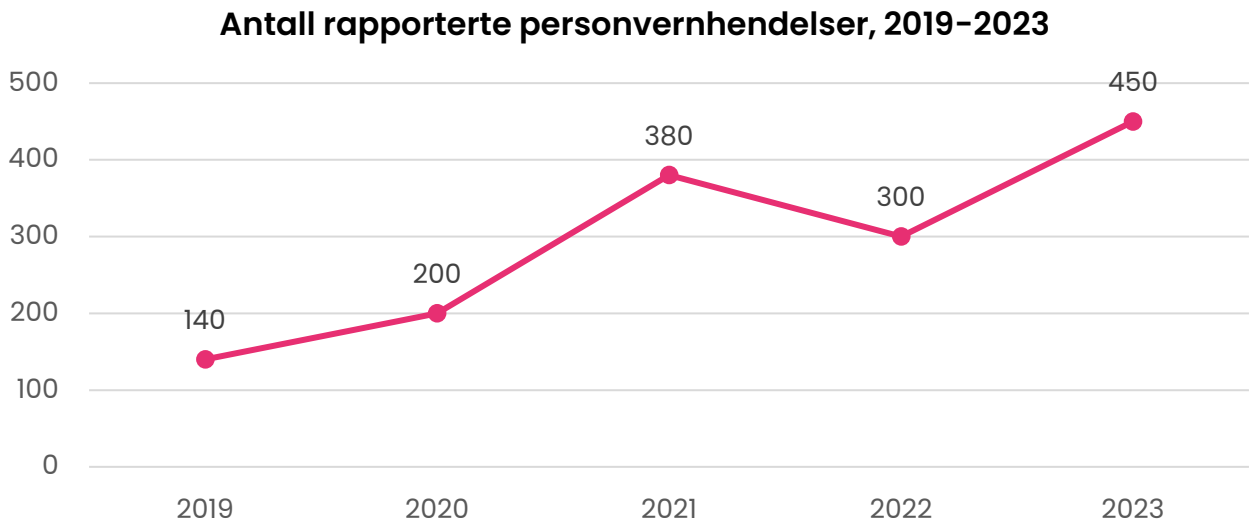
Personvern – brudd og hendelser i 2023

Universitetene og høgskolene ble bedt om å oppgi hvilke personvernsaker de hadde registrert i 2023. Dette inkluderer også saker hvor brudd på sikkerheten til personopplysninger ble vurdert å være meldepliktig til Datatilsynet. Men primært 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

Til sammen rapporterte universitetene og høgskolene om ca. 450 personvernhendelser. Dette er en økning på ca. 33 prosent sammenlignet med 2022 (ca. 300).

Fem institusjoner rapporterte om en betydelig økning av avvik og hendelser i 2023 sammenlignet 2022. Disse fem institusjonene står for brorparten av økningen i statistikken, men også flere av de øvrige institusjonene registrerte små økninger i antall avvik og hendelser i 2023. Den vanligste forklaringen på økningen i avvik og hendelser, var forbedret avviksmelding og registrering hos institusjonene.



Figur 3 - Antall rapporterte personvernhendelser, 2019-2023

Typer personvernsaker

De fleste avvikene og hendelsene i 2023, handlet om feil i behandling av personopplysninger og brudd på interne rutiner (avvik). Vanlige feil og avvik inkluderte manglende oppdatering av behandlingsprotokollen ved innføring av nye applikasjoner eller tjenester, behandlinger av personopplysninger uten lovlig grunnlag, og feil i tilgangsstyringen.

I 2022 handlet de fleste hendelsene og avvikene om at påbegynte registreringer av forsknings- og studentprosjekter hos Sikts personverntjenester ikke var ferdigstilt. Det var også en stor andel av avvikene og hendelsene som dreiede seg om manglende bekreftelse på sletting og anonymisering av personopplysninger i slike prosjekter.

Den årlige statistikken påvirkes av om enkelte institusjoner gjennomfører større opprydninger i sine registeringer hos Sikts personverntjenester i løpet av kartleggingsperioden. Vi ser at institusjoner som gjennomfører slike opprydninger, registrerer en god del flere avvik enn andre institusjoner. Likevel var det en klar overvekt av denne

typen avvik også hos flere institusjoner som ikke gjennomførte slike opprydninger i 2022, hele 74 prosent av alle registrerte personvernavvik- og hendelser i 2022 var av denne typen.

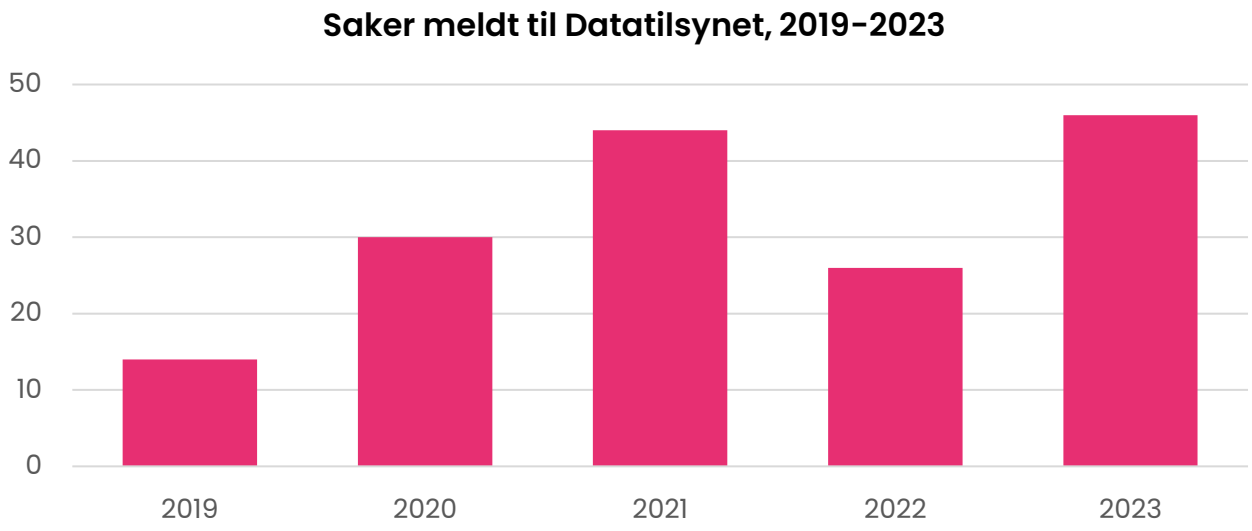
I årets kartlegging er imidlertid den største økningen i antall avvik og hendelser endret, og handler om andre typer avvik og feil enn de som gjelder forsknings – og studentprosjekter registrert hos Sikts personverntjenester. Som nevnt ovenfor, handlet hendelsene og avvikene hovedsakelig om feil i behandlinger av personopplysninger, og i tilgangsstyringen i IT-systemer. Dette er tilfellet både om vi teller med og uten de institusjonene som gjennomførte slike opprydninger i 2023. Vi mener derfor at det har vært en reell endring i hvilke typer personvernhendelser og avvik institusjonene rapporterte om i 2023, sammenlignet med tidligere år.

Som for hendelser og brudd på informasjonssikkerheten, er det variasjon blant institusjonene i antall rapporterte personvernhendelser. En viktig forskjell er imidlertid at alle institusjonene behandler betydelige mengder personopplysninger, mens mengden og typer andre informasjonsverdier kan variere mellom institusjonene. Flere institusjoner har påpekt i møtene med HK-dir at de mistenker at det fortsatt er mørketall i rapporteringen.

Saker meldt til Datatilsynet

Brudd på personopplysningssikkerheten som innebærer risiko for krenkelser av personvernet, skal meldes til Datatilsynet.[45] Som ved tidligere års kartlegginger rapporterte universitetene og høgskolene om hvor mange og hvilke typer saker de hadde meldt til Datatilsynet.

Figur 4 viser at det ble meldt om 20 flere saker til Datatilsynet i 2023 enn i 2022. Økningen i antall saker skyldtes at institusjonene meldte inn flere brudd av samme type som tidligere, hvor personopplysninger ble tilgjengelige for uvedkommende (konfidensialitetsbrudd). De vanligste årsakene til bruddene var feilsending av epost, feil publisering av personopplysninger, og lagring av slike opplysninger på lagringsområder som var tilgjengelige for uvedkommende (egne ansatte eller studenter). Dette samsvarer med tidligere kartlegginger.



Figur 4 - Saker meldt til Datatilsynet, 2019-2023

Det var likevel enkelte årsaker som skilte seg ut i 2023: ca. 14 av bruddene kom som følge av feil i innføring eller bruk av sektorens felles identitets og tilgangsstyring (IAM). En annen årsak som forårsaket fem av bruddene var

[45] 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.

knyttet til en feil hos Direktoratet for Forvaltning og Økonomistyring (DFØ), som ga uvedkommende tilgang til personopplysninger.

Det ble ikke opplyst om meldinger til Datatilsynet 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.

Oppsummering og behov for tiltak

EOS-tjenestene fremhever i sine årlige vurderinger at trusselbildet er mer utfordrende enn tidligere. Russland har fortsatt et stort etterretningsbehov rettet mot vestlig teknologi og kunnskap etter invasjonen av Ukraina. Etterretningstrusselen fra Kina er opprettholdt på samme nivå som tidligere, og forventes å bli mer fremtredende i tiden som kommer. Norske forskningsmiljøer innen en rekke fagområder kan fortsatt være aktuelle mål for cyberoperasjoner. I tillegg har både de statlige og nettkriminelle trusselaktørene styrket sin kompetanse og rekkevidde gjennom forbedret evne til samarbeid og kontinuerlig tilpasning av sine metoder.

Antallet rapporterte informasjonssikkerhetshendelser og -brudd hos universitetene og høgskolene redusert med 35 prosent. Den største nedgangen ble registrert hos de største institusjonene. Enkelte institusjoner opplyste om en økning i antall registrerte hendelser og brudd.

Det ble heller ikke meldt om at hendelsene og bruddene hadde medført alvorlige skadevirkninger. For første gang ble det ikke rapportert om mistenkt eller bekreftet aktivitet fra statlige eller statsstøttede hackergrupper fra institusjonene.

Nettkriminalitet utgjorde fortsatt den klart største kategorien hendelser og brudd. Deretter fulgte utilsiktede menneskelige og tekniske feil eller uhell. Flere institusjoner rapporterer om forbedringer i innhold og målrettingen av nettfiskeforsøk mot ansatte og studenter. Statistikken fra Cybersikkerhetssenteret i Sikt viser at det er hovedsakelig de samme typene hendelsene og sårbarhetene i utdannings- og forskningssektoren utover de 28 virksomhetene i HK-dirs kartlegginger.

I 2023 har vi registrert en økning på ca. 33 prosent flere hendelser og avvik innen personvernområdet sammenlignet med 2022. Det er også en økning på 20 flere sikkerhetsbrudd som er meldepliktige til Datatilsynet sammenlignet med fjorårets kartlegging. Antall meldte saker til Datatilsynet er derfor tilbake på 2021-nivå.

På bakgrunn av disse funnene ser vi at sektoren har behov for å forbedre følgende områder:

i. Evne og system for å oppdage og registrere informasjonssikkerhetsbrudd- og hendelser ved den enkelte institusjon.

ii. Styrke samhandling og kompetansedeling om informasjonssikkerhet og personvern mellom organisatoriske enheter (fakulteter, institutter, og administrative enheter) hos institusjonene.

Vi registrerer at det er varierende evne og gjennomføring av registering av avvik og hendelser mellom institusjonene. Vi merker oss at også Riksrevisjonen peker på det samme.[40] Etter vårt syn vil lokal ledelse ved institusjonene være tjent med bedre oversikt over avvik og hendelser i sektoren for å kunne iverksette hensiktsmessige tiltak.

Vi registrerer at også i 2023 er utilsiktede menneskelige feil og uhell blant de to øverste årsakene til at brudd og hendelser oppstår hos institusjonene. Spesielt avvik eller brudd på personvernet ser ut til å være forårsaket av slike feil og uhell. Samtidig ser vi en forbedring i rapportering av avvik blant institusjoner med informasjonssikkerhets-

og personvernkontaktnettverk. Slik vi ser det, er det hovedsakelig den bevisstgjørende og kompetansehevende effekten av slike nettverk som vil være viktig for å oppdage og håndtere utilsiktede feil og uhell.

Vi ser derfor behov for tiltak som kan bidra til at slike nettverk opprettes og videreutvikles blir prioritert. Dette vil sannsynligvis kunne bidra til alvorlighetsgraden i slike hendelser fortsetter å være forholdsvis lav. Når det gjelder antall avvik, antar vi at dette vil øke noe på kort sikt dersom avviksrapporteringen bedres. Samtidig mener vi at behandling av personopplysninger vil bli sikrere, og sannsynligvis vil skadevirkningene av slike hendelser reduseres ytterligere.

Kapittel 3: Universiteter og høgskoler – sårbarheter, forbedringer og status

Innledning

De to første kapitlene indikerer at selv om antallet rapporterte hendelser og brudd er redusert i 2023, er UH-sektoren fortsatt sårbar for trusler mot informasjonssikkerheten og personvernet. For å forebygge, oppdage og håndtere nye hendelser og brudd, er det derfor 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 departementets policy for informasjonssikkerhet og personvern.

I dette kapitlet drøftes tre hovedspørsmål:

1. Hvilke sårbarheter mente universitetene og høgskolene at de har behov for å utbedre?
2. Hvilke tiltak hadde universitetene og høgskolene iverksatt 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 Kunnskapsdepartementets policy for informasjonssikkerhet og personvern?

Det gis også en oversikt over hvordan institusjonene hadde fulgt opp HK-dir sine anbefalinger for arbeidet med informasjonssikkerhet og personvern. Anbefalingene ble gitt i brev til den enkelte institusjon etter fjorårets kartlegging.

Rapporterte sårbarheter i 2023

I kartleggingen blir universitetene og høgskolene spurt om å oppgi sårbarheter som kan medføre brudd på informasjonssikkerheten og personvernet ved deres institusjon.

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

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.

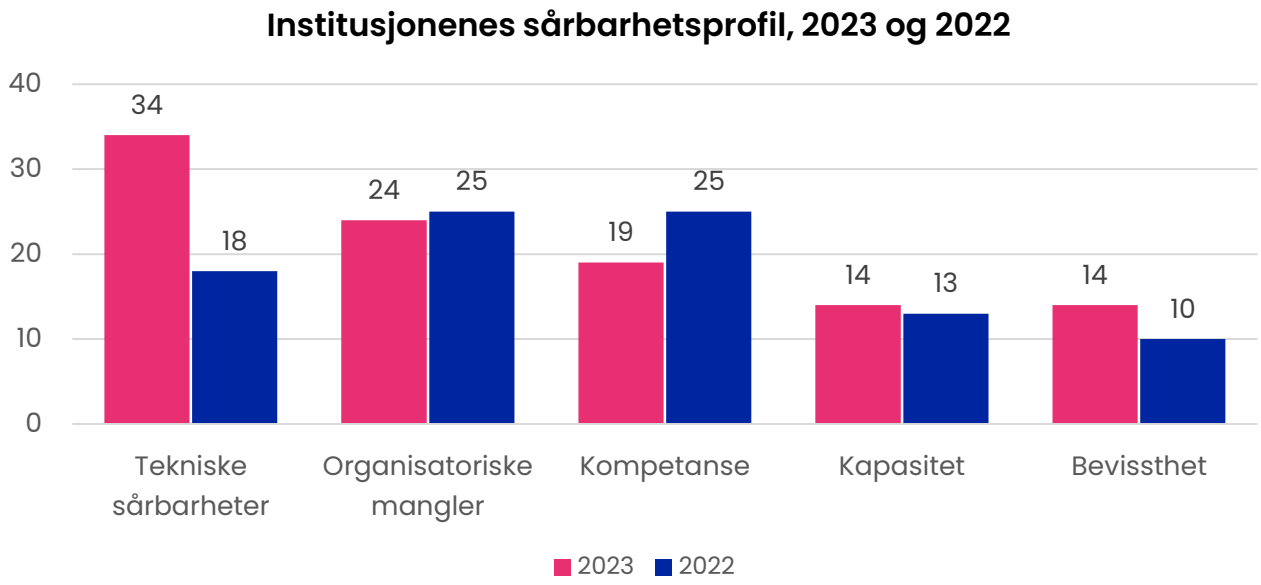
Organisatoriske mangler: svakheter med måten arbeidet med informasjonssikkerhet og personvern er strukturert på, og mangler ved eller fravær av rutiner og prosedyrer for sikker og lovlig håndtering av informasjonsverdier, spesielt personopplysninger.

Tekniske sårbarheter: ulike typer tekniske svakheter i digitale arbeidsredskaper og 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.

Figur 5 viser institusjonenes sårbarhetsprofil, det vil si de fem hovedtyper sårbarheter som de 21 universitetene og høgskolene mente at de hadde behov for å utbedre. Sårbarhetsprofilen for 2023 er sammenlignet med profilen i 2022.



Figur 5 - Institusjonenes sårbarhetsprofil, 2023 og 2022

Sårbarhetsprofilen – endringer fra i fjor

I 2022 ble organisatoriske mangler og manglende kompetanse om informasjonssikkerhet og personvern oppgitt som de viktigste sårbarhetene. Deretter var tekniske sårbarheter på tredjeplass etterfulgt av manglende kapasitet. Bevissthet om utfordringer knyttet til informasjonssikkerhet ble rangert som den minst viktige sårbarhetstypen.

Som figuren viser, er sårbarhetsprofilen for 2023 endret sammenlignet med forrige kartlegging. Tekniske sårbarheter ved institusjonene ble i årets kartlegging oppgitt som den viktigste sårbarheten. Denne typen sårbarheter har utviklet seg fra å være lite viktig både i 2019 og 2020, til å bli gradvis viktigere i 2021 og 2022, og nå oppgis som den viktigste sårbarhetstypen.

Publiseringen av Riksrevisjonens rapport om informasjonssikkerheten hos 10 forskningsinstitusjoner i januar 2024 viste blant annet at forskningsdata ikke var tilstrekkelig sikret mot dataangrep hos disse institusjonene, og det ble påpekt behov for flere konkrete tekniske sikringstiltak til institusjonene som ble undersøkt. Riksrevisjonen opplyste i samme rapport at det var sannsynlig at andre institusjoner i norsk forsknings- og utdanningssektor hadde flere av de samme sårbarhetene som de institusjonene som ble revidert. Det er grunn til å tro at dette kan ha påvirket vurderingene av egne sårbarheter hos institusjoner som omfattes av HK-dirs kartlegging.

Deretter følger organisatoriske mangler, for eksempel uklar fordeling av roller og ansvar eller manglende rutiner for behandling av personopplysninger, som er oppgitt på omtrent samme nivå som i fjor. Vi ser videre at det er en nedgang i hvor ofte kompetanse oppgis som en sårbarhet i arbeidet med informasjonssikkerhet og personvern, mens kapasitet ble oppgitt å være omkring på samme nivå som i 2022.

Universitetene og høgskolene rapporterte bevissthet som den minst viktige sårbarheten i årets kartlegging, på samme måte som i 2022. Det er verdt å bemerke at dette var en relativt vesentlig endring mellom kartleggingene i 2021 og 2022, ettersom bevissthet i 2021 ble oppgitt som den nest viktigste sårbarheten.

Iverksatte tiltak i 2023

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 2023 for å utbedre sårbarheter og forbedre evnen til å forebygge, oppdage, og håndtere brudd på informasjonssikkerheten og 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 årets kartlegging oppga 12 av 21 institusjoner manglende kapasitet som en sårbarhet, hvilket er en reduksjon fra 18 i 2022. Som i tidligere kartlegginger har vi spurt universitetene og høgskolene om hvor mange årsverk som er øremerket til arbeidet med informasjonssikkerhet og personvern ved deres institusjon.

Figur 6 gir en oversikt over endringene som ble oppgitt sammenlignet med årsverksinnsatsen i 2022.

Figur 6 - Endringer i årsverksinnsatsen, 2022-2023

Vi ser at ni institusjoner opplyste om en økning i antall årsverk øremerket til arbeid med informasjonssikkerhet og personvern fra 2022 til 2023. Like mange institusjoner oppga at årsverksinnsatsen var uendret fra 2022. I motsetning til fjorårets kartlegging var det i år tre institusjoner som rapporterte om en reduksjon i antall årsverk øremerket til arbeidet med informasjonssikkerhet og personvern.

Samlet sett har de 21 universitetene og høgskolene rapportert om en økt årsverksinnsats sammenlignet med fjorårets kartlegging. Denne økningen er omtrent lik som i tidligere kartlegginger. 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

Med innleid kapasitet menes at universitetene og høgskolene henter inn eksterne spesialister til oppgaver som institusjonene selv mangler kapasitet eller kompetanse til å utføre. Spesialistkapasitet kan kjøpes hos tilbydere av fellestjenester i UH-sektoren eller hos private aktører.

I 2023 rapporterte 10 institusjoner at de hadde kjøpt tjenester fra private aktører for å styrke arbeidet med informasjonssikkerhet og personvern.

Institusjonene leide inn spesialistkapasitet fra private aktører for å løse en rekke oppgaver. Det gjaldt i særlig grad revisjoner av ledelsessystemet for informasjonssikkerhet eller internkontrollen for personvern (GDPR), etablere beredskaps- og kontinuitetsplaner, fylle rollen som personvernombud, gjennomføre kriseøvelser, og kartlegge behandlinger av personopplysninger.

Sikkerhetsfunksjonalitet som kan kjøpes hos leverandører av viktige IT-tjenester, for eksempel MS 365, bidrar også til å styrke institusjonenes kapasitet innen informasjonssikkerhet og personvern. Eksempelvis har flere institusjoner oppgitt at de benyttet Crayon[46] til å utnytte sikkerhetsfunksjonalitet i deres M365-lisenser.

I kapittel 1 har vi i tillegg sett at Sikt sine personverntjenester kan være viktige kapasitetsøkende ressurser for institusjonenes arbeid med personvern i forskning.[47] Institusjonene benytter også tjenester fra Cybersikkerhetssenteret for forskning og utdanning hos Sikt, blant annet regelmessig testing av den tekniske sikkerheten i datamaskiner som er eksponert mot Internett.[48]

Hvor mye den innleide spesialistkapasiteten utgjorde i form av årsverk i 2023, har vi ikke informasjon om.

Andre viktige tiltak i 2023

Vi spurte institusjonene om hva egne årsverk og den innleide kapasiteten hadde jobbet med i 2023: hvilke og hvor mange tiltak hadde universitetene og høgskolene iverksatt for å utbedre sårbarheter og styrke arbeidet med informasjonssikkerhet og personvern?

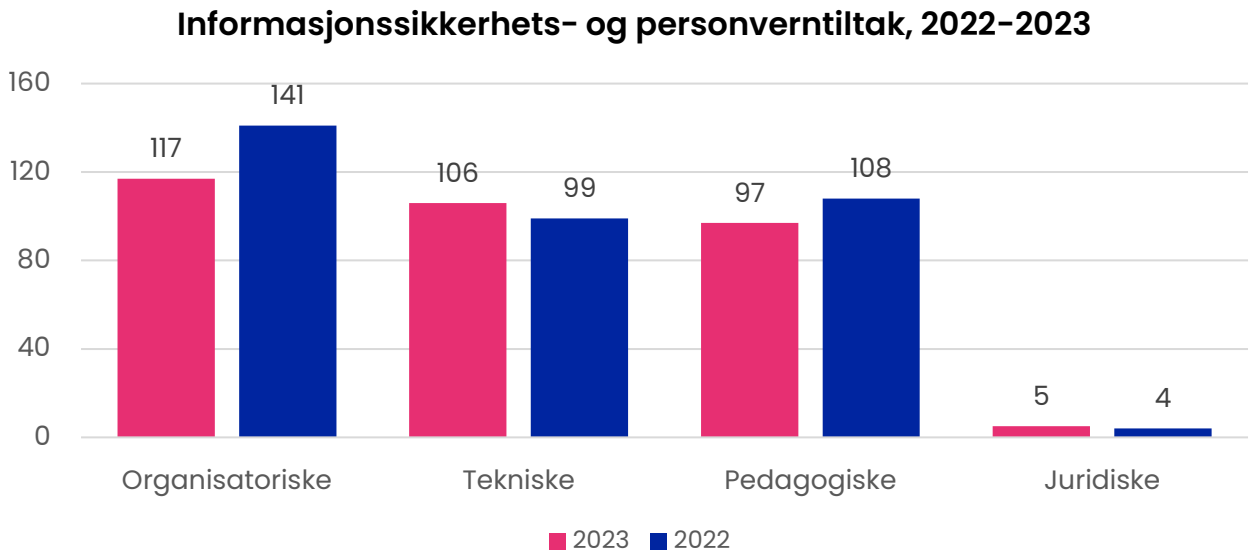
Om tiltakene

Enkelte av tiltakene i figur 7 er konkrete informasjonssikkerhets- eller personverntiltak (slik som spesifisert i ISO/IEC 27001 vedlegg A eller 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» eller «opplæring i risikovurderinger» romme flere kurs- eller opplæringssamlinger. Vi regner imidlertid dette som kun to tiltak. Tiltaksaktiviteten har derfor vært noe større enn det som fremgår av figuren.

[46] Se Crayon | Hjem - Crayon, sist besøkt 21.05.2024.
[47] 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 19.03.2024.
[48] Oversikt over Sikt sine digitale sikkerhetstjenester, se https://sikt.no/tjenester/cybersikkerhetssenter-forskning-og-utdanning#abonnementer. Sist besøkt 19.03.2024.

Figur 7 gir en oversikt over antall og hovedtyper rapporterte informasjonssikkerhets- og personverntiltak i 2022 og 2023. Tiltakene kategoriseres i fire hovedkategorier: organisatoriske, tekniske, pedagogiske, og juridiske.



Figur 7 - Informasjonssikkerhets- og personverntiltak, 2022-2023

Figuren viser at universitetene og høgskolene totalt rapporterte om at de hadde iverksatt 325 tiltak innen informasjonssikkerhets- og personvernområdet i 2023. Dette er en reduksjon sammenliknet med 352 rapporterte tiltak for 2022, og er på nivå med 2021 hvor det totale antallet rapporterte tiltak var 322.

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.

Tiltaksprofilen – hvordan de ulike tiltakene fordeler seg mellom de ulike kategoriene – har en viss endring fra 2022 til 2023. Organisatoriske tiltak var fremdeles den største tiltakskategorien både i 2022 og 2023, men hadde en nedgang i antallet fra 141 i 2022 til 117 i 2023. Samtidig var det flere tekniske tiltak i 2023 enn ved forrige kartlegging, noe som medførte et plassbytte med pedagogiske tiltak. Det var få juridiske tiltak både i 2022 og i 2023.

Organisatoriske tiltak

De viktigste organisatoriske tiltakene som institusjonene rapporterte om, handler om det vi kan kalle for systemtiltak. Dette er tiltak som har til hensikt å etablere eller forbedre systematikken og helheten i arbeidet med informasjonssikkerhet og personvern. Mange institusjoner rapporterte om at de hadde videreutviklet ledelsessystemet for informasjonssikkerhet eller internkontrollen for personvern (GDPR), for eksempel tydeliggjøring av rollene i sikkerhetsorganisasjonen eller revisjoner av arbeidet med informasjonssikkerhet.

I likhet med tidligere kartlegginger oppga de fleste av institusjonene at de arbeidet med etablering eller videreføring av interne strukturer som informasjonssikkerhetsforum, faggrupper eller nettverk av personvernkontakter på enhetsnivå. Forumene består av medarbeidere med viktige roller i sikkerhetsorganiseringen (informasjonssikkerhetsleder, personvernombud, system-, tjeneste- eller prosesseiere). Formålet med slike tiltak er vanligvis erfaringsutveksling og kompetanseheving, planlegging og gjennomføring av større tiltak, og forankring av arbeidet med informasjonssikkerhet og personvern i hele organisasjonen.

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

Som omtalt i kapittel 1, nevnte 10 institusjoner ulike tiltak knyttet til eksportkontroll, blant annet kartlegginger og ekstra sikringstiltak ved behov.

Tekniske tiltak

Denne typen tiltak har som hovedformål å forhindre at trusselaktører, spesielt nettkriminelle grupper og statlige aktører, stjeler eller ødelegger viktig informasjon eller misbruker institusjonenes datamaskiner.[49] Tiltakene skal også sørge for at tekniske eller menneskelige feil og uhell ikke fører til brudd på informasjonssikkerheten og krenkelser av personvernet.

Samtlige institusjoner oppga at de hadde gjennomført to eller flere tekniske tiltak for å forebygge brudd på informasjonssikkerheten og krenkelser av personvernet i årets kartlegging. Viktige tiltak som ble trukket frem var arbeid med totrinnsinnlogging, styrking av sikkerhetsbarrierer i nettverket, og forbedret kontroll på tilganger.

Det ble rapportert om en rekke tekniske tiltak for å styrke evnen til å oppdage og håndtere digitale sikkerhetshendelser. Flere av universitetene og høgskolene nevnte ulike aktiviteter relatert til sikkerhetsverktøyet Defender, og de hadde arbeidet med å utnytte sikkerhetsfunksjonalitet som følger med deres lisensnivå. Dette gjaldt både funksjonalitet for å forebygge angrep og for å etablere alarmer ved sikkerhetsrelaterte hendelser. Flere av de samme institusjoner trakk også frem arbeid med ulike loggløsninger og verktøy for logganalyse for å bedre oppfølgingen av informasjonssikkerhetshendelser.

Sårbarhetsskann gjennomføres for alle de 21 universitetene og høgskolene for å avdekke sikkerhetshull i institusjonenes internetteksponerte tjenester. Flere av institusjonene trakk frem målrettede aktiviteter for å rette avdekkede sårbarheter forbundet med denne skanningen. Videre var det enkelte institusjoner som opplyste om gjennomføring av interne sårbarhetsskann for å finne sikkerhetshull i deres systemer og arbeid med utbedring av funnene.

Flere institusjoner rapporterte også om tiltak knyttet til totrinnsinnlogging. Dette var i stor grad forbedringer av eksisterende løsninger eller utvidelser av hvilke tjenester som krever totrinnsinnlogging. Arbeid som ble nevnt var utfasing av sms, etablering av «number-matching», og krav om totrinnsinnlogging på flere tjenester.

På samme måte som for sårbarhetsprofilen er det grunn til å anta at Riksrevisjonens rapport om informasjonssikkerheten hos 10 forskningsinstitusjoner har hatt betydning for institusjonenes aktivitet rundt tekniske sikringstiltak.

Pedagogiske tiltak

Pedagogiske tiltak har som formål å utbedre sårbarheter med hensyn til medarbeidernes kompetanse og bevissthet om informasjonssikkerhet og personvern. Som ved tidligere kartlegginger, var det to hovedtyper tiltak det ble opplyst om.

For det første, skreddersydd opplæring og kompetanseheving. Disse tiltakene var rettet mot medarbeidere med ansvar eller 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 øke bevisstheten og å opplyse om vanlige digitale trusler, for eksempel nettfiske eller

[49] Datamaskiner kan blant annet misbrukes til utvinning av kryptovaluta og gjennomføring av dataangrep mot andre virksomheter.

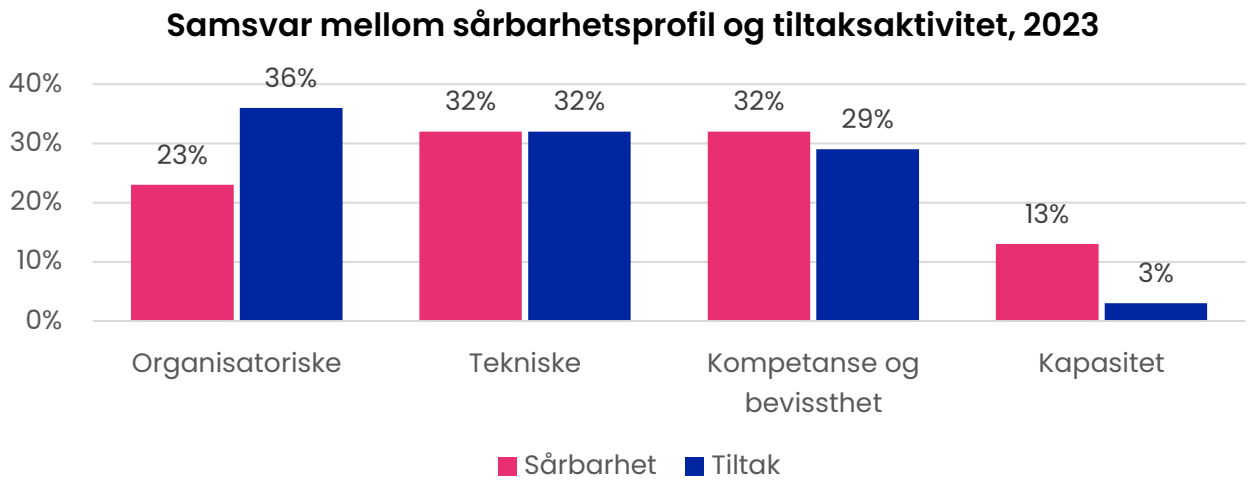
svindelepost. Det var også aktiviteter som formidlet mer omfattende informasjon om informasjonssikkerhet og personvern f.eks. i møter med studenter og ansatte, eller på institusjonenes hjemmesider.

Et siste viktig pedagogisk tiltak var kriseøvelser – håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser. I 2023 hadde de fleste av universitetene og høgskolene gjennomført minst en kriseøvelse som omhandlet informasjonssikkerhet eller personvern.

Samsvar mellom sårbarhetsprofil og tiltaksaktivitet?

I hvilken grad samsvarte tiltaksaktiviteten diskutert ovenfor med institusjonenes sårbarhetsprofil diskutert tidligere? Var det sammenfall mellom det universitetene og høgskolene mente var de viktigste sårbarhetskategoriene og de tiltakskategoriene hvor aktiviteten hadde vært størst?

Figur 8 gir en oversikt over forholdet mellom sårbarhetsprofilen og tiltaksaktivitet hos de 21 institusjonene i 2023.



Figur 8 - Samsvar mellom sårbarhetsprofil og tiltaksaktivitet, 2023[50]

I figuren ser vi at det er varierende sammenfall mellom sårbarhetsprofilen og tiltaksaktiviteten i denne delen av UH-sektoren i 2023. Det innebærer at fordelingen av tiltaksaktiviteten hos universitetene og høgskolene bare til en viss grad speiler de områdene (sårbarhetskategoriene) hvor institusjonene mente at de hadde størst behov for forbedringer.

Vi ser at organisatoriske tiltak utgjør den største tiltakskategorien til tross for at både tekniske sårbarheter og kompetanse og bevissthet ble oppgitt som viktigere sårbarheter av institusjonene. Et tilsvarende misforhold ser vi mellom sårbarhetsvurderingen og tiltak relatert til kapasitet, hvor tiltaksaktiviteten er lavere enn hva institusjonenes sårbarhetsvurderinger skulle tilsi. Til tross for at institusjonene samlet sett har styrket sin kapasitet (årsverksinnsats) de senere årene, opplyste flere av institusjonene om kapasitetsutfordringer som en viktig sårbarhet i 2023.

Flere av institusjonene rapporterte om endringer i organisering for bedre utnyttelse av personalressurser og kompetanse innen informasjonssikkerhet og personvern. For eksempel hadde en institusjon justert på rolle- og

[50] 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 hvorvidt tiltaksaktiviteten samsvarer med de sårbarhetene som det ble opplyst om. Kapasitet er her målt som økningen i antallet årsverk fra 2022 til 2023, hvor ett årsverk er regnet som ett tiltak.

ansvarsfordelingen for å kompensere for redusert stillingsandel for høgskolens personvernombud. Det er derfor mulig at samsvaret mellom disse tiltaks- og sårbarhetstypene påvirkes av denne typen endringer.

Det er et samsvar mellom vurderingen av tekniske sårbarheter og mengden tekniske tiltak. Antallet tekniske tiltak som ble rapportert økte i 2023, noe som gjenspeiler sårbarhetsbildet institusjonene oppga. For kompetanse og bevissthet ble det rapportert om gjennomførte tiltak som ligger tett opp mot vurderingen av denne typen sårbarheter.

Samlet vurdering og forbehold

Fjorårets vurdering oppga et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak, og viste til en trend fra tidligere kartlegginger. Årets kartlegging viser at tiltakene som institusjonene iverksatte i 2023 var mer treffsikre enn tidligere. Dette indikerer at institusjonene i større grad har iverksatt tiltak som er tilpasset de manglene (sårbarhetene) som universitetene og høgskolene mener påvirker deres arbeid med informasjonssikkerhet og personvern.

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 totalt 325 rapporterte tiltakene i 2023.

Forbedringer og status

Neste spørsmål er om institusjonenes tiltak i 2023 hadde effekt på arbeidet med informasjonssikkerhet og personvern – har institusjonene forbedret sin etterlevelse av kravene i departementets policy sammenlignet med fjoråret?[51]

Vurdering av forbedring og status

Vurderinger av status og forbedring 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 digitale verdier

(ii) tiltak for å gjenopprette normal drift etter større sikkerhetsbrudd (beredskap/kontinuitet)

(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

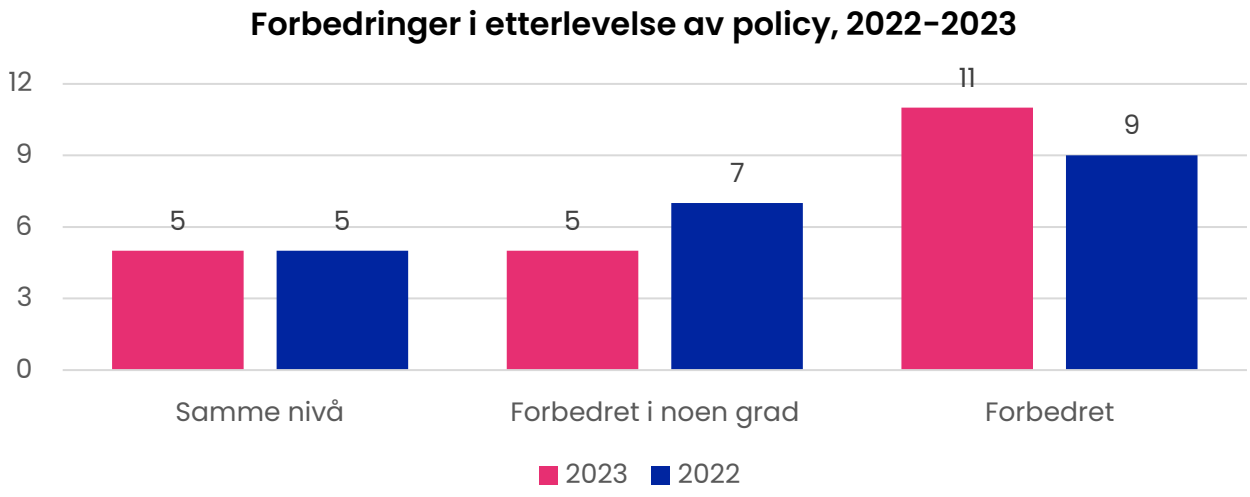
(iii) tiltak for økt bevissthet og kompetanse om reglene i personopplysningsloven og personvernforordningen, og hvordan reglene kan etterleves.

I tillegg legges det særlig vekt på hvor langt arbeidet med innføring av en helhetlig internkontroll for GDPR var kommet (jf. artikkel 24 i personvernforordningen).

[51] Se «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». F-04-20 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning - regjeringen.no. Sist besøkt 12.03.2024.

Forbedret etterlevelse på enkeltområder

Figuren oppsummerer våre vurderinger av forbedringer eller mangelen på forbedringer i etterlevelsen av kravene i departementets policy fra 2022 til 2023. Vurderingene gjelder både informasjonssikkerhet og personvern.



Figur 9 - Forbedringer i etterlevelse av policy, 2022-2023

Vår vurdering er at 16 av 21 universiteter og høgskoler hadde forbedret sin etterlevelse av departementets policy fra 2022 til 2023. Hos 11 av disse 16 institusjonene var forbedringene tydeligere enn hos de øvrige institusjonene, mens fem av dem hadde forbedret seg i noen grad.

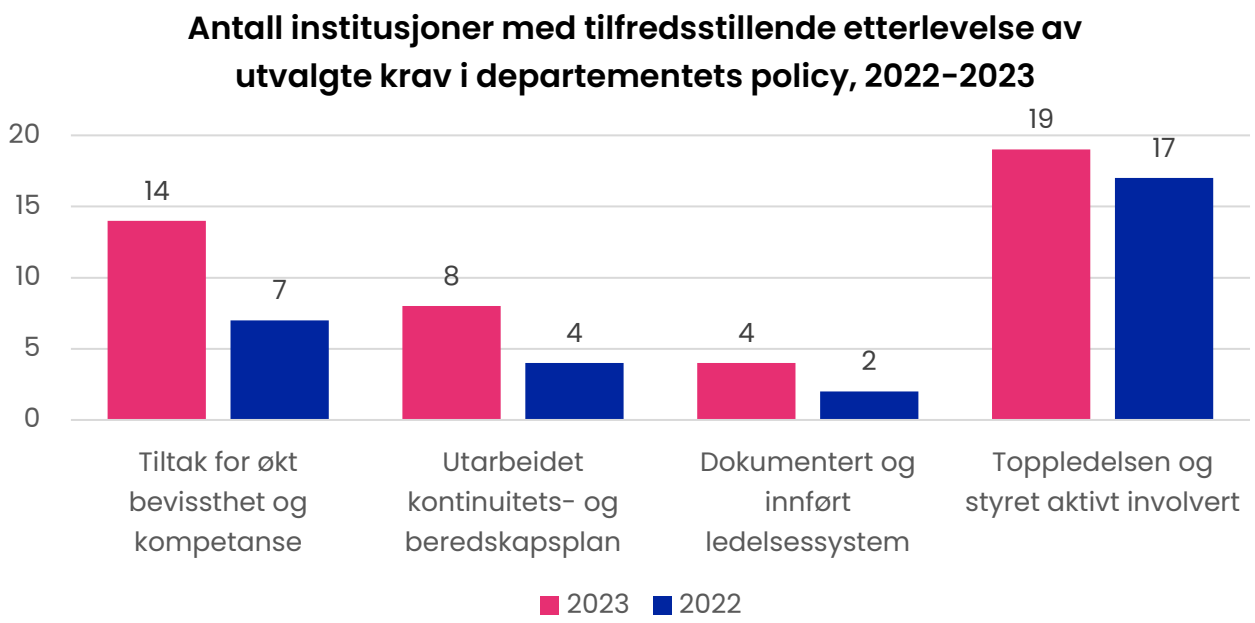
De fem siste institusjonene hadde verken forbedret eller svekket sin etterlevelse av kravene i policyen – de befant seg på omtrent samme nivå som i 2022.

Forbedringene i etterlevelse av policyen synes å være jevnt fordelt mellom informasjonssikkerhet og personvern i årets kartlegging.

Forbedringstakt

Forbedringstakten – hvor mange institusjoner som forbedrer seg hvert år, var noe bedre i 2023 sammenlignet med forrige kartlegging. Forbedringen skyldtes at to institusjoner hadde flyttet seg fra «forbedret i noen grad» til «forbedret»-kategorien i 2023.

Figur 10 gir en mer detaljert oversikt over hvilke krav i policyen institusjonene hadde forbedret mest i 2023. Den viser økningen i antall institusjoner med tilfredsstillende etterlevelse av de aktuelle kravene i policyen sammenliknet med 2022.



Figur 10 - Institusjoners etterlevelse av utvalgte krav i departementets policy, 2022-2023

Figuren viser at den største utviklingen fra 2022 til 2023 har skjedd når det gjelder antallet institusjoner som etterlever kravene til bevissthet og kompetanse om personvernregelverket. Disse institusjonene har systematisert tiltak som sikrer relevant opplæring og kompetanseheving for ledere, medarbeidere og studenter om plikter og ansvar ved behandling av personopplysninger. De har også tiltak for å forbedre bevissthet om vanlige trusler mot personvernet og informasjonssikkerheten, for eksempel epostsvindel.

Videre viser figuren at antall institusjoner med tilfredsstillende etterlevelse av de kravene som stilles til beredskaps- og kontinuitetsplaner på IT-området og kriseøvelser, økte fra fire i 2022 til åtte i 2023. Disse institusjonene har etablert planverk for hvordan informasjonssikkerhetshendelser skal oppdages og håndteres, og iverksatt tiltak for å opprettholde viktige arbeidsoppgaver ved bortfall av systemer, tjenester eller datanettverk. De har også utpekt medarbeidere med særlig ansvar for disse oppgavene, som oftest i egne hendelseshåndterings-team (IRT).

Også kravene som gjelder å ha et dokumentert og innført ledelsessystem som praktiseres i alle deler av kjernevirksomheten ble etterlevd i større grad i 2023 enn året før, med en økning til fire fra to i 2022. Tilsvarende økning ser vi med hensyn til kravene om å involvere toppledelsen og styret aktivt i arbeidet med informasjonssikkerhet og personvern, som økte fra 17 i 2022 til 19 i 2023.

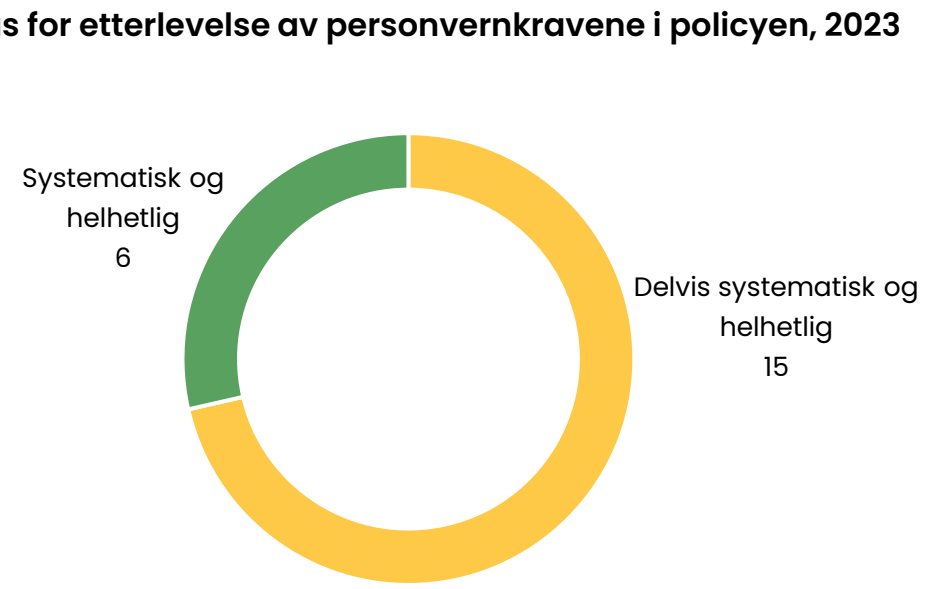
For de øvrige områdene var forbedringene mindre, og ble ikke vurdert som tilstrekkelig til å medføre oppjustering av modenhetsnivå for institusjonene.

Status – etterlevelse av kravene til personvern (GDPR)

Neste spørsmål er hvorvidt forbedringene innenfor enkeltområder skissert ovenfor hadde ført til endringer i status for den samlede etterlevelsen av personvernkravene i policyen.[52] Ga forbedringene grunnlag for

[52] Dette gjelder primært kravene i punktene 6-10 i policyen, men også punktene 11-12.

statusoppgradering av én eller flere institusjoner, det vil si at de i 2023 etterlevde samtlige personvernkrav på en tilfredsstillende måte? I figur 11 besvares dette spørsmålet.[53]



Figur 11 - Status for etterlevelse av personvernkravene i policyen, 2023

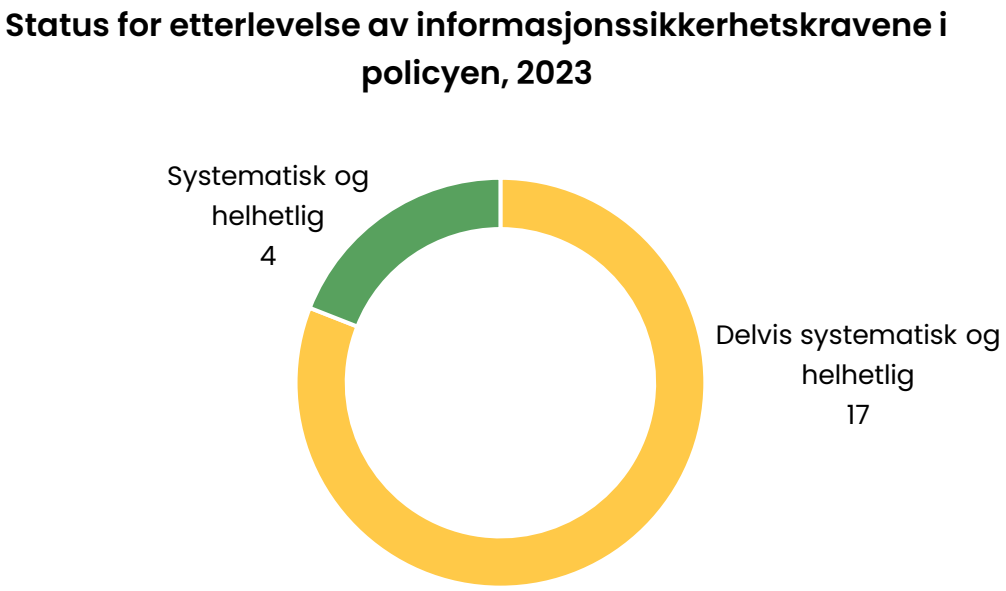
Det viktigste policyavviket hos de 15 resterende institusjonene gjaldt mangler i innføring og gjennomføring av internkontroll for behandling av personopplysninger i alle deler av kjernevirksomheten. Hos ni av disse gjensto det også noe arbeid med registrering og oversikt over behandlinger av personopplysninger.

Status – etterlevelse av kravene til informasjonssikkerhet

Figur 12 under gir en tilsvarende statusvurdering for institusjonenes etterlevelse av de særskilte kravene som departementets policy stiller til arbeidet med informasjonssikkerhet.[54]

[53] Statusvurderingen i figuren omfatter ikke krav som stilles til sikring av personopplysninger. De inngår i vurderingene av status for arbeidet med informasjonssikkerhet.

[54] Dette gjelder primært kravene i punktene 1-5 i policyen, men også punktene 11-12.



Figur 12 - Status for etterlevelse av informasjonssikkerhetskravene i policyen, 2023

Figuren viser at i 2023 hadde fire institusjoner etablert et systematisk og helhetlig informasjonssikkerhetsarbeid som ivaretar de relevante kravene i departementets policy på en tilfredsstillende måte.[55] Dette er en økning fra fjorårets kartlegging på en institusjon.

Til tross for viktige forbedringer, hadde altså de 17 resterende institusjonene fortsatt enkelte viktige avvik fra policyens krav. Det mest gjennomgående avviket var at ledelsessystem 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.

Flere av institusjonene har også behov for å forbedre etterlevelsen av kravet om å arbeide systematisk med risikovurderinger og følge opp med nødvendige sikringstiltak. Hos disse institusjonene virker behovet å være størst på enhetsnivå, men også i fellesadministrasjonen.

Vi ser at deler av våre vurderinger er forskjellige fra funn i Riksrevisjonens rapport om informasjonssikkerhet hos 10 forskningsinstitusjoner. Riksrevisjonen fant blant annet avvik vi ikke kjente til hos enkelte institusjoners kontroll av hvorvidt sikkerhets- og personvernreglene i ledelsessystemet faktisk blir fulgt. Det ble også funnet mangler i hvordan risikovurderinger blir utført. Forskjellene i funn og vurderinger er sannsynligvis et resultat av begrensninger i metodene vi bruker.[56]

Oppfølging av anbefalinger

Iverksatte tiltak og aktiviteter kan settes i sammenheng med oppfølgingen av HK-dir sine anbefalinger til det enkelte universitet og høgskole. Anbefalingene ble formidlet i brev til den enkelte institusjon etter kartleggingen i

[55] Statusvurderingene som oppsummeres i figuren inkluderer hovedkravene som policyen stiller til sikring av personopplysninger. Vurderingene omfatter derfor viktige forhold knyttet til personvern.
[56] Se «Om begrensninger» i rapportens innledning.

fjor, og gjaldt hvilke tiltak som burde iverksettes i 2023 for å redusere sårbarheter og forbedre etterlevelsen av departementets policy for informasjonssikkerhet og personvern.

Av de totalt 69 hovedanbefalingene som HK-dir ga institusjonene, ble det rapportert om at 50 av dem enten var iverksatt eller var i ferd med å bli gjennomført. 13 anbefalinger hadde ikke blitt fulgt opp. For de seks siste hovedanbefalingene mangler vi empiri til å avgjøre om de hadde blitt iverksatt (helt eller delvis) eller ikke.[57]

Hovedanbefalinger og øvrige anbefalinger

HK-dir gir to typer anbefalinger om lukking av avvik fra kravene i departementets policy[3] til virksomhetene som er underlagt departementets styringsmodell.[2] Hovedanbefalingene adresserer de viktigste avvikene fra departementets policy, og er mer omfattende enn de øvrige anbefalingene. Disse anbefalingene handler ofte om forbedringer i gjennomføring og kontroll av arbeidsoppgaver i ledelsessystem for informasjonssikkerhet, og internkontroll for personvern (GDPR).

De øvrige anbefalingene adresserer ofte underpunktene til kravene i departementets policy hvor HK-dir vurderer at virksomheten trenger å forbedre sitt arbeid. Disse anbefalingene er derfor mindre omfattende enn hovedanbefalingene, og presumptivt enklere å gjennomføre. Eksempler på slike anbefalinger er å definere maksimalt datatap og gjenopprettelsestid i kontinuitetsplan for alvorlige informasjonssikkerhetshendelser, eller å oppdatere protokoll for behandling av personopplysninger.

[57] Det ble i tillegg gitt 144 særskilte 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 76 blitt fulgt opp (helt eller delvis). 30 anbefalinger hadde ikke blitt fulgt opp. For 38 anbefalinger mangler vi empiri til å avgjøre graden av oppfølging.

Forventninger til 2024

Tre institusjoner tilfredsstilte kravene i departementets policy både med hensyn til informasjonssikkerhet og personvern i 2023. Vi forventer at alle disse tre vil opprettholde og styrke sin policyetterlevelse i 2024.

Nedenfor vurderer vi sannsynligheten for at de øvrige institusjonene følger i fotsporene til disse institusjonene i 2024. Som i tidligere risiko- og tilstandsvurderinger, har vi delt de 18 universitetene og høgskolene inn i tre kategorier basert på hvor sannsynlig vi mener det er at de vil etterleve samtlige krav i policyen på tilfredsstillende vis i løpet av inneværende år.

Etterlevelse sannsynlig: Det er sannsynlig at en av institusjonene vil kunne etterleve samtlige krav i policyen ved utgangen av 2024. Denne institusjonen befinner seg i «grenseområdet» mellom delvis tilfredsstillelse og tilfredsstillende etterlevelse. Forutsetningen for at de skal krysse grenselinjen er at de ferdigstiller pågående prosesser, og har større fremgang i etterlevelsesarbeidet i løpet av inneværende år enn de hadde i 2022 og 2023.

Etterlevelse mulig: Det er mulig at fire andre institusjoner vil kunne etterleve samtlige krav i policyen ved utgangen av 2024. For disse institusjonene vil det imidlertid kreve betydelig fremgang i etterlevelsesarbeidet. Vi regner det derfor som mindre sannsynlig at disse institusjonene vil etterleve policyen ved utgangen av 2024 enn hva tilfelle er for institusjonen i kategorien ovenfor.

Etterlevelse lite sannsynlig: For de resterende 13 institusjonene mener vi det er lite sannsynlig at de vil kunne etterleve samtlige krav i policyen ved utgangen av 2024. Vår vurdering er derfor at disse institusjonene vil trenge noe lengre tid enn de øvrige på å oppnå tilfredsstillende etterlevelse.

Om sannsynlighetskategoriene

Vi benytter følgende sannsynlighetsverdier i vår vurdering av om institusjonene vil kunne etterleve kravene i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning:

Sannsynlig: det er mer sannsynlig enn ikke at institusjonen vil kunne overholde kravene i policyen ved utgangen av 2024 (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 2024 (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 2024 (mindre enn 30 prosent sannsynlighet).

Som beskrevet innledningsvis har årets tilstands- og risikorapport et bedre informasjonsgrunnlag enn tidligere utgaver. Undersøkelsen av sektorens utvikling i perioden fra 2018 til 2022[58] gir økt innsikt som er benyttet i vurderingen overfor. Vi har også lagt til grunn funn i kartleggingen av digital omstilling [59] som viser press på ressurser i sektoren, og Riksrevisjonens rapport[60] som peker på mangler i sektorens arbeid med informasjonssikkerhet og personvern.

[58] Rapporten «Informasjonssikkerhet og personvern i et femårsperspektiv - Utvikling i UH-sektoren 2018-2022» er tilgjengelig på HK-dir | HK-dir (hkdir.no). Sist besøkt 27.03.2024.
[59] Rapporten «Digital omstilling i UH-sektoren status, muligheter og utfordringer 2023» er tilgjengelig på HK-dir | HK-dir (hkdir.no). Sist besøkt 04.03.2024.
[60] Rapporten «Informasjonssikkerhet i forskning innenfor kunnskapssektoren» er tilgjengelig på Dokument 3:11 (2023–2024) (riksrevisjonen.no). Sist besøkt 26.03.2024.

Oppsummering og behov for tiltak

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

Ni av institusjonene hadde imidlertid styrket kapasiteten – årsverksinnsatsen – i 2023. I tillegg hadde universitetene og høgskolene gjennomført 325 andre typer informasjonssikkerhets- og personverntiltak. Her var organisatoriske tiltak den største tiltakskategorien. Deretter fulgte tekniske, pedagogiske, og juridiske tiltak.

I 2023 var det et bedre samsvar mellom rapporterte sårbarheter og iverksatte tiltak enn foregående kartlegging. Hovedårsaken til dette var at antallet tekniske tiltak hadde økt sammenlignet med forrige kartlegging.

Universitetene og høgskolene hadde styrket sin etterlevelse av kravene i departementets policy innenfor viktige enkeltområder. Det gjaldt spesielt kravene som omhandler tiltak for økt bevissthet og kompetanse, og utarbeidelse av kontinuitets- og beredskapsplaner. Vi så videre en forbedring innen etterlevelse for dokumentert og innført ledelsessystem, og toppledelsens og styrets involvering i arbeidet med informasjonssikkerhet og personvern.

I 2023 økte antallet institusjoner som etterlevde hovedkravene i policyen fra to til tre. Vi ser muligheter for at ytterlige fem institusjoner vil kunne etterleve kravene i policyen for informasjonssikkerhet og personvern innen utgangen av 2024. Det forutsetter imidlertid at disse institusjonene øker progresjonen i arbeidet. For de øvrige institusjonene er tilfredsstillende etterlevelse i løpet av 2024 lite sannsynlig.

Med bakgrunn i funnene som er diskutert i dette kapitlet mener vi at institusjonene i sektoren har behov for tiltak spesielt på to områder:

(i) Styrking av evnen til å forebygge, oppdage, og håndtere informasjonssikkerhetshendelser. Institusjonenes egen sårbarhetsvurdering viser til et behov for å styrke den tekniske sikkerheten for informasjonssikkerhet og personvern i sektoren.

(ii) Etablere periodiske dybdeundersøkelser av institusjonenes arbeid med informasjonssikkerhet og personvern for alle institusjoner. Dette kan gi innsikt i kvaliteten og effekten av institusjonenes rapporterte tiltak, og kunnskap om institusjoners etterlevelse av policyen i ulike deler av virksomheten.

I årets kartlegging var tekniske sårbarheter ved institusjonene den største kategorien som ble oppgitt. Denne sårbarhetskategorien kan omfatte både lokale forhold, som svakheter i oppbygning av nettverk eller passordkrav, men også sikkerhetshull i dataprogrammer eller operativsystemer. Tiltak som etablering av felles sjekklister, eksempelvis med utgangspunkt i NSMs grunnprinsipper, og tilbud om løsninger for intern sårbarhetsskanning kan være hensiktsmessig for å imøtekomme disse utfordringene.

Det er videre et behov for tekniske tiltak i arbeidet med å oppdage og håndtere sikkerhetshendelser, spesielt fordi lokal kapasitet og kapabilitet varierer blant institusjonene. Derfor kan fellesløsninger for logging, analyse, og varsling være hensiktsmessig.

Vi registrerer at institusjonenes arbeid med etterlevelse av policyen er omfattende og tidkrevende, og at flere institusjoner uttrykker behov for harde prioriteringer i arbeidet fremover. For å effektivisere innsatsen lokalt og på sektornivå, kan periodiske revisjoner av institusjonenes arbeid med informasjonssikkerhet og personvern bidra til at tiltak med størst effekt blir prioritert.

Kapittel 4: Øvrige virksomheter – forvaltningsorganer og selskaper

Innledning

Sju øvrige forvaltningsorganer 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).

I tillegg til å være færre, er det også vesentlige forskjeller i oppgaver, struktur og størrelse blant disse 7 virksomhetene sammenlignet med de 21 universitetene og høgskolene. Vi har derfor valgt å behandle forvaltningsorganene og selskapene i et eget kapittel. Det er likevel de samme hovedspørsmålene som drøftes for disse virksomhetene som for universitetene og høgskolene i kapittel 1- 3.

Kapitlet starter med en kort beskrivelse av informasjonsverdiene i virksomhetene. Deretter diskuteres hendelser knyttet til brudd på informasjonssikkerheten og personvernkrenkelser. Videre ser vi på hvilke sårbarheter som ble identifisert i 2023, og hvilke tiltak som ble iverksatt for å håndtere disse. Kapitelet avsluttes med en oversikt over hvordan virksomhetene har overholdt departementets policy.[61]

Oversikt over informasjonsverdier

De sju virksomhetene forvalter viktige informasjonsverdier. For eksempel forvalter Sikt sentrale sektorverdier som forskningsnettet,[62] i tillegg til andre viktige fellestjenester som for eksempel Feide. Simula forsker blant annet på kryptologi og kunstig intelligens, mens NUPI utfører forskning innen sikkerhets- og forsvarspolitiske tema. UNIS opererer i et multinasjonalt miljø på Svalbard, og forsker på blant annet biologi og geologi. NOKUT, NFR, og FEK utfører viktige forvaltningsoppgaver for UH-sektoren, og behandler personopplysninger som en del av sin virksomhet.

Fellesnevneren for virksomhetene er at de har færre informasjonsverdier – opplysninger, datamaskiner, programvare, osv. – sammenlignet med universitetene og høgskolene, men samtidig at de har mindre ressurser til arbeidet med disse forvaltningsområdene. Likevel gjør dette at utfordringen med å holde oversikt over hvilke informasjonsverdier som skal beskyttes blir mer håndterbar i denne delen av sektoren, enn hos universitetene og høgskolene.

[61] Utfyllende informasjon om status for virksomhetenes etterlevelse av departementets policy, og hvilke tiltak virksomhetene hadde iverksatt i 2022, finnes i vedlegg 5.
[62] Se Sikt sin tjenesteoversikt. https://sikt.no/tjenesteoversikt. Sist besøkt 11.03.2023.

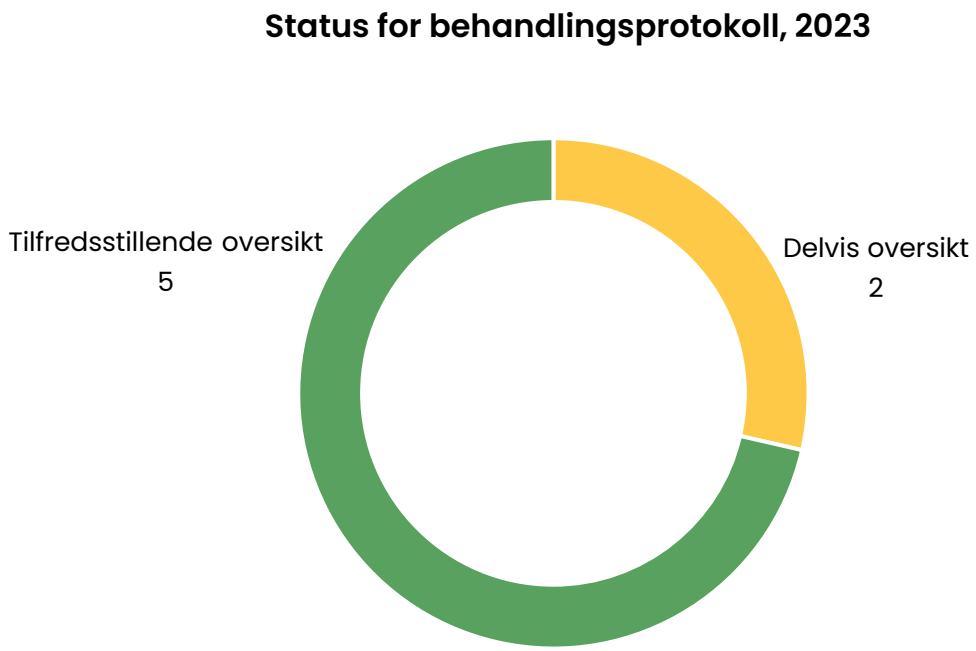
Årsrapportene til de sju virksomhetene for 2022 gir indikasjoner på at avhengigheten av digital teknologi fortsetter å øke. Sikt skriver for eksempel at kunstig intelligens og datadeling vil bli stadig viktigere i arbeidet med innovasjon og verdiskapning.[63] Samtidig uttrykker flere av virksomhetene at de økonomiske fremtidsutsiktene er mer utfordrende enn tidligere. [64]

Utviklingen som skisseres i virksomhetenes årsrapporter indikerer at de økonomiske rammene blir strammere samtidig som avhengigheten av digital teknologi øker. Den digitale utviklingen byr på nye muligheter for virksomhetene, men det blir også stadig viktigere å ha god oversikt over programvare, datamaskiner, IT-tjenester, og opplysninger som behandles i deres IT-systemer.

Behandlingsprotokoll

Personopplysningsloven og personvernforordningen (GDPR) krever at virksomhetene fører protokoll over sin behandling av personopplysninger. Behandlingsprotokollen skal blant annet gi en oversikt over hvilke typer personopplysninger som virksomheten behandler og hvem opplysningene gjelder (jf. kapittel 1).[65]

Figur 13 viser hvor mange av de sju virksomhetene som oppga at de enten har en fullstendig og oppdatert, delvis dekkende eller svært mangelfull behandlingsprotokoll.



Figur 13 - Status for behandlingsprotokoll, 2023

[63] Se Sikts årsrapport 2022, side 21-22, Arsrapport 2022 Sikt - Kunnskapssektorens tjenesteleverandør-ENDELIG (1).pdf. Sist besøkt 09.02.2024.
[64] Se for eksempel Simulas årsrapport for 2022, side 5, simula_arsrapport_2022.pdf, eller NOKUTs årsrapport for 2022, side 53, nokuts-arsrapport_2022.pdf. Sist besøkt 09.02.2024.
[65] 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 09.02.2024.

Figuren viser at fem av de sju virksomhetene rapporterte om at behandlingsprotokollen var fullstendig og oppdatert. De to siste virksomhetene oppga at protokollen ikke ga en fullgod oversikt over deres behandling av personopplysninger. Ingen opplyste om at protokollen var svært mangelfull.

Dette er en forbedring sammenliknet med resultatet fra fjorårets kartlegging, da hadde fire av virksomhetene tilfredsstillende oversikt over sin behandling av personopplysninger. I tillegg har de to virksomhetene med mangler planlagt eller iverksatt tiltak for å utbedre sine protokoller i løpet av 2024.

Andre informasjonsverdier

Virksomhetene vurderer egen oversikt over oppdatering av programvare, skytjenester, og leverandører av IT-tjenester og systemer som god. To virksomheter opplyste om at de har gjennomført og startet nye kartlegginger av sine informasjonsverdier i 2023.

En virksomhet opplyste om at de hadde styrket arbeidet med å kartlegge og behandle informasjonsverdier som er omfattet av eksportkontrollreguleringer eller internasjonale sanksjoner. Ingen av de andre virksomhetene opplyste om lignende tiltak eller kartlegginger i 2023.

Oppsummert innebærer dette at de sju forvaltningsorganene og selskapene samlet sett har bedre oversikt enn tidligere over hvilke personopplysninger de behandler og som skal beskyttes. Virksomhetene virker også å ha forbedret sin oversikt over andre informasjonsverdier enn personopplysninger noe i 2023.

Hendelser og avvik

Virksomhetene rapporterte samlet om 30 informasjonssikkerhets- og personvernhendelser i 2023. 21 var informasjonssikkerhetshendelser, mens de siste ni var avvik fra interne rutiner for håndtering av personopplysninger. Tre virksomheter hadde ikke registrert hendelser eller avvik i 2023. Det betyr at det er en nedgang på ca.50 prosent i antall hendelser fra forrige kartlegging (62). Nedgangen skyldtes hovedsakelig en reduksjon i hendelser og brudd forårsaket av menneskelige eller tekniske feil og uhell.

Vi spurte virksomhetene om de hadde merket seg endringer i hvilke type og antall forsøk på sikkerhetsbrudd fra trusselaktører i 2023. Kun en av virksomhetene oppga at de hadde registrert en slik nedgang i antall forsøk på sikkerhetsbrudd fra trusselaktører i 2023. Tre andre oppga at de ikke hadde registrert noen endring i antall forsøk på sikkerhetsbrudd, mens de tre siste ikke kommenterte dette. En virksomhet mente at forsøk på fakturasvindel utgjorde en større andel av forsøkene på sikkerhetsbrudd hos dem i 2023 enn tidligere.

Hendelsesprofilen

Det ble rapportert om de samme typene informasjonssikkerhetshendelser fra virksomhetene i 2023 som i forrige kartlegging. De fleste hendelsene skyldtes menneskelige feil og uhell, men det var også enkelte forsøk på datainntrenging og nettsvindel ved kompromittering av brukerkontoer. Ingen av forsøkene lyktes.

Ingen av virksomhetene rapporterte om mistenkt eller bekreftede forsøk på datainnbrudd eller andre hendelser som kunne knyttes til statlige eller statsstøttede trusselaktører (APT) i 2023.

Av de ni rapporterte avvikene fra interne rutiner for behandling av personopplysninger, handlet seks om avvik fra interne prosedyrer for sletting og manglende informasjon til de registrerte om behandling av personopplysninger. De tre siste bruddene handlet om manglende samtykke for publisering av et videoopptak, overføring av personopplysninger utenfor EU, og en feil hos DFØ som tilgjengeliggjorde personopplysninger for uvedkommende.

Skadevirkninger

Vi spurte virksomhetene om å vurdere hvilke skadevirkninger hendelsene og avvikene hadde ført til i 2023. To av avvikene fra interne rutiner for behandling av personopplysninger ble vurdert som alvorlige, og ble meldt til Datatilsynet. De to avvikene var feilen hos DFØ som tilgjengeliggjorde personopplysninger for uvedkommende, og publisering av et videopptak på internett uten samtykke. Utover de to avvikene førte ingen av de øvrige hendelsene eller avvikene til at virksomhetene opplevde skadevirkninger av betydning.

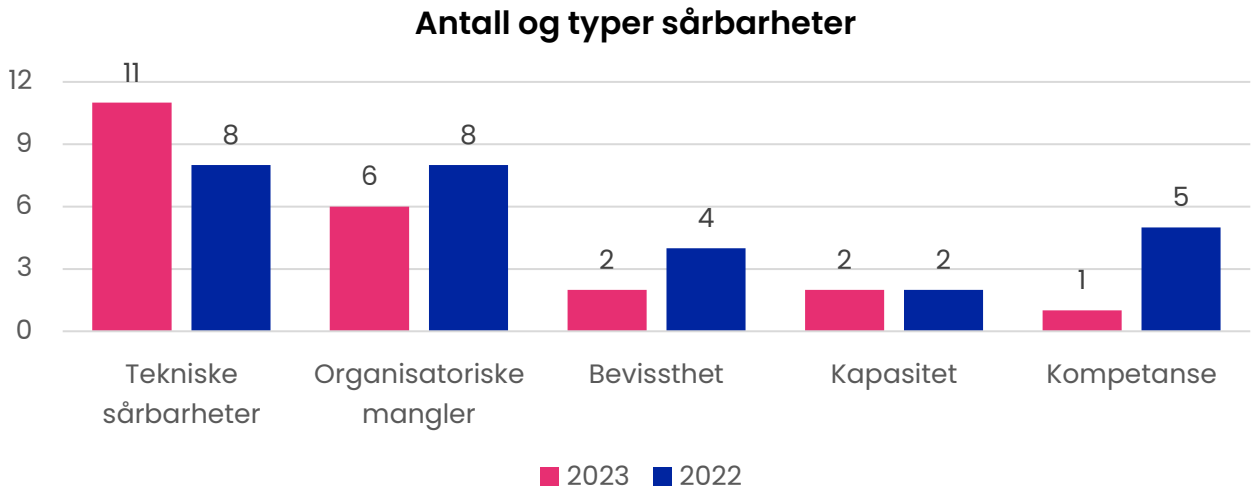
Når det gjaldt informasjonssikkerhetshendelsene ble skadevirkningene kortere avbrudd i tilgjengeligheten til IT-tjenester, og arbeidstid avsatt til håndtering av brukerkontoene som ble kompromitterte.

De øvrige avvikene fra interne rutiner for behandling av personopplysninger ble vurdert til lite alvorlige fordi de handlet om ikke-sensitive personopplysninger som ble midlertidig tilgjengelig for uvedkommende. I tillegg ble det raskt gjennomført tiltak for å rette opp feilene og hindre gjentakelse.

Sårbarheter

Brudd, hendelser, og avvik kan forårsakes av utnytelse av sårbarheter. Når en sårbarhet utnyttes, kan det resultere i krenkelser av personvernet og brudd på informasjonssikkerheten med varierende konsekvenser for enkeltpersoner og virksomheter. Brudd og hendelser kan også forårsakes av utilsiktede feil og uhell.

Figur 14 gir en samlet oversikt over sårbarhetstyper som virksomhetene rapporterte om i 2023. Stolpene viser hvor mange ganger de ulike sårbarhetstypene i tabellen ble nevnt av de sju forvaltningsorganene og selskapene.



Figur 14 - Antall og typer sårbarheter

Virksomhetene rapporterte om 27 sårbarheter som kunne føre til hendelser og brudd på informasjonssikkerheten og krenkelser av personvernet i 2023. Det er samme antall sårbarheter som ble rapportert fra denne delen av sektoren i 2022.

Figuren viser at tekniske og organisatoriske sårbarhetstyper ble vurdert som viktigst hos de syv virksomhetene i 2023. Eksempler på tekniske sårbarheter som ble nevnt var sikkerhetshull i IT-systemer, mangelfull oppdatering av utstyr og programvare, og stor grad av avhengighet til leverandører av IT-tjenester og systemer. De organisatoriske

sårbarhetene dreide seg om uklare rolle- og ansvarsfordelinger, og manglende rutiner og prosedyrer i arbeidet med informasjonssikkerhet og personvern.

Sårbarheter som dreide seg om manglende bevissthet om utfordringer i informasjonssikkerhets- og personvernarbeidet, ble vurdert som mindre viktig enn de overnevnte sårbarhetstypene. Det samme ble kapasitetsutfordringer – om arbeidsmengden knyttet til informasjonssikkerhet og ivaretakelse av personvernet oversteg tilgjengelige ressurser til å utføre oppgavene.

Den minst viktige sårbarhetstypen i 2023 var kompetanse. Det vil si at virksomhetene i liten grad opplever at ansatte har manglende ferdigheter og erfaring til å utføre de praktiske oppgavene innenfor disse forvaltningsområdene på en tilfredsstillende måte. Kun en virksomhet opplyste om denne typen sårbarhet i 2023, mot fem i 2022.

Virksomhetene vurderte rangeringen av sine sårbarhetstyper annerledes i 2023 enn i 2022. Tekniske og organisatoriske sårbarheter har byttet plass, og antallet tekniske sårbarheter er høyere i årets kartlegging enn i 2022. Kompetanse ble vurdert som den tredje mest viktige sårbarhetstypen i 2022, men er på sisteplass i 2023. Sårbarheter knyttet til manglende bevissthet og kapasitet ble vurdert relativt likt begge årene.

Kapasitetstiltak

Tre av virksomhetene oppga at de hadde styrket ressursinnsatsen som er avsatt til å arbeide med informasjonssikkerhet og personvern i 2023. De øvrige virksomhetene rapporterte at ressursinnsatsen var uendret fra 2022. Ressursinnsatsen ble derfor styrket noe i denne delen av sektoren i 2023.

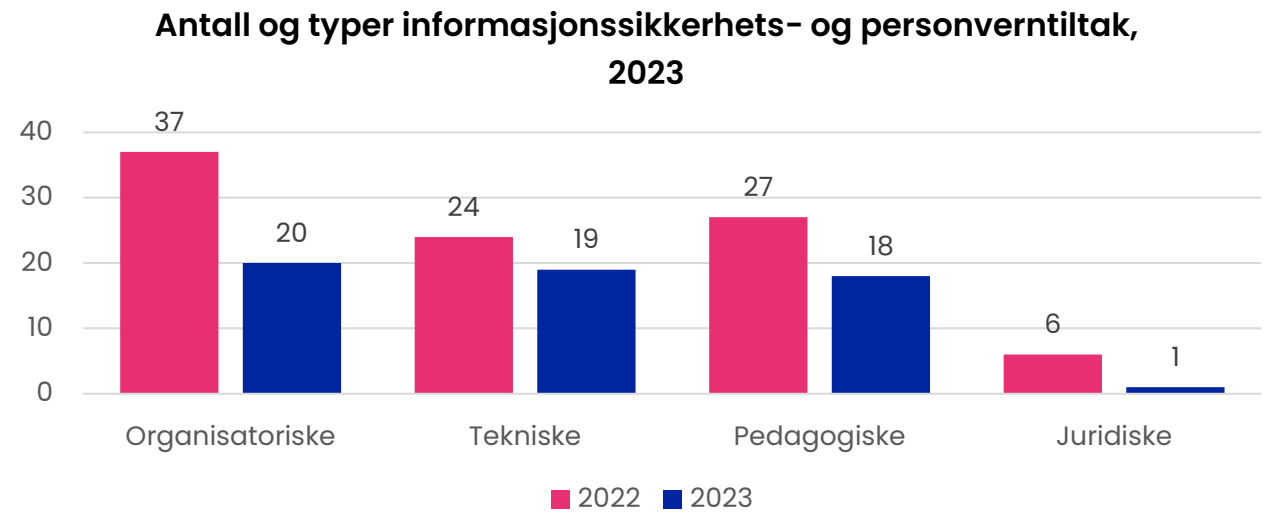
Brorparten av kapasitetsøkningen kom av nye årsverk, mens noe av kapasitetsøkningen fulgte av omprioriteringer av arbeidsoppgaver hos virksomhetene.

Andre viktige tiltak i 2023

Virksomhetene ble spurt om hvilke typer tiltak de hadde iverksatt i 2023 for å utbedre sårbarheter, og styrke arbeidet med informasjonssikkerhet og personvern.

På samme måte som med sårbarhetstyper, viser figur 15 en oversikt over hovedtyper tiltak som virksomhetene opplyste om. Stolpene viser antall ganger virksomhetene nevnte et tiltak innen de respektive tiltakstypene i møtet med HK-dir.

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



Figur 15 – Antall og typer informasjonssikkerhets- og personverntiltak, 2023

Virksomhetene rapporterte at de hadde iverksatt 58 tiltak innen arbeidet med informasjonssikkerhet og personvern i 2023. Det er en nedgang i rapporterte tiltak fra 2022 (94). I 2021 ble det rapportert om like mange tiltak som i 2023 fra denne delen av UH-sektoren.

Det ble rapportert om flest organisatoriske tiltak (20), nest flest tekniske tiltak (19), og deretter pedagogiske tiltak (18). Den klart minste kategorien var juridiske tiltak (1). Forskjellen i 2023 fra 2022 er at tekniske og pedagogiske tiltakstyper har byttet plass. Utover det er rangeringen lik som i 2022. Vi merker oss at både antallet tiltak og rangeringen av tiltakstyper er lik i 2023 og i 2021.

Tiltaksprofilen

Samtlige virksomheter hadde iverksatt organisatoriske tiltak i 2023. Tiltakene som ble gjennomført var for eksempel avklaring av roller og ansvar i ledelsessystem for informasjonssikkerhet, revisjon av behandlingsprotokoll for personopplysninger, og utarbeidelse av policy eller retningslinjer for bruk av KI-verktøy.

Alle virksomhetene hadde iverksatt minst ett teknisk tiltak i 2023. Eksempler på tekniske tiltak som ble iverksatt var utvidet bruk av totrinnsinnlogging på IT-tjenester og systemer, forbedret nettverkssegregering, penetrasjonstesting, og sårbarhetsskann av IT-systemer og tjenester som er eksponert på internett.

De pedagogiske tiltakene besto hovedsakelig av øvelser på alvorlige informasjons- og personvernhendelser, e-læringskurs, og opplærings- og bevisstgjøringstiltak som informasjonskampanjer for ansatte med arbeidsoppgaver innen personvern og informasjonssikkerhet. Alle virksomhetene gjennomførte minst ett pedagogisk tiltak i 2023.

Kun en virksomhet gjennomførte et juridisk tiltak i 2023. Tiltaket handlet om en ny gjennomgang av behandlingsprotokollen med tanke på EU-kommisjonens adekvansbeslutning for overføring av personopplysninger til USA.

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.

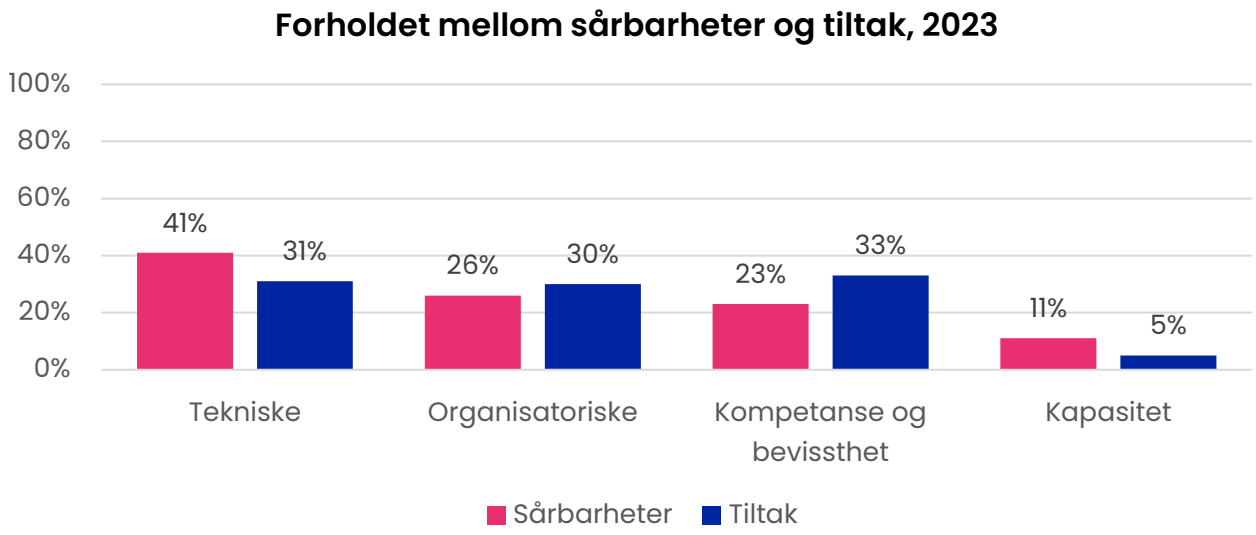
Pedagogiske tiltak: Planlegging eller iverksetting av informasjons- eller opplæringsaktiviteter. Eksempler på dette kan være informasjon på hjemmesider, kurs i risikovurderinger, grunnleggende opplæring i GDPR, utarbeidelse av veiledere eller maler, deltakelse i sikkerhetsmåneden eller gjennomføring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

Sårbarheter og tiltak

Antallet tiltak er redusert sammenlignet med forrige kartlegging, men i hvilken grad er tiltakene treffsikre sett opp mot sårbarhetene som virksomhetene rapporterte om: iverksettes det tiltak innenfor de områdene hvor virksomhetene mener de har størst utfordringer?



Figur 16 - Forholdet mellom sårbarheter og tiltak, 2023[66]

Figuren viser hvordan rapporterte tiltak fordeler seg på de ulike sårbarhetsområdene. I 2023 hadde virksomhetene iverksatt omtrent like mange tiltak på de tre største sårbarhetsområdene, men samtidig rapportert om et ujevnt antall sårbarheter. [67] Det er for eksempel rapportert om flere tekniske sårbarheter enn tiltak (10 prosentpoeng avvik). Det samme gjelder sårbarheter og tiltak innenfor kompetanse og bevissthet. Slike forskjeller indikerer at virksomhetene kan ha utbytte av å justere innretningen på flere tiltak mot områdene hvor de hadde størst utfordringer.

Ett tiltak kan virke mot flere sårbarheter, for eksempel kan økt kapasitet i IT-avdelinger føre til mer eller ny kompetanse, og samtidig bidra til å tette IT-sikkerhetshull. Det samme gjelder for sårbarheter – lav eller manglende kompetanse på hendelseshåndtering kan kreve både organisatoriske tiltak, som anskaffelse av tjenester fra en ekstern partner, og pedagogiske tiltak som kursing av egne ansatte.

Det betyr at små forskjeller mellom sårbarheter og tiltak i figuren indikerer at virksomhetene samlet sett iverksetter et proporsjonalt antall tiltak sett opp mot antallet sårbarheter. Dette er tilfellet for organisatoriske tiltak og sårbarheter (4 prosentpoeng).

Forbedringer og status – etterlevelse av kravene i departementets policy

I 2023 etterlevde tre av virksomhetene hovedkravene KDs policy for informasjonssikkerhet og personvern. Det var de samme virksomhetene som etterlevde kravene i policyen på et tilfredsstillende nivå i 2022.

I 2023 ble en virksomhet underlagt styringsmodellen vurdert til å ha tilfredsstillende etterlevelse av samtlige krav i policyen. Det betyr at i den grad denne virksomheten har avvik fra kravene i policyen, er avvikene få og vurdert som uten stor konsekvens for det helhetlige og systematiske arbeidet med informasjonssikkerhet og personvern. De to

[66] 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 2022 til 2023, hvor ett årsverk er regnet som ett tiltak.

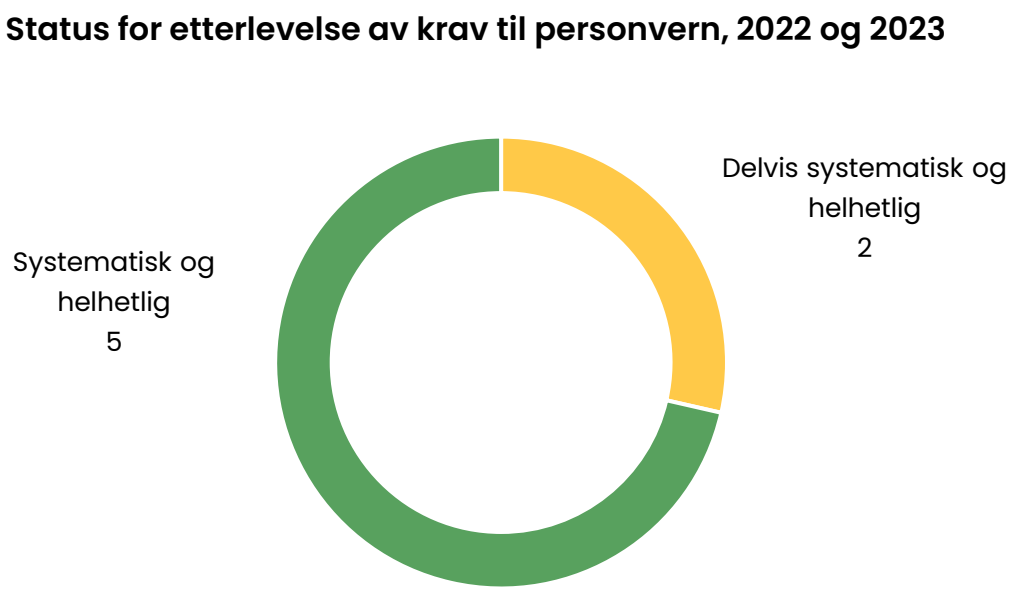
[67] Vi har utelatt det ene juridiske tiltaket fra figuren for å forbedre lesbarheten.

øvrige virksomhetene på samme modenhetsnivå har også kun enkelte mindre avvik fra kravene, men i noe større grad enn den førstnevnte virksomheten.

De fire øvrige virksomhetene har flere og viktigere avvik fra kravene i departementets policy. Vi kommer tilbake til avvikene nedenfor.

Status – etterlevelse av kravene til personvern (GDPR)

Figur 17 oppsummerer etterlevelsen av de særskilte kravene som departementets policy stiller til arbeidet med personvern (GDPR). Dette gjelder punktene 6-10 og 11-12 i policyen.[68] Figuren inneholder ikke kravene som stilles til sikring av personopplysninger, de dekkes under policyens særskilte krav til informasjonssikkerhet.



Figur 17 - Status for etterlevelse av krav til personvern, 2022 og 2023

Figuren viser at antall virksomheter som etterlever policyens krav til arbeidet med personvern (GDPR) har holdt seg på samme nivå som i 2022. Det er de samme fem virksomhetene som har tilfredsstillende etterlevelse av disse kravene som 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.

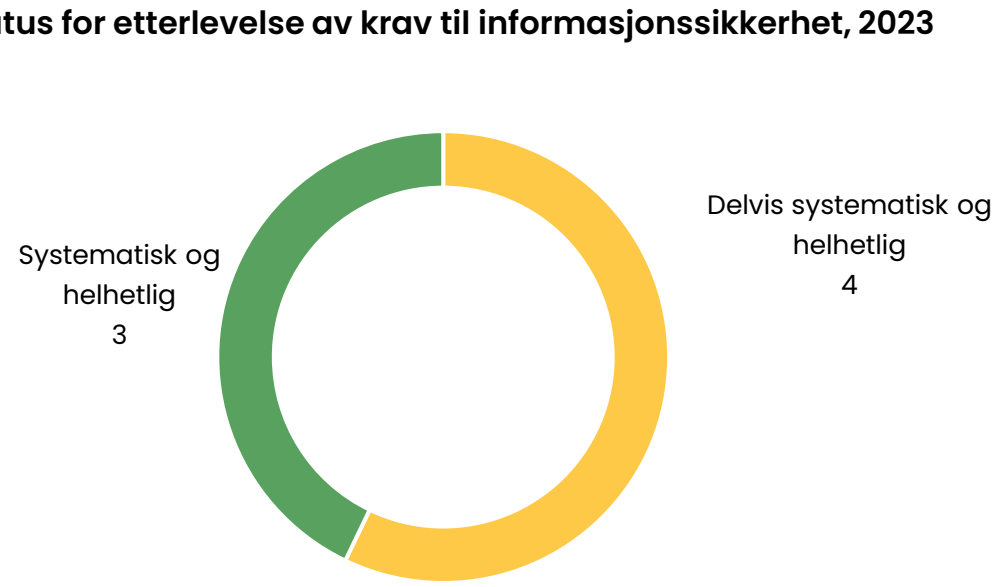
To virksomheter har en noe lavere grad av etterlevelse av disse kravene enn de øvrige fem virksomhetene. Avvikene fra policyens krav besto blant annet av mangler i gjennomføring av internkontroll for GDPR, og at de mangler en fullstendig og oppdatert protokoll for behandling av personopplysninger. Det var også mangler i arbeidet med kompetanseheving og bevisstgjøring av egne ansatte om kravene til arbeidet med personvern.

Status – etterlevelse av kravene til informasjonssikkerhet

Figur 18 oppsummerer den samlede vurderingen av de syv virksomhetenes etterlevelse av de særskilte kravene til informasjonssikkerhet i departementets policy. Dette gjelder primært krav i punktene 1-5 i policyen, men også

[68] Kriteriene for vurdering av status i figur 14 og 15 er de samme som for universitetene og høgskolene. Kriteriene er gjort rede for i kapittel 3.

punktene 11-12. Statusvurderingen i figuren omfatter også kravene som departementets policy stiller til sikring av personopplysninger.



Figur 18 - Status for etterlevelse av krav til informasjonssikkerhet, 2023

Også den samlede statusen for de særskilte kravene til informasjonssikkerhet er lik i 2023 som i 2022. Det er de samme tre virksomhetene som har tilfredsstillende etterlevelse av disse kravene i årets som i fjorårets kartlegging. Det innebærer at disse tre jobber langsiktig og planmessig med informasjonssikkerhet, prinsippet om kontinuerlig forbedring er institusjonalisert, og arbeidet har støtte fra toppledelsen, eventuelt styret.

De øvrige fire virksomhetene hadde en noe lavere etterlevelse av disse kravene. Alle fire hadde avvik fra kravene i gjennomføring og kontroll av arbeidsoppgaver tilknyttet virksomhetens ledelsessystem for informasjonssikkerhet.

Forbedringer i arbeidet med informasjonssikkerhet og personvern 2023

Selv om det fortsatt er mangler i etterlevelse av departementets policy har 6 av 7 virksomheter forbedret seg i noen grad eller helt i 2023. Av de til sammen 63 anbefalingene som virksomhetene mottok etter fjorårets kartlegging, hadde 41 blitt fulgt opp helt eller delvis. Virksomhetene hadde ikke fulgt opp 13 av anbefalingene fra HK-dir, og for ni av anbefalingene ble det ikke rapportert om grad av oppfølgning. Dette er omtrent like stor andel helt eller delvis fulgte anbefalinger som ved forrige kartlegging.

Hovedanbefalinger og øvrige anbefalinger

HK-dir gir to typer anbefalinger om lukking av avvik til virksomhetene som er underlagt departementets styringsmodell. Hovedanbefalingene adresserer de viktigste avvikene fra departementets policy, og er mer omfattende enn de øvrige anbefalingene. Disse anbefalingene handler ofte om forbedringer i gjennomføring og kontroll av arbeidsoppgaver i ledelsessystem for informasjonssikkerhet, og internkontroll for personvern (GDPR).

De øvrige anbefalingene adresserer ofte underpunktene til kravene i departementets policy hvor HK-dir vurderer at virksomheten trenger å løfte sitt arbeid. Disse anbefalingene er derfor mindre omfattende enn hovedanbefalingene, og presumptivt enklere å gjennomføre for virksomhetene. Eksempler på slike anbefalinger er å definere maksimalt datatap og gjenopprettelsestid i kontinuitetsplan for alvorlige informasjonssikkerhetshendelser, eller å oppdatere protokoll for behandling av personopplysninger.

Vi ser en sammenheng mellom forbedringene i virksomhetenes etterlevelse av departementets policy, og oppfølgningen av HK-dir sine skriftlige anbefalinger om lukking av avvik fra policyen. De fire virksomhetene som hadde forbedret seg hadde gjennomført samtlige hovedanbefalinger fra HK-dir. De tre siste virksomhetene hadde i mindre grad enn de øvrige fulgt anbefalingene til HK-dir i 2023.

Flere av virksomhetene hadde derfor forbedret seg tydelig på enkelte krav i departementets policy. Forbedringene er for eksempel innenfor risikostyring og gjennomføring av sikkerhetstiltak, protokollføring av behandlinger av personopplysninger, og tiltak for å øke bevissthet og kompetanse om disse forvaltningsområdene. Denne fremgangen vises imidlertid ikke i figurene som oppsummer virksomhetenes etterlevelse av samtlige krav i departementets policy til hverken informasjonssikkerhet eller personvern.

Forventninger til 2024

Tre virksomheter tilfredsstilte kravene i departementets policy både med hensyn til informasjonssikkerhet og personvern i 2023. Det er imidlertid muligheter for forbedring på ulike områder hos disse tre virksomhetene, men det arbeides planmessig og systematisk i alle deler av kjernevirksomheten. Vi forventer derfor at disse tre virksomhetene vil opprettholde og styrke sin policyetterlevelse i 2024.

Nedenfor vurderer vi sannsynligheten for at de øvrige virksomhetene kan etterleve kravene i departementets policy på et tilfredsstillende nivå i 2024.

Etterlevelse sannsynlig: Det er sannsynlig at ytterligere en virksomhet vil kunne etterleve samtlige krav i policyen ved utgangen av 2024. Denne virksomheten har ikke hatt vesentlig fremgang i 2023, men har opplyst om flere planlagte tiltak for 2024 som vil kunne forbedre arbeidet dersom de gjennomføres. Forutsetningen for at denne virksomheten skal krysse grenselinjen er derfor større fremgang i etterlevelsesarbeidet i løpet av inneværende år enn i 2022 og 2023.

Etterlevelse mulig: Det er mulig at to virksomheter vil kunne etterleve samtlige krav i policyen ved utgangen av 2024. For disse institusjonene vil det imidlertid kreve betydelig fremgang i etterlevelsesarbeidet.

Etterlevelse lite sannsynlig: Vi mener det er lite sannsynlig at den siste virksomheten vil kunne etterleve samtlige krav i policyen ved utgangen av 2024. Vår vurdering er derfor at denne virksomheten vil trenge noe lengre tid enn de overnevnte på å oppnå tilfredsstillende etterlevelse.

Om sannsynlighetskategoriene

Vi benytter følgende sannsynlighetsverdier i vår vurdering av om virksomhetene vil kunne etterleve kravene i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning:

Sannsynlig: det er mer sannsynlig enn ikke at virksomheten vil kunne overholde kravene i policyen ved utgangen av 2024 (mer enn 50 prosent, men mindre enn 80 prosent sannsynlig).

Mulig: det er mer usannsynlig enn sannsynlig at virksomheten vil kunne overholde kravene i policyen ved utgangen av 2024 (mer enn 30 prosent, men mindre enn 50 prosent sannsynlighet).

Lite sannsynlig: det er liten grunn til å forvente at virksomheten vil kunne overholde kravene i policyen ved utgangen av 2024 (mindre enn 30 prosent sannsynlighet).

Oppsummering og anbefalinger

De sju øvrige forvaltningsorganene og selskapene har et mindre omfattende og komplekst «verdilandskap» enn universitetene og høgskolene. Det avspeiler seg blant annet i at disse virksomhetene har relativt god oversikt over sine informasjonsverdier. Det er også positivt at arbeidet med å opprette og vedlikeholde oversikter ser ut til å ha hatt fremgang også i 2023.

I årets kartlegging er det registrert en nedgang på omtrent 50 prosent færre rapporterte brudd på informasjonssikkerheten og krenkelser av personvernet sammenlignet med forrige kartlegging. Både i 2022 og 2023 handlet slike saker i hovedsak om feil og uhell eller avvik fra egne rutiner. Samtidig ble det i 2023 registrert enkelte forsøk på datainnbrudd og fakturasvindel. Det ble ikke rapportert om bekreftet eller mistenkt statlig hacking. Heller ikke tidligere har det vært rapportert om at dette er et vesentlig problem i denne delen av UH-sektoren.

Forvaltningsorganene og selskapene rapporterte om 38 prosent færre tiltak i 2023 sammenlignet med 2022. Videre ble det rapportert om samme antall sårbarheter, og det var et større avvik i samsvaret mellom sårbarhetstypene og iverksatte tiltak enn i 2022. Samtidig har virksomhetene i stor grad fulgt opp våre skriftlige anbefalinger, og iverksatt hensiktsmessige tiltak. Forbedringene var størst med hensyn til de særskilte personvernkravene i policyen, men også når det gjaldt kravene til informasjonssikkerhet hadde det skjedd viktige forbedringer. Dette har bidratt til at seks av syv virksomheter har forbedret sin etterlevelse av kravene i departementets policy.

Kapittel 5: Risiko, mål og anbefalinger

Innledning

Tidligere rapporter har vurdert risikoen for hendelser (risikoscenarier) som kan føre til at informasjonsverdier i sektoren går tapt, skades, misbrukes eller eksponeres for uvedkommende.[69] I dette kapitlet følger en revidert og oppdatert vurdering av risikoscenariene.

Det gis også en oppdatert vurdering av om målene for informasjonssikkerhet og personvern i strategien for digital omstilling i UH-sektoren[70] kan realiseres i løpet av strategiperioden. En forutsetning for å nå målene i strategien, er tilfredsstillende etterlevelse av departementets policy for informasjonssikkerhet og personvern.[71] Graden av policyetterlevelse gir derfor en indikasjon på mulighetene for måloppnåelse.

Til slutt peker vi på områder hvor sektoren har behov for tiltak i arbeidet med informasjonssikkerheten og personvernet.

Bakgrunnen for vurdering av risiko

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

- Sektoren hadde til en viss grad forbedret sin oversikt over informasjonsverdier – opplysninger, programvare, datamaskiner, nettverksutstyr, osv. – som skal beskyttes mot trusler og håndteres i henhold til rettslige krav. Sektoren ser ut til å være på riktig kurs gjennom at flere prioriterer kartlegging av informasjonsverdier og fortsetter arbeidet med å redusere bruken av skygge-IT.
- EOS-tjenestene rapporterer om et komplekst trusselbilde. Til tross for at mengden sikkerhetstruende aktivitet kan virke redusert sammenlignet med tidligere år, er UH-sektoren på samme nivå som forsvarssektoren i NSMs oversikt over cyberhendelser siden sommeren 2022. Det varsles også om en økende cyber-trussel som følge av samarbeid mellom statlige og kriminelle aktører, i tillegg til utviklingstrekk som tyder på at sosial manipulasjon gjør det vanskeligere å forebygge, oppdage, og håndtere forsøk på svindel og datainnbrudd.
- Sektoren registrerte færre brudd på informasjonssikkerheten. Sammenlignet med foregående kartlegging rapporterte universitetene og høgskolene om en nedgang på omkring 35 prosent, og for de sju øvrige virksomhetene var nedgangen om lag 50 prosent. Nettkriminalitet utgjør den største kategorien, etterfulgt av utilsiktede menneskelige eller tekniske feil og uhell. Det var ingen i sektoren som rapporterte at hendelsene medførte alvorlige skadevirkninger, men flere av institusjonene bemerket at de ser en økning i frekvens og kvalitet på svindelforsøk. Det ble ikke rapportert om mistenkt eller bekreftet aktivitet fra statlige eller statsstøttede hackergrupper.
- Universitetene og høyskolene rapporterte om en økning på 50 prosent i antall personvernhendelser og -avvik i 2023, noe flere av institusjonene forklarte med økt bevissthet om varslingsrutiner. Antallet meldinger til Datatilsynet om brudd på personopplysningssikkerheten gikk opp over 80 prosent fra 2022 til 2023. Majoriteten

[69] Se «Risiko- og tilstandsvurdering 2023», kapittel 5. https://hkdir.no/rapportar/informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning. Sist besøkt 18.03.2024.
[70] 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 18.03.2024.
[71] 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 18.03.2024.

av økningen på 22 varsler handler om 14 rapporterte feil under innføring eller bruk av sektorens felles identitets- og tilgangsstyring, samt fem varsler fra institusjoner som var rammet av en feil hos DFØ.

- Tekniske sårbarheter ble oppgitt som den viktigste sårbarheten i sektoren, med organisatoriske mangler på andreplass. Tiltaksaktiviteten i sektoren var også i 2023 relativt høy. Det ble iverksatt flest organisatoriske, tekniske, og pedagogiske forbedringstiltak. Fordelingen av tiltakene samsvarte i større grad enn tidligere med de rapporterte sårbarhetene hvor universitetene, høgskolene og de øvrige virksomhetene selv mente at de hadde størst behov for forbedringer. Antallet årsverk øremerket for arbeidet med informasjonssikkerhet og personvern økte i 2023.
- Sektoren som helhet hadde styrket sin etterlevelse av kravene i departementets policy for informasjonssikkerhet og personvern. Dette var stort sett jevnt fordelt over sektoren, og over halvparten hadde tydelig forbedret sin etterlevelse.

Rammeverket for vurdering av risiko

Vi benytter det samme rammeverket for vurdering av risiko som i foregående risiko- og tilstandsvurderinger. Risikoscenarier – hendelser som fører til at informasjonsverdier ødelegges, går tapt, eksponeres for uvedkommende eller at personopplysninger håndteres på uforsvarlige måter – vurderes langs to dimensjoner: (i) sannsynligheten for at brudd og krenkelser skjer og (ii) mulige skadevirkninger dersom brudd og krenkelser 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.

Både sannsynlighet og skadevirkninger beror på hvor godt institusjonene og virksomhetene er i stand til å forebygge, oppdage og håndtere uønskede informasjonssikkerhets- og personvernhendelser.

Tekstboksen gir en kort forklaring til hvordan vi har operasjonalisert sannsynlighet og skadevirkninger.

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 dette er overtidsarbeid ved hendelseshåndtering, innleie av ekstern assistanse i forbindelse med hendelseshåndtering og gjenoppretting, gjenskaffe tapte data/opplysninger, gjenkjøp av IT-utstyr, overtredelsesgebyr fra Datatilsynet.
- **Omdømme og tillit**: eksempler på dette 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 får politiske følger (spørsmål til og kritikk av politisk ledelse, osv.).
- **Nasjonale interesser**: eksempler på dette er uautorisert tilgang til forskningsdata/-resultater innen områder som har betydning for nasjonale interesser, brudd på internasjonale forpliktelser, for eksempel ulovlig kunnskapsoverføring.

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

Risiko i sektoren

Gradvis forbedret oversikt over informasjonsverdier og høy tiltaksaktivitet, indikerer at risikoen i sektoren for brudd på informasjonssikkerheten og krenkelser av personvernet er noe redusert. Det har også vært en markant nedgang i antall registrerte informasjonssikkerhetshendelser de siste kartleggingene, og at ingen av hendelsene hadde alvorlige skadevirkninger peker i samme retning.

Trusselbildet er imidlertid komplekst og krevende for en sektor som legger stor vekt på åpenhet og akademisk frihet. Riksrevisjonens gjennomgang av «Informasjonssikkerhet i forskning innenfor kunnskapssektoren» avdekket manglende sikringstiltak, og demonstrerte hvordan offentlig tilgjengelig informasjon og åpne lokaler medfører sårbarheter.

Sektoren betrakter tekniske sårbarheter som viktigst i 2023, og har justert sin tiltaksaktivitet i tråd med dette. Samtidig er det utviklingstrekk som tyder på at arbeidet med å forebygge, oppdage, og håndtere informasjonssikkerhets- og personvernhendelser blir mer krevende. Flere av institusjonene ga uttrykk for at sosial manipulasjon og informasjon på deres nettsider blir benyttet i stadig mer avanserte svindelforsøk, hvilket taler for et skjerpet risikobilde.

Antallet årsverk øremerket til arbeid med informasjonssikkerhet og personvern øker i sektoren som helhet, og det benyttes ulike former for faggrupper, forum, og nettverk for å utnytte kompetanse og øke bevisstheten. Det er imidlertid tre institusjoner som har redusert antallet årsverk, og flere forteller om en presset ressurssituasjon, noe som skjerper risikobildet ytterligere.

Samlet sett er vår vurdering at disse momentene taler for at generell risiko i sektoren for brudd på informasjonssikkerheten og personvernet fortsatt er høy. Som tidligere år vil risikoen variere mellom de ulike institusjonene, og kan også være noe lavere for øvrige forvaltningsorganer og selskaper.

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.[72]

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

Scenario 1: skadevare, spesielt løsepengevirusangrep[73] – høy risiko

Vår vurdering er at risikoen for hendelser relatert til skadevare, og særlig løsepengevirus-angrep, fortsatt er høy, til tross for at ingen av institusjonene og virksomhetene rapporterte om alvorlige tilfeller av slike angrep i 2023. Det er imidlertid flere eksempler på denne typen angrep som har hatt omfattende konsekvenser mot ulike virksomheter i en rekke bransjer.[74]

I 2023 ble det rapportert om en hendelse som ble klassifisert som forsøk på løsepengevirusangrep i UH-sektoren. Dette var et tilfelle av «Rasberry Robin»-skadevare[42] hos en institusjon som ble oppdaget og håndtert. Det var ytterligere to hendelser som kan ha vært forsøk på løsepengevirus, hvor en modifisert versjon av «Cobalt Strike» ble brukt for å ta over datamaskiner.[41]

Virksomhetene i UH-sektoren har iverksatt tiltak for å forebygge, oppdage, og håndtere denne typen angrep, i tillegg til at flere rapporterte om tiltak for å begrense skadevirkningene dersom de skulle bli rammet, spesielt nye løsninger for lagring av sikkerhetskopier. Riksrevisjonens dybdeundersøkelse ved tre institusjoner avdekket imidlertid tekniske sårbarheter som kunne utnyttes, og pekte på grunnleggende tiltak som kan redusere risiko for at hendelser oppstår.

---

[72] En endring i årets kartlegging er at ingen institusjoner eller virksomheter opplyste om hendelser eller bekymringer knyttet til misbruk av lokale dataressurser. Dette risikoscenarioet er derfor utelatt fra årets risikovurdering.

[73] Løsepengevirus er skadelige programvare som kan gjøre alle datamaskiner i et datanettverk ubrukbare (innholdet på maskinene krypteres). Offeret 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.

[74] Se for eksempel «Tietoevry: full focus on final recovery steps after the ransomware attack». Tietoevry: full focus on final recovery steps after the ransomware attack – and continuous improvement in the evolving era of cybercrime. Sist besøkt 23.03.2024.

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 svært høye[75]. 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 at større løsepengevirusangrep vil medføre medieoppslag som påvirker omdømme og tilliten til enkelt-institusjoner eller til sektoren som sådan.

Scenario 2: kunnskapsspionasje (APT) – En delt sektor: høy til lav risiko

Vår vurdering er at risikoen for kunnskapsspionasje er ujevnt fordelt i sektoren, og for enkelte institusjoner og virksomheter er risikoen høy. Vi vurderer risikoen for å være lav hos flere av de mindre høgskolene. Disse institusjonene har en faglig profil som i liten grad samsvarer med kunnskapsområder som EOS-tjenestene mener kan være gjenstand for utenlandsk etterretning.

I årets kartlegging var det ingen som rapporterte om mistenkt eller bekreftet aktivitet fra statlige eller statsstøttede aktører. Dette er en videreføring av trenden fra fjorårets kartlegging hvor rapportene om slik trusselaktivitet var betydelig redusert siden kartleggingen for 2021.

Tiltakene som er iverksatt for å forebygge, oppdage, og håndtere angrep bidrar til å redusere sannsynligheten for at denne typen angrep lykkes. Sektoren jobber også med kartlegging av informasjonsverdier som er underlagt eksportkontroll, og dette vil kunne redusere skadevirkningene av vellykkede forsøk.

Vi mener likevel at risikoen for kunnskapsspionasje 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 fremvoksende teknologier og forskningsområder kan være av særlig interesse for fremmede stater.[76] Videre viser EOS-tjenestene til at samarbeidet mellom statlige og kriminelle aktører blir tettere, hvilket gjør trusselbildet mer uforutsigbart. Mangler i sikkerhetsarbeidet ble også avdekket i Riksrevisjonens revisjon av informasjonssikkerhet i forskning innenfor kunnskapssektoren.

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 (sanksjoner). Slike hendelser kan også medføre omfattende opprydningskostnader, og skade omdømme og tillit til enkelt-institusjoner og sektoren som sådan.

[75] Eksempler fra norske tilfeller finnes i «Risiko 2024», side 33.
[76] I kapittel 2 har vi sett at det kan gjelde ulike teknologier og forskningsområder, blant annet kunstig intelligens, kvantedatamaskiner, kjernefysikk, kryptografi, nanoteknologi, metallurgi, og robotikk. Også forskning knyttet til nordområdene kan være av interesse for statlige trusselaktører.

Scenario 3: utilsiktede feil og uhell – middels risiko

Vår vurdering er at det er en middels risiko i sektoren for innsidehendelser - brudd eller krenkelser som skyldes utilsiktede menneskelige eller tekniske feil og uhell (ikke fremprovosert av trussel-aktører). Denne typen hendelser fremstår som relativt vanlige, men skadevirkningene virker å være relativt begrensede.

Det ble rapportert om en økning av denne typen hendelser i 2023, noe som institusjonene til dels tilskriver bedrede rutiner og bevissthet om varsling av feil og avvik. Flertallet av saker som ble oppgitt var relatert til mindre feil som manglende avklaringer om behandlingsgrunnlag for personopplysninger, eller manglende sluttmelding i forskningsprosjekter. Det har også vært en økning i antallet saker som ble vurdert som varslingspliktige til Datatilsynet.

I årets kartlegging ble det rapportert om ulike former for menneskelige feil, typisk gjelder dette feilsending av opplysninger enten på e-post eller i arkivsystemer, lagring på områder uten tilstrekkelig adgangsbegrensning, og feilaktig publisering av opplysninger. Det har også vært flere tilfeller av hendelser og avvik relatert til tilgangsstyring, enten ved at tilganger har vært for vide, eller at tilganger ikke har vært rettidig avsluttet.

Virksomhetene har iverksatt pedagogiske og organisatoriske tiltak for å redusere sannsynligheten for utilsiktede feil og uhell, for eksempel for å øke kompetansen og øke bevisstheten om rapportering av avvik. Dette vil bidra til sikker og lovlig håndtering av personopplysninger og andre viktige informasjonsverdier, samt redusere skadevirkningene ved at slike hendelser varsles og håndteres raskere enn tidligere.

Skadevirkningene av utilsiktede feil og uhell var heller ikke i 2023 svært alvorlige. Det handlet primært om noe tapt arbeidstid ved kortere avbrudd i tjenesteleveranser og personvernkrenkelser. Det siste dreide det seg i hovedsak om at ansatte hadde fått tilgang til personopplysninger de ikke hadde tjenstlige behov for. Det var likevel snakk om mindre krenkelser – feil og uhell som rammet få personer.

Vi mener likevel at risikoen for slike hendelser fortsatt er middels fordi de fremstår som relativt hyppige, og kan medføre ikke-uvesentlige skadevirkninger.

Scenario 4: direktør- og fakturasvindel – middels risiko

Vår vurdering er at risikoen for at det utbetales større beløp som følge av direktør- eller fakturasvindel er relativt lav. Det rapporteres om økt bevissthet om direktør- og fakturasvindel, og i tillegg har effektive løsninger for deteksjon og sperring av skadelig epost ført til en reduksjon i antallet svindelforsøk som kom frem til sluttbrukere i 2023.

Samtidig har skadevirkningene av vellykket direktør- eller fakturasvindel vanligvis ikke vært veldig alvorlige i UH-sektoren.[77] Likevel er det viktig å være oppmerksom på at nettsvindel, inkludert direktør- og fakturasvindel, er en profitabel form for kriminalitet internasjonalt.[78]

Det ble ikke rapportert om alvorlige direktør- eller fakturasvindelsaker i UH- sektoren i 2023. Det var kun en institusjon som hadde registrert to tilfeller av svindel knyttet til kjøp av Apple gavekort. De oppga at i begge tilfellene var både ansatte og studenter blitt svindlet, og bemerket at angrepene viste hvordan offentlig tilgjengelig informasjon ble benyttet til å utgi seg for å være en bekjent eller kollega (såkalt «spoofing»).

[77] Det har imidlertid vært ett tilfelle i sektoren de siste årene der 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.

[78] Se for eksempel Federal Bureau of Investigation: Internet Crime Report 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. Sist besøkt 23.03.2024.

Det var imidlertid bare én av institusjonene som oppga at det hadde vært en nedgang i antall svindelforsøk, og virksomhetene utsettes kontinuerlig for forsøk på direktør- og fakturasvindel. I tillegg har flere av institusjonene rapportert om at forsøkene fremstår som mer profesjonelle og målrettede. Dermed er det fortsatt behov for årvåkenhet i sektoren når det gjelder nettsvindel generelt og direktør- eller fakturasvindel spesielt.

Scenario 5: tjenestenekt (DDoS[79]) – lav risiko

Vår vurdering er at det er lav risiko for større hendelser relatert til tjenestenektangrep i UH-sektoren. Det ble ikke rapportert om skadevirkninger relatert til denne typen angrep i årets kartlegging.

Kun en institusjon rapporterte om denne typen angrep i 2023, og da ikke mot deres egne tjenester, men mot enheter satt opp av studenter i deres nettverk. NSM oppgir at en rekke tjenestenektangrep har truffet transport-, finans-, og helsesektoren i 2023.[80]

Skadevirkningene av slike angrep kan variere noe, for eksempel at hjemmesiden er midlertidig nede, at eksamen må utsettes fordi den digitale eksamensløsningen er utilgjengelig, eller at tjenester ikke kan aksesseres på grunn av at autentiseringsløsningen er nede. Vi er ikke kjent med at tjenestenektangrep har ført til skadevirkninger av betydning i UH-sektoren de siste fem årene.

Vi mener derfor at risikoen for tjenestenektangrep mot virksomheter i UH-sektoren bør reduseres – fra middels til lav.

Risikomatrisen

Risikoen for de seks scenariene oppsummeres i risikomaterien nedenfor. Scenariene benevnes S1 – S5:

- S1 = skadevare, spesielt løsepengevirusangrep.
- S2 = kunnskapsspionasje (APT).
- S3 = utilsiktede feil og uhell.
- S4 = direktør- og fakturasvindel.
- S5 = tjenestenekt (DDoS).

Skadevirkning					
	Meget alvorlig		S2	S1	
	Alvorlig				
	Mindre alvorlig		S5	S4	S3
	Lite alvorlig				
		Svært lite sannsynlig	Lite sannsynlig	Sannsynlig	Svært sannsynlig
			Sannsynlighet		

[79] 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.
[80] «Risiko 2024», side 30.

Muligheter for måloppnåelse

Hvordan påvirker funnene i denne rapporten mulighetene for at informasjonssikkerhets- og personvernmålene i sektorens strategi for digital omstilling[81] kan realiseres?

Målene i strategien for digital omstilling

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

Det sies også at informasjonssikkerhet og personvern må prioriteres høyt i forskningsinfrastrukturer og ved deling av forskningsdata.[82] Forvaltning av data i sektoren stiller store krav til forsvarlig behandling av personopplysninger og god informasjonssikkerhet.[83] Ansatte og studenter må derfor ha god kunnskap om informasjonssikkerhet og personvern.[84]

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

Vurdering av måloppnåelse

Den økte innsikten som kommer fra gjennomgangen av sektorens utvikling i perioden 2018-2022[85], kartleggingen av sektorens digitaliseringsarbeid[86], og Riksrevisjonens undersøkelse av informasjonssikkerhet innenfor kunnskapssektoren[87], gir grunnlag for endringer i våre vurderinger av måloppnåelse sammenlignet med fjorårets risiko- og tilstandsvurdering.

Vår vurdering av måloppnåelse er derfor følgende:

- Målene om informasjonssikkerhet og personvern i strategien for digital omstilling vil trolig kunne nås hos fem av de 21 universitetene og høgskolene.

- De sju øvrige forvaltningsorganene og selskapene vil kunne oppnå strategimålene om informasjonssikkerhet og personvern.

---

[81] «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 23.03.2024.
[82] Ibid., side 19.
[83] Ibid., side 22.
[84] Ibid., side 26-29 og 32.
[85] Rapporten «Informasjonssikkerhet og personvern i et femårsperspektiv - Utvikling i UH-sektoren 2018-2022» er tilgjengelig på HK-dir | HK-dir (hkdir.no). Sist besøkt 27.03.2024.
[86] Rapporten «Digital omstilling i UH-sektoren status, muligheter og utfordringer 2023» er tilgjengelig på HK-dir | HK-dir (hkdir.no). Sist besøkt 04.03.2024.
[87] Rapporten «Informasjonssikkerhet i forskning innenfor kunnskapssektoren» er tilgjengelig på Dokument 3:11 (2023–2024) (riksrevisjonen.no). Sist besøkt 26.03.2024.

- Det er mer usikkert om de 13 siste universitetene og høgskolene vil gjøre det samme. Vi regner det som sannsynlig at disse institusjonene vil trenge lengre tid på å oppnå tilfredsstillende måloppnåelse.

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

Risikohåndtering – behov for sektortiltak

Vi mener 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 viser vi behov i sektoren på bakgrunn av funnene og konklusjonene diskutert i de tidligere kapitlene.

Scenarier med høy risiko

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

Sektoren har behov for styrking av evnen til å oppdage og registrere informasjonssikkerhetsbrudd og -hendelser. Tekniske tiltak vil kunne bidra til dette, spesielt løsninger for logging, analyse og varsling. Det er også nødvendig å kartlegge den lokale kapasiteten til dette arbeidet for å innrette hensiktsmessige sektortiltak mot institusjonene og virksomhetene med størst behov for bistand.

Informasjonsverdier

Virksomhetene i sektoren har utfordringer i arbeidet med å etablere og oppdatere behandlingsprotokoller for personopplysninger innenfor administrasjon og undervisning. Situasjonen er langt bedre når det gjelder protokoller innen forskning, som blir ivaretatt av sektortilbudet for personverntjenester i Sikt. Det fremstår derfor som hensiktsmessig å undersøke muligheten for å etablere tilsvarende tilbud for personopplysninger innen administrasjon og undervisning.

Flere institusjoner opplyste i møtene med HK-dir om at de har behov for bedre arbeidsverktøy for verdikartlegging og etablering av verdioversikter. På bakgrunn av forskjellene mellom sektorens institusjoner, både i størrelse, organisering, og faglig profil, fremstår det som vanskelig å etablere en løsning som ivaretar alles behov. Derfor virker det mer hensiktsmessig at institusjonene selv finner løsninger for verdioversikter som er tilpasset deres virksomhet.

Brudd, hendelser og sårbarheter

Sektoren har behov for å styrke evnen til å forebygge, oppdage, og håndtere informasjonssikkerhetshendelser. I institusjonenes egen sårbarhetsvurdering handler dette om behov for tekniske tiltak, og funnene i kartleggingen viser at kapasitet og kapabilitet til dette arbeidet varierer stort. Fremtidige sektortiltak på dette området bør hensynta variasjonen i mottakskapasitet, og tilby støtte til institusjoner uten tilstrekkelig kapasitet.

Flere av institusjonene varsler om press på ressurser og behov for prioriteringer av oppgaver. I enkelte tilfeller har vi sett at det gjøres organisatoriske grep for å oppnå bedre utnyttelse av ressurser. Det virker hensiktsmessig å styrke slike former for samhandling og kompetansedeling. Dette bidrar både til å utnytte ressurser og kompetanse bedre, og styrker kjennskap til prosesser og rutiner innenfor informasjonssikkerhet og personvern.

Periodiske dybdeundersøkelser

For å få innsikt effekten og kvaliteten på institusjonenes tiltak og aktiviteter, er periodiske dybdeundersøkelser et nødvendig virkemiddel. Dette vil bidra til et bedre informasjonsgrunnlag for styring, og føre til mer presise anbefalinger for arbeidet fremover.

Oppfølging av den enkelte virksomhet

Som tidligere år, vil de 28 virksomhetene motta brev fra HK-dir. I brevene gis anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern.

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 styringsmodellen for informasjonssikkerhet og personvern i UH-sektoren.

Kartleggingsmøtene med til sammen 28 virksomhetene ble gjennomført i perioden 28. oktober 2023 til 2. februar 2023.

Forberedelse og kontakt

Virksomhetene mottok brev fra HK-dir om kartlegging. Brevene til 19 første virksomhetene ble sendt ut i oktober 2023. Brevene til de siste 9 virksomhetene ble sendt ut i desember 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 seks ledere og medarbeidere. Dette var primært sikkerhets- og beredskapsledere, informasjonssikkerhetsledere eller -rådgivere, rådgivere i forskningsadministrasjonen og personvernombud.

HK-dir stilte med to eller tre deltakere.

Gjennomføring og datainnsamling

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

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

Fra to 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 mottok tilbakemeldinger – korreksjoner og utfyllende kommentarer – fra 11 virksomheter.

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

Ni av institusjonene og virksomhetene som det ble gjennomført kartleggingsmøter med i oktober og november 2023, mottok sine anbefalingsbrev i februar og mars 2024. De øvrige 18 virksomhetene mottok sine brev i april og mai 2024.

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 2022,
- 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 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 2023?
    - 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 2023?
    - 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 2023.
    - 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 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 2023 og ble vurderingene fulgt opp med nødvendige sikringstiltak?
9. Hvilke initiativ/tiltak (om noen) ble gjennomført i 2023 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 2023?
    - 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 2023?
    - Viktige initiativ/forbedringstiltak innen informasjonssikkerhet og personvern som planlegges gjennomført i 2024.
    - 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).

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.

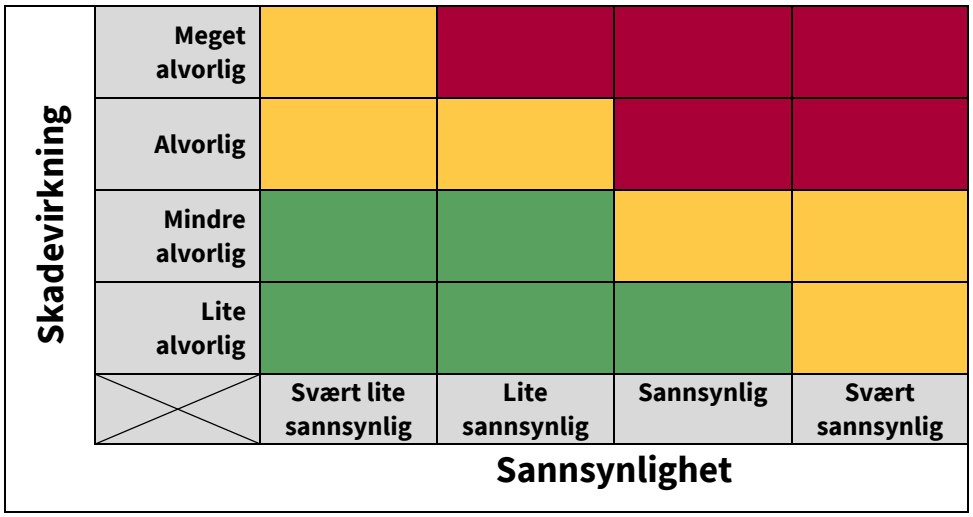
Lav risiko

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.

Figurliste

Figur 1 - Status for behandlingsprotokoll 2023, universiteter og høgskoler 14
Figur 2 - Hendelser og sårbarheter registrert hos eduCSC, 2018-2023 28
Figur 3 - Antall rapporterte personvernhendelser, 2019-2023 29
Figur 4 - Saker meldt til Datatilsynet, 2019-2023 30
Figur 5 - Institusjonenes sårbarhetsprofil, 2023 og 2022 35
Figur 6 - Endringer i årsverksinnsatsen, 2022-2023 36
Figur 7 - Informasjonssikkerhets- og personverntiltak, 2022-2023 38
Figur 8 - Samsvar mellom sårbarhetsprofil og tiltaksaktivitet, 2023 41
Figur 9 - Forbedringer i etterlevelse av policy, 2022-2023 44
Figur 10 - Institusjoners etterlevelse av utvalgte krav i departementets policy, 2022-2023 45
Figur 11 - Status for etterlevelse av personvernkravene i policyen, 2023 46
Figur 12 - Status for etterlevelse av informasjonssikkerhetskravene i policyen, 2023 47
Figur 13 - Status for behandlingsprotokoll, 2023 52
Figur 14 - Antall og typer sårbarheter 54
Figur 15 – Antall og typer informasjonssikkerhets- og personverntiltak, 2023 56
Figur 16 - Forholdet mellom sårbarheter og tiltak, 2023 58
Figur 17 - Status for etterlevelse av krav til personvern, 2022 og 2023 59
Figur 18 - Status for etterlevelse av krav til informasjonssikkerhet, 2023 60