Direktoratet for høyere utdanning og kompetanse

Risiko- og tilstandsvurdering 2022

Informasjonssikkerhet og personvern i høyere utdanning og forskning

Innhold

Sammendrag

Årets risiko- og tilstandsrapport presenterer status for og endringer i arbeidet med informasjonssikkerhet og personvern i universitets- og høgskolesektoren. Med universitets- og høgskolesektoren menes i denne sammenheng de 28 statlige universitetene, høgskolene, øvrige forvaltningsorganer og selskapene som inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[1]

Rapporten gir først en oversikt over statusen for arbeidet med informasjonssikkerhet og personvern i sektoren – hvor langt er de 28 institusjonene og virksomhetene har kommet i dette arbeidet. Statusdrøftelsene danner deretter grunnlaget for vurderinger av (i) risiko i sektoren for brudd på informasjonssikkerheten og krenkelser av personvernet, og (ii) sektorens etterleve av «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».

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

Til slutt gis enkelte anbefalinger for hvordan arbeidet med informasjonssikkerhet og personvern i sektoren kan styrkes.

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

1 Dette gjelder de 21 statlige universitetene og høgskolene, og følgende forvaltningsorganer og selskaper: Sikt, NFR, NOKUT, Simula, NUPI, FEK og UNIS. Se vedlegg 4.

Risiko for brudd og krenkelser

Vår vurdering er at den generelle risikoen i sektoren for brudd på informasjonssikkerheten og krenkelser av personvernet ikke har forandret seg vesentlig sammenliknet med forrige kartlegging. Det innebærer at risikoen fortsatt er høy når det gjelder universitetene og høgskolene. Som tidligere år, kan risikoen være noe lavere for øvrige forvaltningsorganer og selskaper.

Vi begrunner denne vurderingen med at trusselbildet i sektoren er utfordrende og at statlig hackere har økt sin trusselaktivitet rettet mot universitetene og høgskolene. Samtidig kan de tiltakene som iverksettes for å bedre informasjonssikkerheten og personvernet bli noe mer målrettede.

På den annen side har tiltaksaktiviteten i sektoren økt – flere forbedringstiltak iverksettes enn tidligere – og det ble rapportert om færre alvorlige brudd på informasjonssikkerheten og krenkelser av personvernet enn i 2020. Disse endringene gjør at vi ikke har grunnlag for å si at den generelle risikoen i sektoren har økt.

Vi har i tillegg vurdert risikoen for viktige hendelser (risikoscenarier) som kan føre til brudd på informasjonssikkerheten og krenkelser av personvernet. Disse risikoscenariene er:

1. Skadevare, spesielt løsepengevirus.
2. Statlig kunnskapsspionasje (APT).
3. Kompromitterte brukerkontoer.
4. Utilsiktede tekniske eller menneskelige feil og uhell.
5. Nettsvindel, direktør- og fakturasvindel.
6. Tjenestenektangrep (DDoS).

Vår vurdering er at risikoen for de tre første scenariene – skadevare (løsepengevirus), statlig kunnskapsspionasje og kompromitterte brukerkontoer – er høy. Dette begrunner vi med at scenariene er sannsynlige og at skadevirkningene kan bli omfattende og sammensatte.

For brudd og hendelser som skyldes utilsiktede feil og uhell (tekniske eller menneskelige) mener vi at risikoen er middels, primært fordi skadevirkningene vanligvis er mer begrensede.

Når det gjelder de to siste scenariene – nettsvindel (direktør- og fakturasvindel) og tjenestenektangrep – mener vi at risikoen er lav.

Etterlevelse av policy

Når det gjelder etterlevelsen av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern, er vår vurdering at 16 av 21 universiteter og høgskoler hadde forbedret sin etterlevelse i 2021. De øvrige institusjonene har ikke forbedret etterlevelsen vesentlig.

To institusjoner etterlevde policyen på tilfredsstillende måter i 2021. Vi mener det er sannsynlig at ytterligere fem institusjoner kan oppnå samme status i 2022. For seks andre institusjoner mener vi at tilfredsstillende etterlevelse er mulig. For de resterende institusjonene er det, slik vi vurderer det, lite sannsynlig at de vil kunne etterleve policyens krav i 2022.

De øvrige forvaltningsorganene og selskapene er generelt nærmere å etterleve policykravene enn det universitetene og høgskolene er. Vi forventer derfor at flere av disse vil kunne etterleve policyen på tilfredsstillende måter i 2022.

Oppnåelse av strategimål

Strategien for digital omstilling i UH-sektoren, 2021-2025, inneholder enkelte mål for sektorens arbeid med informasjonssikkerhet og personvern. Strategien stiller likevel ikke strengere krav til arbeidet enn det som følger av departementets policy.

Vi mener at målene i strategien i stor grad kan oppnås før strategiperiodens utløp. Vi er noe usikre på om målene kan nås for alle de åtte universitetene og høgskolene hvor etterlevelse av policyen vurderes som lite sannsynlig i 2022. Vi regner det likevel som realistisk at flertallet av disse virksomhetene vil kunne etterleve policyen og oppfylle målet i strategien innen 2025.

Anbefalinger til 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 foreslår derfor følgende sektortiltak:

1. Gjeldende sektortiltak innrettes slik at risikoen for uønskede hendelser med høy risiko (skadevare, spesielt løsepengevirus; statlig kunnskapsspionasje; kompromitterte brukerkontoer) reduseres.

2. Universitetene og høgskolene tilbys råd og veiledning om hvordan kartlegging av informasjonsverdier best kan gjennomføres, inkludert hvilke arbeidsverktøy som kan benyttes. De bør også tilbys råd og veiledning om hvordan oversikter over slike verdier bør være, spesielt innholdselementer og detaljeringsgrad.

3. Sektorens evne til å oppdage og håndtere brudd på informasjonssikkerheten og krenkelser av personvernet bør videreutvikles. Det omfatter følgende tiltak:
   - utvikling av sektordekkende analyse- og responskapasitet,
   - gjennomføring av sårbarhets- og inntrengingstesting,
   - veiledning om håndtering av IKT-hendelser,
   - kurs for operativt sikkerhetspersonell,
   - bistand til beredskaps- og kontinuitetsarbeidet,
   - tilbud om bruk av VDI.

4. Opplærings- og kompetansetiltak innen informasjonssikkerhet og personvern bør styrkes. Det omfatter følgende tiltak:
   - videreutvikle møteplassene i sektoren for informasjonsutveksling og erfaringsdeling (CISO- og personvernforum),
   - styrke rådgivings- og veiledningstilbudet,
   - tilby rådgiving og veiledning tilpasset den enkelte institusjon eller virksomhet,
   - gjennomføre revisjoner av arbeidet med informasjonssikkerhet og personvern hos den enkelte institusjon eller virksomhet,
   - styrke veiledning om innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet,
   - tilby kurs for ledere i informasjonssikkerhet og personvern.

5. Det bør stilles tydelige forventninger om ivaretakelse av krav til informasjonssikkerhet og personvern til virksomheter som leverer sektortjenester eller som forvalter rammeavtaler med sektoreksterne tjenesteleverandører.

6. Samarbeidet og informasjonsutvekslingen mellom departementet, HK-dir og Nasjonal sikkerhetsmyndighet om trusler mot informasjonssikkerheten og personvern bør videreutvikles og utdypes.

7. Det er ikke behov for egne tiltak for de sju øvrige forvaltningsorganene og selskapene. Anbefalingene som gjelder for universitetene og høgskolene vil møte behovet til disse virksomhetene.

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

Det er, etter vår vurdering, viktig at funnene i denne rapporten følges opp av Kunnskapsdepartementet i styringsdialogen med institusjonene og virksomhetene.

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 2021.

Kartleggingen ble gjennomført i perioden 8. november 2021 til 15. februar 2022. Den omfatter 28 virksomheter – 21 statlige universiteter og høgskoler, sju øvrige forvaltningsorganer og selskaper – som inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[2] Oversikt over hvem disse er finnes i vedlegg 4.

I denne rapporten presenteres funnene fra kartleggingen. Først drøftes status for og endringer i arbeidet med informasjonssikkerhet og personvern i UH-sektoren. Deretter – og med bakgrunn i statusbeskrivelsene – drøftes tre problemstillinger:

- Sektorens etterlevelse av «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».[3]
- Mulighetene for at sektoren når målene om informasjonssikkerhet og personvern i Kunnskapsdepartementets digitaliseringsstrategi.[4]
- Risikoen for konkrete uønskede hendelser som innebærer brudd på informasjonssikkerheten og krenkelser av personvernet.

Til slutt gis det anbefalinger til Kunnskapsdepartementet om sektortiltak. Anbefalingene har til hensikt å forbedre policyetterlevelsen, styrke måloppnåelsen og redusere risikoen for uønskede hendelser.

For nærmere informasjon om hvordan kartleggingen ble gjennomført, se vedlegg 1.

2 Beskrivelse av styringsmodellen finnes på https://www.unit.no/styringsmodell-informasjonssikkerhet-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

3 Policyen er fastsatt av Kunnskapsdepartementet i rundskriv F-04-20. Den ble gjort gjeldende fra 1. oktober 2020.

4 «Strategi for digital omstilling i universitets- og høgskolesektoren, 2021-2025». Se https://www.regjeringen.no/no/dokumenter/strategi-for-digital-omstilling-i-universitets-og-hoyskolesektoren/id2870981/. Sist besøkt 25.05.2022.

Kort om informasjonssikkerhet og personvern

Med informasjonssikkerhet menes vanligvis evnen til å beskytte informasjonsverdier – data, 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.[5]

Informasjonssikkerhet er et virkemiddel og ikke et mål i seg selv. Det betyr at informasjonssikkerhet kan bidra til å realisere en rekke ulike mål: effektiv forvaltning, forsvarlig saksbehandling, tilfredsstillende økonomistyring, ivareta private og offentlige interesser, osv.

Personvern handler om å unngå urettmessige inngrep i privat- og familieliv, hjem og korrespondanse, krenkelser av anseelse og den personlige integriteten. I motsetning til informasjonssikkerhet, er personvern er et mål i seg selv – det er en grunnleggende rettighet nedfelt i internasjonale konvensjoner og i den norske Grunnloven.

Personvernet skal beskyttes ved behandling av opplysninger om enkeltpersoner. Det stilles derfor egne rettslige krav til hvordan slike opplysninger skal håndteres, spesielt i personopplysningsloven og EUs personvernforordning (GDPR). Her er tanken at personvernet ivaretas ved at de som opplysningene gjelder, for eksempel studenter, har medinnflytelse over og en viss kontroll med bruken av dem.[6]

Policy, styringsdokument og strategi

Kravene som stilles til arbeidet med til informasjonssikkerhet og personvern i UH-sektoren fremgår av «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».[7] Tilsvarende forventninger følger av «Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor».[8]

Departementets policy krever at virksomhetene jobber systematisk og helhetlig med informasjonssikkerheten og personvernet. Det betyr at

i. arbeidet med informasjonssikkerhet skal være risikobasert og skje innenfor rammen av et ledelsessystem for informasjonssikkerhet, og

ii. det etableres og vedlikeholdes en internkontroll for behandling av personopplysninger som sørger for lovlig og forsvarlig håndtering av opplysningene.

Videre inneholder «Strategi for digital omstilling i universitets- og høgskolesektoren, 2021-2025» enkelte målformuleringer gjeldende informasjonssikkerhet og personvern.[9] Her fremheves informasjonssikkerhet og personvern som forutsetninger for arbeidet med digital omstilling. Målet er at utdanning, forskning, formidling og administrasjon skal utføres på sikre og tillitsvekkende måter.

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

---

5 ISO/IEC 27001: 2013: Information Technology Security Techniques. Information Security Management Systems – Requirements. Se også Audun Jøssang (2021): Informasjonssikkerhet. Teori og praksis. Oslo: Universitetsforlaget, og Håkon Bergsjø, Ronny Windvik og Lasse Øverlier (red.) (2020): Digital sikkerhet. En innføring. Oslo: Universitetsforlaget.

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

7 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 25.05.2022.

8 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 25.05.2022.

9 Se https://www.regjeringen.no/no/dokumenter/strategi-for-digital-omstilling-i-universitets-og-hoyskolesektoren/id2870981/. Sist besøkt 25.05.2022.

Innholdet i rapporten

Drøftelsene av status for og endringer i arbeidet med informasjonssikkerhet og personvern, er strukturert etter tre hovedtema:

Oversikt over informasjonsverdier
Informasjonsverdier er utgangspunktet for arbeidet med informasjonssikkerhet og personvern: det er disse verdiene som skal beskyttes mot fare, skade eller 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 kontroll med og oversikt over sine informasjonsverdier, drøftes i kapittel 1 (universitetene og høgskolene) og kapittel 4 (øvrige forvaltningsorganer og selskaper).

Trusler mot informasjonssikkerheten og personvernet
Trusler kan defineres som kilder til fare, skade eller uforsvarlig håndtering av informasjonsverdier. Eksempler på trusler er nettkriminelle grupper, statlige hackere og menneskelige feil eller uhell.

Trusler som kan føre til brudd på informasjonssikkerheten eller krenkelser av personvernet, drøftes i kapittel 2 (universitetene og høgskolene) og kapittel 4 (øvrige forvaltningsorganer og selskaper).

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

Sårbarheter som kan føre til brudd på informasjonssikkerheten og krenkelser av personvernet – og hvilke tiltak institusjonene og virksomhetene har iverksatt for å utbedre sårbarhetene – drøftes i kapittel 3 (universitetene og høgskolene) og kapittel 4 (øvrige forvaltningsorganer og selskaper).

Risiko, etterlevelse og anbefalinger

Risikoen for uønskede informasjonssikkerhets- og personvernhendelser vurderes i kapittel 5. Vurderingene av risiko bygger på drøftelsene i de foregående kapitlene.

I kapittel 5 vurderes også sektorens etterlevelse av departementets policy og mulighetene for at hovedmålene om informasjonssikkerhet og personvern i strategi for digital omstilling kan nås ved strategiperiodens utløp.

Til slutt i kapittel 5 gis anbefalinger om hvilke sektortiltak som kan iverksettes for å redusere risikoen for uønskede hendelser, styrke policyetterlevelsen og forbedre måloppnåelsen.

Om begrensninger

Denne rapporten bygger primært på informasjon innhentet i møter med den enkelte virksomhet, dokumentasjon publisert på virksomhetenes hjemmesider og offentlig tilgjengelig informasjon om trusler mot informasjonssikkerheten og personvernet (se vedlegg 1). Ut over den informasjonen som er publisert på virksomhetenes hjemmesider, ble det ikke bedt om tilgang til annen skriftlig dokumentasjon av arbeidet med informasjonssikkerhet og personvern.

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

Hensikten med undersøkelsen har isteden vært å kartlegge (i) systematikken i arbeidet med informasjonssikkerhet og personvern hos den enkelte virksomhet, (ii) forbedringstiltak som sektoren gjennomførte i 2021, og (iii) trusler og sårbarheter som utfordrer sektorens evne til å ivareta informasjonssikkerheten og personvernet.

Vedlegg

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

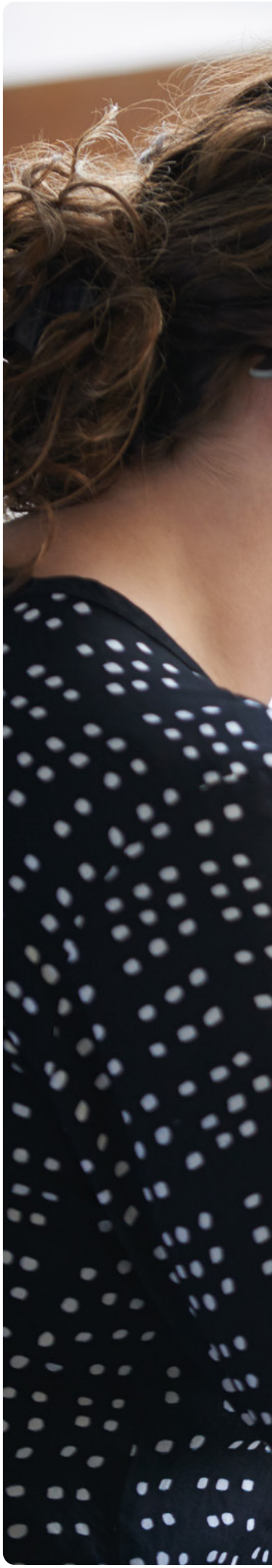
Vedlegg 2: spørsmålene (kartleggingsskjemaet) som ble benyttet i kartleggingen av universitetene, høgskolene, øvrige forvaltningsorganer og selskaper.

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

Vedlegg 4: oversikt over de 28 institusjonene og virksomhetene underlagt Kunnskapsdepartementet som omfattes av sektorstyringen innen informasjonssikkerhet og personvern.

Kapittel 1

Informasjonsverdier i UH-sektoren



Kapittel 1

Informasjonsverdier i UH-sektoren

Innledning

Utgangspunktet for arbeidet med informasjonssikkerhet og personvern er å vite hvilke informasjonsverdier som skal beskyttes og forvaltes. Med informasjonsverdier menes i denne sammenheng:

i. data og opplysninger som virksomhetene behandler, blant annet personopplysninger, forskningsdata og annen viktig informasjon, og

ii. ulike typer digitale ressurser som benyttes i behandlingen av data og opplysninger: datamaskiner, programvare, nettverksutstyr, laboratoriemaskiner, osv.

I dette kapittelet ser vi litt nærmere på de ulike informasjonsverdiene som arbeidet med informasjonssikkerhet og personvern har til hensikt å ivareta. Sektorens «verdilandskap» er sammensatt og uoversiktlig.[10] Vi kan derfor ikke gi et detaljert kart over hele landskapet.

Som tidligere år,[11] er formålet med kapitlet todelt:

- å gi en tentativ oversikt over sektorens sammensatte «verdilandskap», og
- drøfte hvordan institusjonene og virksomhetene jobber med å få oversikter over informasjonsverdiene som de forvalter.

10 Internasjonale studier indikerer at oversikt over og kontroll med informasjonsverdier er en betydelig utfordring på tvers av bransjer og sektorer. Se for eksempel https://www.helpnetsecurity.com/2022/04/15/protecting-data-challenges/. Sist besøkt 27.05.2022.

11 Se for eksempel «Risiko- og tilstandsvurdering 2021», kapittel 1. https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

«Verdilandskapet» – hovedtyper informasjonsverdier

Det finnes ingen standard måte å systematisere og kategorisere UH-sektorens informasjonsverdier på. I Ulven og Wangen (2021: 10-15) gis imidlertid en oversikt over 10 hovedtyper informasjonsverdier det vanligvis handler om.[12] Oversikten er basert på en kartlegging gjennomført ved Queensland University of Technology i Brisbane, Australia.

Hovedtyper informasjonsverdier hos universiteter og høgskoler

1. **Studentadministrasjon**. Informasjon som typisk behandles i studentadministrative systemer. Det kan blant annet være navn, fødselsnummer, bosteds- og epostadresse, tidligere utdanning, kurs og emner, semesteravgift, studieprogresjon/-poeng, tilrettelagt undervisning, praksis og eksamensresultater. Det vil også dreie seg om informasjon som behandles i elektroniske kommunikasjonsplattformer som universitetet eller høgskolen tilbyr studentene.
2. **Læring, vurdering og undervisning**. Informasjon knyttet til gjennomføring og administrasjon av undervisning og eksamen eller andre vurderingsformer. Det kan for eksempel være undervisningsplaner, emneinformasjon, pensumlister, eksamensoppgaver og -besvarelser, innleveringer, master- og bacheloroppgaver, bibliotekressurser, nettbaserte læringsressurser og informasjon som behandles om studenter og undervisere i læringsplattformer.
3. **Forskning og utvikling**. Informasjon om innholdet i, administrasjon og gjennomføringen av forskningsprosjekter. Eksempler på slik informasjon er prosjektbeskrivelser, finansiering, kontrakter, deltakere og samarbeidspartnere, datakilder, rådata, bearbeidede data, forskningsresultater, publikasjoner og kommersielle rettigheter (patenter).
4. **Medarbeidere og ledere**. Informasjon om ansettelsesforhold som blant annet behandles i HR-systemer. Det kan være navn, fødselsnummer, bostedsadresse, stilling, lønn, kontonummer, sykefravær, ferie, avspasering, opplæring/kurs, særskilt tilrettelegging, osv. Det vil også omfatte informasjon om personer som ikke er ansatt ved universitetet eller høgskolen, men som mottar godtgjøring for oppdrag, for eksempel sensorer.
5. **Økonomi og regnskap**. Informasjon om finansiering av virksomheten og forvaltning og styring av økonomiske verdier. Slik informasjon kan blant annet omhandle budsjetter på virksomhets- og enhetsnivå, årsregnskap, lønnskostnader, prosjektkostnader, bestillinger, utbetalinger og økonomirapporter.

12 Joachim Bjørge Ulven og Gaute Wangen: «A Systematic Review of Cybersecurity Risks in Higher Education». Future Internet 2021, 13, 39. https://www.mdpi.com/1999-5903/13/2/39. Sist besøkt 25.05.2022.

6. **Virksomhetsstyring og -strategi**. Informasjon om viktige forhold i virksomheten og planer for den videre administrative eller faglige utviklingen, for eksempel utviklingsavtaler med departementet. Informasjon som har betydning for styringen av virksomheten, vil ofte samles i ulike datavarehusløsninger. Dette kan omfatte økonomiske nøkkeldata, studenttall, studiepoengproduksjon, omfanget av eksternfinansiert forskning, ph.d.-programmer, midlertidighet, likestilling og kjønnsbalanse, osv.

7. **Eiendom og fysisk infrastruktur**. Informasjon om bygningsmessige forhold og andre deler av det fysiske miljøet. Det kan omfatte informasjon om campus-bygg, byggeprosjekter, laboratorier og -utstyr, heisanlegg, andre elektriske anlegg, osv. Det kan også omfatte ulike typer sensordata om det fysiske miljøet, for eksempel fra adgangskontrollen, varslingsanlegg (brann, vann, fukt), ventilasjon, oppvarming og kameraovervåking.

8. **IT-ressurser og digital infrastruktur**. Informasjon om forvaltning og styring av IT-porteføljen. Det kan inkludere informasjon om IT-anskaffelser, datamaskiner, programvare, databaser, tjenesteutsetting og databehandlere, nettverkskonfigurasjon, digital sikkerhet, tilgangsstyring og brukerstøtte.

9. **Media og kommunikasjon**. Informasjon som benyttes i det interne og eksterne formidlings- og kommunikasjonsarbeidet. Det vil for eksempel omfatte informasjon på hjemmesider, intranett og i sosiale media (Facebook, Instagram, Twitter, osv.). Det vil også inkludere informasjon om konferanser, seminarer, workshops og deltakere på slike arrangementer.

10. **Alumni**. Kontaktinformasjon til tidligere studenter og annen relevant informasjon, for eksempel påmeldinger til nyhetsbrev, arrangementer og sammenkomster.

Vår vurdering er at det i særlig grad er informasjonsverdiene i kategoriene 1-6 og 8 som er særlig kritiske. Dette er verdier som gjerne er undergitt rettslige reguleringer med hensyn til sikring og forsvarlig behandling, og som er avgjørende for å kunne gjennomføre virksomhetenes kjerneoppgaver på tilfredsstillende måter.

Disse informasjonsverdiene kan også ha stor betydning for eksterne interessenter, for eksempel deltakere i forskningsprosjekter, finansiører, samarbeidspartnere og offentlige myndigheter.

Behandlingsprotokoll – universiteter og høgskoler

I hvilken grad har institusjonene og virksomhetene i sektoren en rimelig oversikt over informasjonsverdiene i oversikten ovenfor?

Under kartleggingen i 2022 spurte vi de 21 statlige universitetene og høgskolene om dette. Vi var i første rekke opptatt av om de hadde oversikter over behandling av personopplysninger. Dette fordi det i personvernregelverket stilles krav om slike oversikter, omtalt som behandlingsprotokoller.[13] En dekkende og oppdatert behandlingsprotokoll vil derfor gi en samlet fremstilling av mange av de viktigste (mest kritiske) informasjonsverdier som institusjonene skal beskytte og håndtere på lovlig vis.

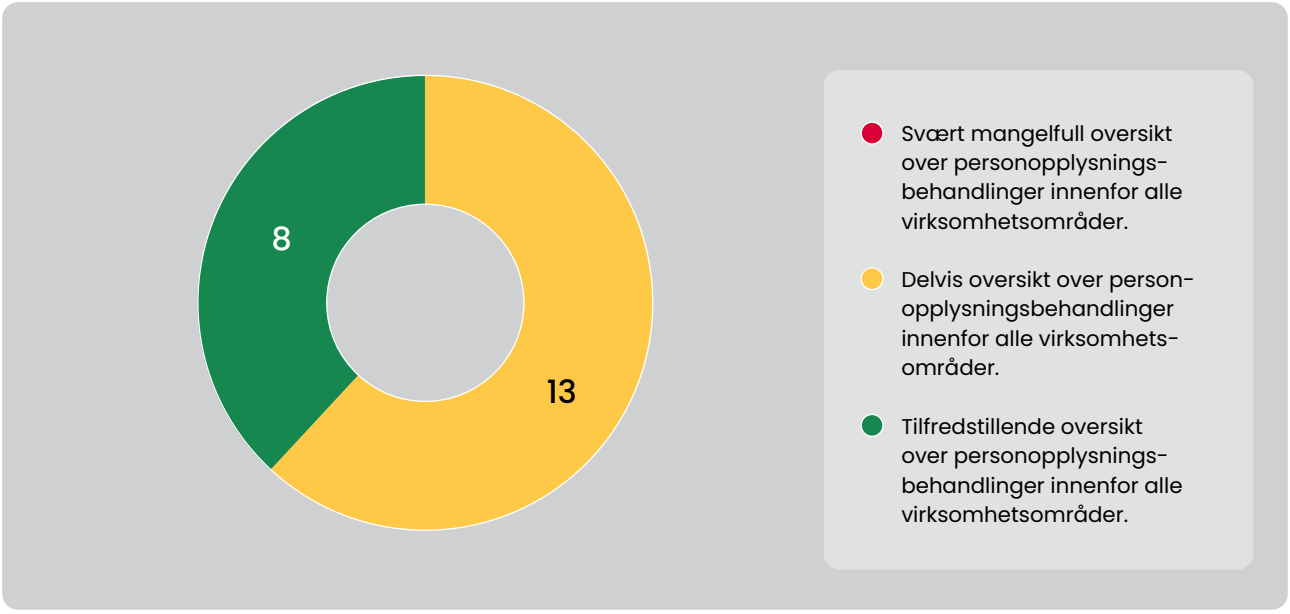
Figur 1 viser hvor mange universiteter og høgskoler som i 2021 oppga at de enten har tilfredsstillende oversikt over personopplysninger, delvis oversikt eller manglende oversikt.

Åtte av de 21 universitetene og høgskolene opplyste om at oversikten – behandlingsprotokollen – var dekkende og oppdatert innenfor undervisning, forskning, administrasjon og formidling. 13 universiteter og høgskoler opplyste om at behandlingsprotokoll var delvis dekkende og oppdatert: den var tilfredsstillende innenfor enkelte områder, men mangelfull innenfor andre. Ingen av universitetene og høgskolene oppga at protokollen var generelt mangelfull.

Institusjonenes behandlingsprotokoll var vanligvis todelt: én for forskning og én for øvrige kjerneområder. Protokollen for forskning var vanligvis Sikt sitt meldingsarkiv.[14] Dette er en fellestjeneste hvor forsknings- og studentprosjekter som behandler personopplysninger, inkludert medisinsk og helsefaglig forskning, skal registreres og evalueres før datainnsamling skjer. Prosjektene følges også opp av Sikt ved prosjektslutt, spesielt at opplysninger som ikke er anonymisert blir slettet. I hvilken grad institusjonene anvender disse oppfølgingstjenestene varierer noe. De fleste gjør det, men noen har valgt å bygge opp personvernkompetanse i forskningsadministrasjonen som ivaretar dette behovet.

I tillegg til Sikt sitt meldingsarkiv, har enkelte institusjoner utviklet egne applikasjoner for registrering og forvaltning av forsknings- og studentprosjekter hvor personopplysninger behandles. De fleste universiteter og høgskoler

Figur 1: Behandlingsprotokoll, universiteter og høgskoler



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 25.05.2022.

14 Informasjon om meldingsarkivet og øvrige personverntjenester som Sikt tilbyr, er tilgjengelig her: https://www.nsd.no/personverntjenester/. Sist besøkt 25.05.2022.

oppga imidlertid at de ikke har egne løsninger for registrering av nøkkelinformasjon om denne typen forskning.

Innenfor de øvrige kjerneområdene tilbys ikke en tilsvarende fellestjeneste for registrering og oppfølging av personopplysningsbehandling. Institusjonene må derfor finne sine egne løsninger, vanligvis i form av Excel-ark eller kommersielt tilgjengelige protokollverktøy. Ifølge institusjonene selv, er konsekvensen av denne «alenegangen» at oversikten over personopplysninger i undervisning, administrasjon og formidling er noe mer mangelfull enn for forsknings- og studentprosjekter.

Det betyr ikke at kunnskapen om hvilke personopplysninger (eller andre informasjonsverdier) som behandles er fraværende – den finnes på system-, tjeneste- eller prosessnivå. Utfordringen er å aggregere opp lokale oversikter til et samlet bilde av «det institusjonelle verdilandskapet», slik universitetene og høgskolene har muligheter for når det gjelder forsknings- og studentprosjekter.[15]

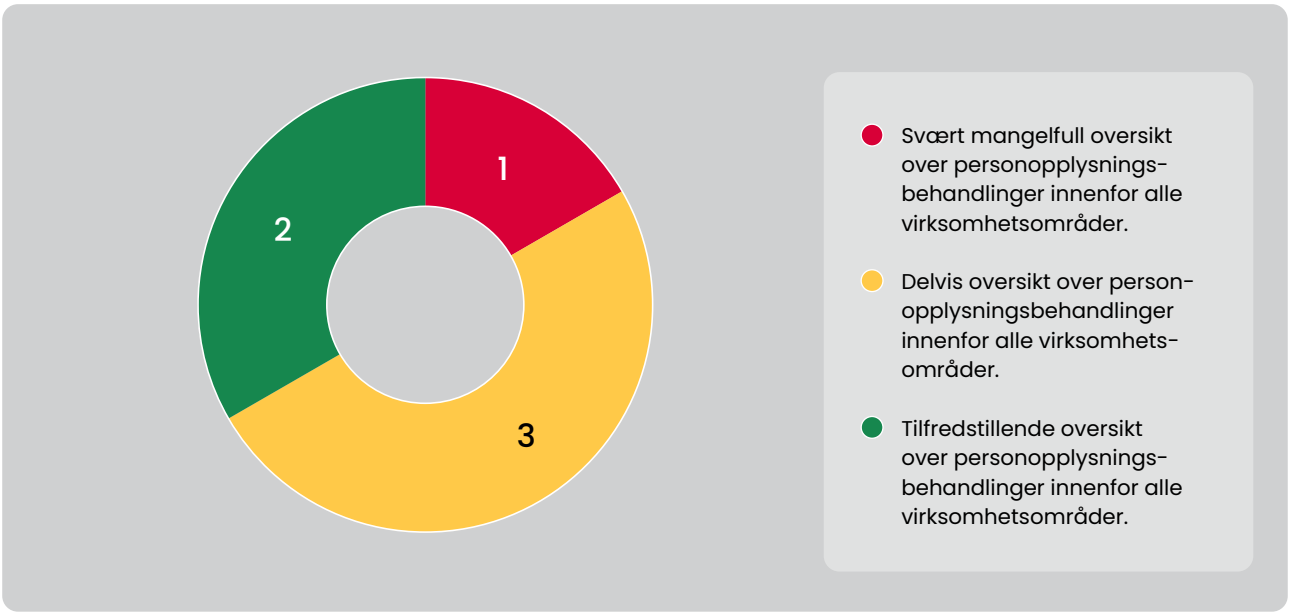
Behandlingsprotokoll – øvrige forvaltningsorganer og selskaper

Figur 2 viser status for behandlingsprotokoll hos de øvrige forvaltningsorganene og selskapene som omfattes av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.

Her ser vi at to av forvaltningsorganene og selskapene rapporterte at de hadde en dekkende og oppdatert oversikt (protokoll) over behandlinger av personopplysninger innenfor sine kjerneområder. Ytterligere tre virksomheter opplyste om at behandlingsprotokollen var delvis dekkende og oppdatert. Én av virksomhetene hadde generelt mangelfull protokoll.

Som universitetene og høgskolene, opplyste flere av disse virksomhetene om utfordringer knyttet til oppdatering og forvaltning av behandlingsprotokollen. Hos enkelte av virksomhetene fremsto derfor protokollen som noe fragmentert.

Figur 2: Behandlingsprotokoll, øvrige forvaltningsorganer og selskaper



15 Det ble også meldt om utfordringer knyttet til bruk av «skygge-IT». Dette er primært nettbaserte tjenester som ansatte tar i bruk uten at institusjonen er kjent med det. Behandlinger av personopplysninger ved bruk av «skygge-IT» blir ikke registrert i behandlingsprotokollen.

Andre informasjonsverdier i forskning og utvikling

I forsknings- og utviklingsaktiviteter behandles en rekke andre informasjonsverdier enn personopplysninger. Denne delen av sektorens «verdilandskap» inkluderer informasjon i form av rådata, bearbeidede data og forskningsresultater innenfor en rekke fagområder: navigasjons- og sensorteknologi, romfart og satellitteknologi, undervannsteknologi, materialteknologi, datateknologi, IT-sikkerhet og kryptografi, robotikk, biovitenskap, hav- og klimaforskning, geologi, osv. Dette er informasjonsverdier som kan ha betydning for nasjonal sikkerhet, ivaretakelse av internasjonale forpliktelser, utforming av offentlig politikk og gjennomføring av offentlige tiltak.[16] Informasjonen kan også ha betydelig kommersiell verdi.

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

Planer og anbefalinger

Vi har i begrenset grad registrert at slike oversikter finnes. Ansatser til oversikter kan finnes i enkelte fellestjenester, for eksempel Cristin.no[17] og nye tjenester som Nasjonalt vitenarkiv.[18] Det er imidlertid tvilsomt om disse tjenestene ivaretar behovet for oversikt og kontroll, spesielt når det gjelder informasjonsverdier som er undergitt særskilt regulering (se drøftelse nedenfor).

I løpet av de siste fire årene har flere institusjoner opplyst om at de planlegger å kartlegge forekomsten av andre informasjonsverdier enn personopplysninger. Vårt inntrykk er likevel at kartleggingene ofte ikke blir gjennomført som skissert. Videre har vi i brev til institusjonene anbefalt at arbeidet med å fremskaffe oversikter over slike informasjonsverdier bør styrkes. I 2020 mottok 15 av de 21 universitetene og høgskolene anbefalinger om dette. Etter kartleggingen det påfølgende året, rapporterte tre universiteter om at de hadde påbegynt arbeidet med å fremskaffe oversikter. De øvrige 12 institusjonene hadde ikke fulgt opp anbefalingene.

Utfordringen er heller ikke her at hvert enkelt forsknings- eller utviklingsprosjekt mangler oversikt over egne informasjonsverdier. Som på deler av personvernområdet, består utfordringen i å fremskaffe overordnede oversikter på virksomhetsnivå.[19]

Informasjonsverdier og sikkerhetstest

Dataressurser – datamaskiner og programvare – er sentrale informasjonsverdier i forskning og utvikling. Også disse informasjonsverdiene skal beskyttes mot skade, ødeleggelse, kompromittering og uforsvarlig håndtering.

Uninett gjennomførte i 2021 en sikkerhetstest av institusjonenes dataressurser (maskiner og programvare) som kan nås via forskningsnettet.[20] Resultatene fra testen gir ytterligere indikasjoner på

16 Hvilke forskningsområder, og dermed også hvilke informasjonsverdier, som vurderes som særskilt betydningsfulle, beskrives blant annet i «Langtidsplan for forskning og høyere utdanning 2019-2029». Her er satsningsområdene (i) hav, (ii) klima, miljø, miljøvennlig energi, (iii) fornyelse i offentlig sektor og bedre offentlige tjenester, (iv) muliggjørende og industrielle teknologier og (v) samfunnssikkerhet og samhørighet i en globalisert verden. Se https://www.regjeringen.no/no/dokumenter/meld.-st.-4-20182019/id2614131/. Sist besøkt 25.05.2022.

17 Se https://www.cristin.no/. Sist besøkt 25.05.2022.

18 Se https://www.unit.no/prosjekter/nasjonalt-vitenarkiv. Sist besøkt 25.05.2022.

19 Tilsvarende utfordringer drøftes i sluttrapport fra utredningsgruppen som, på oppdrag fra Digitaliseringsstyret for høyere utdanning og forskning, har vurdert problemstillinger og muligheter knyttet til deling og gjenbruk av forskningsdata. Se «Infrastruktur og tjenester for FAIR forskningsdata – status og forslag til videre arbeid». https://www.openscience.no/oa-i-norge/felles-infrastruktur-og-tjenester-fair-forskningsdata. Sist besøkt 25.05.2022.

20 Testen ble gjennomført i mai 2021 på oppdrag fra Unit og i samarbeid med Norsk helsenett. Uninett oppsummerer resultatene fra testen i «Rapport fra sårbarhetsskanning i UH-sektoren». HK-dir mottok rapporten 13.10.2021. I tillegg til samlerapporten, mottok HK-dir egne rapporter for hver av de 28 institusjonene og virksomhetene som var omfattet av testen.

utfordringene som institusjonene står overfor når det gjelder å etablere og oppdatere oversikter over andre informasjonsverdier i forskning og utvikling enn personopplysninger.

Vi spurte derfor institusjonene om hvordan de vurderte resultatene fra sikkerhetstesten for egen del.[21] Da fremkom det at kritiske sårbarheter som sikkerhetstesten avdekket vanligvis gjaldt datamaskiner i den faglige virksomheten. Dette var datamaskiner som inneholdt forskningsdata (eller hadde gjort det), men som vanligvis ble håndtert på siden av institusjonenes ordinære driftsregime. Enkelte av datamaskinene var ikke lenger i bruk – forskningsprosjektet var avsluttet og forskerne som drev det jobbet ikke lenger ved de aktuelle institusjonene. At sikkerhetstesten ikke avdekket flere datamaskiner i den faglige virksomheten med kritiske sårbarheter og som institusjonene manglet kontroll med, kan likevel indikere at kontrollen med dataressurser i forskning og utvikling er styrket.

En annen indikasjon på det samme er at i årets kartlegging opplyste åtte institusjoner om at det var iverksatt tiltak for å styrke oversikten over og håndteringen av forskningsdata, for eksempel innføring av klassifiserings- og lagringsguider. Fire av de åtte institusjonene hadde i tillegg gjennomført særskilte tiltak for å få oversikt over andre informasjonsverdier i forskning og utvikling enn personopplysninger.[22]

Eksportkontroll og internasjonal kunnskapsoverføring

Reglene om eksportkontroll gjelder i UH-sektoren.[23] Reglene innebærer at institusjonene må søke Utenriksdepartementet om lisens for internasjonale overføringer av kunnskap som har eller kan ha militære anvendelsesområder. Lisensplikten skal sikre at overføringer skjer i tråd med norske sikkerhets- og forsvarsinteresser, og at Norge ivaretar sine internasjonale forpliktelser.

Plikten om å søke lisens gjelder på en rekke forskningsområder hvor det i liten grad behandles personopplysninger. Eksempler er materialteknologi, biovitenskap, robotikk, informatikk og datasikkerhet, navigasjons- og sensorteknologi, kryptografi og undervannsteknologi. Men den gjelder også innen fagområder hvor det behandles betydelige mengder personopplysninger, spesielt medisinsk forskning.

Behovet for å skaffe seg oversikt over eksportregulert forskningskunnskap er ulikt fordelt i UH-sektoren: det er mindre for en del av høgskolene enn det er for mange av universitetene. Vi er derfor ikke overrasket over at det i årets kartlegging ikke ble opplyst om særskilte eksportkontrolltiltak fra høgskoledelen av sektoren.

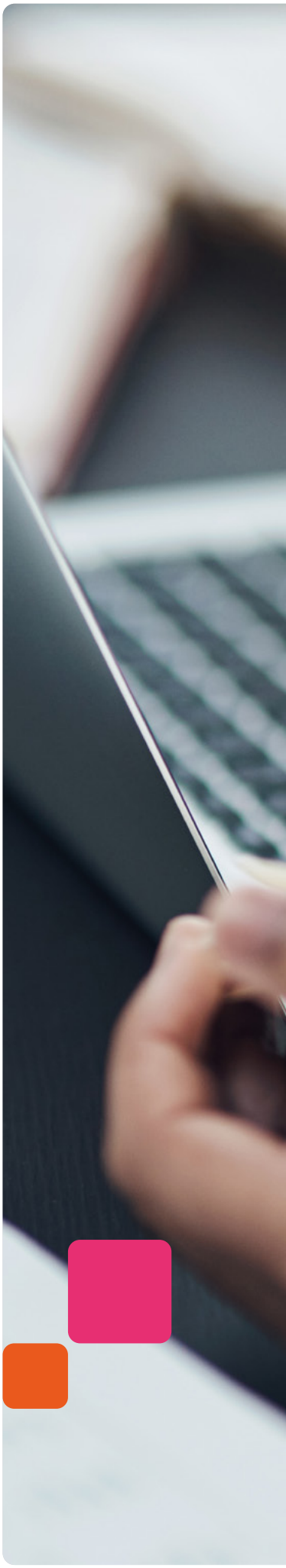
Fem universiteter opplyste imidlertid om at de har iverksatt eller planlegger tiltak for å fremskaffe oversikter over forskningskunnskap som omfattes av eksportkontrollreglene.[24] Disse institusjonene vurderte derfor eksportkontroll som et område hvor de har behov for å styrke innsatsen. Det ble i særlig grad pekt på at lokale enheter (fakulteter, institutter, osv.) ikke har god nok oversikt over kunnskapsområder som omfattes av regelverket. Ved enkelte universiteter var det opprettet egne team eller arbeidsgrupper som, sammen med lokale enheter, hadde i oppgave å kartlegge denne typen forskning og kunnskap. Andre institusjoner oppga at eksportkontroll og internasjonal kunnskapsoverføring var problemstillinger som primært ble vurdert ved ph.d.-ansettelser og ved opprettelse av nye forskningsprosjekter.

21 Testen hadde til hensikt å avdekke tekniske sikkerhetshull i datamaskiner som kan nås via internettet. Resultatene avdekket mange mindre sikkerhetshull hos universitetene, høgskolene og øvrige forskningsinstitusjoner. Den avdekket også 100 kritiske sikkerhetshull, det vil si sårbarheter med særlig stort skadepotensial dersom de utnyttes, for eksempel av nettkriminelle grupper eller statlige hacker.

22 Samtidig opplyste 15 universiteter og høgskoler om andre typer tiltak for å styrke informasjonssikkerheten og personvernet i forskning og utvikling. Ytterligere to forskningsinstitusjoner rapporterte om det samme.

23 Når dette skrives, har Utenriksdepartementet sendt endringer i reglene om eksportkontroll på høring. Se https://www.regjeringen.no/no/dokumenter/eksportkontrollforskrift/id2905352/. Sist besøkt 25.05.2022.

24 Se https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/. Sist besøkt 25.05.2022.



Oppsummering og anbefalinger

Utgangspunktet for arbeidet med informasjonssikkerhet og personvern er at institusjonene og virksomhetene har oversikt over sine informasjonsverdier. Sektoren har imidlertid enkelte utfordringer når det gjelder å fremskaffe dekkende og oppdaterte oversikter over slike verdier.

Sektoren er likevel i ferd med å etablere tilfredsstillende oversikter over behandling av personopplysninger i forskningsprosjekter og studentforskning. Det skyldes dels at personvernregelverket stiller krav om dette og dels at det er etablert en fellestjeneste hvor prosjekter som behandlinger personopplysninger skal registreres (Sikt sitt meldingsarkiv).

Innenfor andre områder, for eksempel i forskning hvor personopplysninger ikke behandles, er oversikter over informasjonsverdier noe mer mangelfulle. Hvert enkelt forskningsprosjekt har vanligvis god oversikt over sine informasjonsverdier, men det kan være vanskelig å fremskaffe dekkende og oppdaterte oversikter på virksomhetsnivå. Utfordringen vanskeliggjøres av manglende verktøystøtte.

Kartleggingstiltak iverksettes likevel av flere institusjoner på områder hvor håndtering av informasjonsverdier er undergitt rettslig regulering (eksportkontroll).

Et spørsmål som institusjonene stiller, er hvor detaljerte verdioversiktene er ment å være. Når det gjelder personopplysninger, er svaret i noen grad gitt i regelverket. Usikkerheten virker å være størst i forskning og utvikling hvor personopplysninger ikke behandles.

Mot denne bakgrunn, anbefaler vi at det iverksettes tiltak for å gi institusjonene tilfredsstillende veiledning og rådgiving om

(i) hvordan oversikter over informasjonsverdier bør være, spesielt innholdselementer og detaljeringsgrad, og

(ii) hvordan kartlegging og vedlikehold av verdioversikter best kan gjennomføres i praksis, inkludert hvilke arbeidsverktøy som kan benyttes.

Kapittel 2

Universiteter og høgskoler – brudd og hendelser

Kapittel 2

Universiteter og høgskoler – brudd og hendelser

Innledning

I hvilken grad ble sektorens informasjonsverdier utsatt for tilsiktede eller utilsiktede brudd på informasjonssikkerheten og krenkelser av personvernet i 2021? Hvor mange og hvilke typer brudd og hendelser ble registrert hos universitetene og høgskolene?

I dette kapitlet gis en oversikt over hvor mange og hvilke typer brudd og hendelser som universitetene og høgskolene rapporterte om i 2021.

Slike brudd og hendelser utløses av trusler mot informasjonsverdiene, for eksempel nettkriminelle grupper eller statlige hackere (APT[25]). Det kan også dreie seg om utilsiktede trusler, blant annet tekniske eller menneskelige feil og uhell.

Resten av kapitlet

I det følgende gis først en kort oversikt over endringer i trusselbildet nasjonalt og internasjonalt.

Deretter gis en oversikt over brudd og hendelser innen informasjonssikkerhet som de 21 universitetene og høgskolene opplyste om i 2021.

Til slutt gis en oversikt over brudd og hendelser på personvernområdet.

Brudd og hendelser

Med brudd menes tilfeller (tilsiktet eller utilsiktet) hvor informasjonsverdier faktisk ble utsatt for uautorisert tilgang, ødeleggelse, endring, sletting eller utilgjengelighet. Det omfatter også reelle krenkelser av personvernet som følge av avvik fra reglene om behandling av personopplysninger.

Med hendelser menes tilfeller (tilsiktet eller utilsiktet) hvor det har vært fare for brudd på informasjonssikkerheten, men hvor dette likevel ikke har skjedd. Det omfatter også avvik fra reglene om behandling av personopplysninger, men hvor det ikke ble rapportert om reelle krenkelser av personvernet.

25 APT kan defineres som trusselaktører som "(…) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time". https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. Sist besøkt 25.05.2022. I denne rapporten benyttes APT kun om statlige eller statsstøttede hackergrupper.

Trusselbildet nasjonalt

De siste par årene er flere norske virksomheter i privat og offentlig sektor blitt utsatt for tilsiktede brudd på informasjonssikkerheten og krenkelser av personvernet enn noen gang tidligere. Nasjonal sikkerhetsmyndighet (NSM) opplyser for eksempel om at det i perioden 2019-21 ble registrert en tredobling i antallet alvorlige digitale sikkerhetshendelser og cyberoperasjoner rettet mot norske virksomheter. Statlige eller statsstøttede hackergrupper sto, ifølge NSM, bak flere av hendelsene[26].

Også nettkriminelle grupper har gjennomført store og ødeleggende dataangrep i 2021, spesielt ved bruk av løsepengevirus. Eksempler på dette er Østre Toten kommune,[27] Helgelands Blad,[28] Nordland fylkeskommune,[29] Nortura,[30] Nordic Choice Hotels[31] og Amedia.[32]

Datainnbruddet på Stortinget i mars 2021 fikk stor medieoppmerksomhet. Da ble en sårbarhet i epostsystemet utnyttet, og innholdet i flere epostkontoer ble stjålet.[33]

EOS-tjenestene – risiko- og trusselvurderinger 2022

I sine risiko- og trusselvurderinger for 2022 fremhever EOS-tjenestene – Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E-tjenesten) – at trusselbildet i Norge er skjerpet. Det pekes på flere utviklingstrekk som utfordrer norske virksomheters evne til å håndtere trusselbildet, særlig økende avhengighet av digitale tjenester, sårbarheter i vanlig brukt maskin- og programvare, mer tjenesteutsetting av IT-drift, og lange og komplekse leverandørkjeder.

Alle de tre EOS-tjenestene mener at forskning og utvikling innen forsvar, helse og maritim teknologi kan være særlig utsatt for «cyberoperasjoner» (kunnskapsspionasje) i 2022. NSM peker i tillegg på at områder som petroleum og romteknologi kan være utsatt for slike operasjoner.[34] NSM mener at land som Russland og Kina vil være interessert i forskningsinstitusjoner med spisskompetanse innen undervannsteknologi, satellitteknologi, droner og kryptografi. Det advares mot trusselen som løsepengevirus og andre former for digital utpressing representerer.

PST mener at norsk forskning er interessante for Russland og Kina på grunn av gode finansieringsordninger, avanserte laboratorier og annen forskningsinfrastruktur.[35] Det pekes på at disse landene benytter forskningssamarbeid for å skaffe seg tilgang til teknologi og kunnskap som er undergitt eksportkontroll. I tillegg til forsvar, helse og maritim forskning, nevner PST en rekke andre områder som kan være utsatt for kunnskapstyveri, blant annet metallurgi, molekylærbiologi, nanoteknologi, datasikkerhet, IKT, sensorteknologi, robotikk og autonomi.

Som NSM og PST, mener E-tjenesten at trusselen er størst fra Russland og Kina, primært innen områder hvor landene ønsker å utvikle seg og hvor norsk forskning er ledende.[36] Det dreier seg spesielt om høyteknologi i maritim sektor. E-tjenesten viser også til at Russland, Kina og Iran anvender samarbeid med akademiske institusjoner for å skaffe seg tilgang til teknologi og kunnskap. Særlig Kina benytter egne akademiske institusjoner som verktøy for innhenting av strategisk viktig teknologi og kunnskap i utlandet.

26 Se «Risiko 2022», side 9. https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf. Sist besøkt 25.05.2022.

27 Se for eksempel https://www.nrk.no/nordland/hurtigruten-rammet-av-dataangrep-med-losepengevirus-1.15288150. Sist besøkt 25.05.2022.

28 Se for eksempel https://www.banett.no/nyheter/i/oW9npB/helgelands-blad-rammet-av-dataangrep. Sist besøkt 25.05.2022.

29 Se for eksempel https://www.nrk.no/nordland/dataangrep-rammer-nordland-fylkeskommune-1.15789412. Sist besøkt 25.05.2022.

30 Se for eksempel https://www.nationen.no/nyhet/nortura-utsatt-for-dataangrep/. Sist besøkt 25.05.2022.

31 Se for eksempel https://www.nrk.no/norge/nordic-choice-angrepet_-hackere-har-lekket-informasjon-om-ansatte-1.15773222. Sist besøkt 25.05.2022.

32 Se for eksempel https://www.nrk.no/norge/amedia-utsatt-for-alvorlig-dataangrep-1.15788535. Sist besøkt 25.05.2022.

33 Se for eksempel https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2020-2021/stortinget-utsatt-for-it-angrep/. Sist besøkt 25.05.2022 28.02.2022. Stortinget fikk i 2021 varsel om overtredelsesgebyr av Datatilsynet for et tidligere datainnbrudd. Se https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/varsel-om-overtredelsesgebyr-til-stortinget/. Sist besøkt 25.05.2022.

34 «Risiko 2022». https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf. Sist besøkt 25.05.2022.

35 «Nasjonal trusselvurdering 2022». https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf. Sist besøkt 25.05.2022.

36 «Fokus 2022». https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus-2022-til-web.pdf/_/attachment/inline/ec6bec00-d2d3-41c0-af08-02b3b494e8b7:e4014ab4d0e3bd8b2509e7974430fe121e0473ba/Fokus-2022-til-web.pdf. Sist besøkt 25.05.2022.

Ukraina-krisen

EOS-tjenestenes risiko- og trusselvurderinger ble lagt frem før Russlands invasjon av Ukraina. Men Nasjonalt cybersikkerhetssenter hos NSM mener at krisen i Ukraina fører til at risikoen for norske virksomheter er forhøyet.[37] PST vurderer det slik at etterretningstrusselen fra Russland har økt.[38] Også Datatilsynet advarer mot økt risiko for nettverksoperasjoner (digitale sikkerhetshendelser) i kjølvannet av Ukraina-krisen.[39] På den annen side, mener amerikanske myndigheter at sanksjonene mot Russland har ført til at russiske nettkriminelle grupper har problemer med å gjennomføre sine aktiviteter på samme måte som tidligere.[40]

UH-sektorens responsmiljø hos Sikt har skjerpet beredskapen mot digitale angrep i forbindelse med krisen.[41] Departementet har i brev til institusjoner og virksomheter i UH-sektoren bedt om at de gjennomgår sine kontinuitets- og beredskapsplaner for IKT-sikkerhetshendelser.[42]

Nettkriminalitet

Tidligere risiko- og tilstandsvurderinger fra Unit viser at flertallet av tilsiktede brudd på informasjonssikkerheten og krenkelser av personvernet skyldes nettkriminalitet.[43] Det er derfor relevant å se på vurderinger som gjelder denne delen av trusselbildet.

I Økokrim sin siste trusselvurdering fremheves det at den daglige kriminaliteten i stor grad preges av massebedragerier i det digitale rom, misbruk av personopplysninger og bruk av kryptovaluta som betalingsmiddel.[44] Det fremheves at en liten andel av nettkriminaliteten anmeldes til politiet og at politiet har begrensede muligheter til å oppklare denne formen for kriminalitet.[45]

De samme trendene påpekes i vurderinger på europeisk nivå.[46] Europol legger for eksempel vekt på at nettkriminelle grupper er godt organisert og innovative i sin metodebruk. Ulike former for sosial manipulasjon og skadevare vurderes som særlig alvorlige trusler. Det samme gjelder utnyttelse av sårbarheter hos leverandører av IT-systemer og -tjenester (verdikjedeangrep).

Enkelte nettkriminelle grupper har uttalt at de ikke lenger vil rette sin aktivitet mot kunnskapssektoren.[47] Det er vanskelig å vite hvor stor vekt som kan tillegges slike påståtte selvpålagte begrensninger.

---

37 Se https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/oppdatert-situasjonsbilde-fra-ncsc. Sist besøkt 25.05.2022.

38 Se https://www.pst.no/alle-artikler/pressemeldinger/oppdatert-trusselvurdering-pst-ser-en-okt-etterretningstrussel-fra-russland-i-norge/. Sist besøkt 25.05.2022.

39 https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/okt-risiko-for-nettverksangrep/. Sist besøkt 25.05.2022.

40 Se Ransomware has gone down because sanctions against Russia are making life harder for attackers | ZDNet. Sist besøkt 25.05.2022.

41 Se https://sikt.no/artikkel/okt-beredskap-etter-invasjonen-av-ukraina. Sist besøkt 25.05.2022.

42 Brev fra Kunnskapsdepartementet 1. mars 2022: «Gjennomgang av kontinuitets- og beredskapsplaner for IKT-sikkerhetshendelser».

43 Se for eksempel «Risiko- og tilstandsvurdering 2021», kapittel 3. https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

44 «Trusselvurdering 2020», side 38-47. https://www.okokrim.no/trusselvurdering-2020.6304950-411472.html. Sist besøkt 25.05.2022.

45 Forhold som påvirker politiets evne til å oppklare nettkriminalitet diskuteres i «Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT». Dokument 3:5, 2020-2021. https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-politiets-innsats-mot-kriminalitet-ved-bruk-av-ikt/. Sist besøkt 25.05.2022.

46 «Internet Organized Crime Threat Assessment 2021». https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf. Sist besøkt 25.05.2022.

47 Se for eksempel https://www.acronis.com/en-us/articles/darkside-ransomware/. Sist besøkt 25.05.2022.

Trusselbildet i kunnskapssektoren – internasjonalt

Internasjonalt ser det ut til at trusselbildet i UH-sektoren har vært relativt stabilt i 2021: det handler i hovedsak om de samme truslene som i 2020 og 2019.[48]

Det som har hatt spesielt fokus i vurderinger av trusselbildet i UH-sektoren internasjonalt, er konsekvensene av pandemihåndteringen[49] Enkelte internasjonale studier tyder på at bekymringene ikke har vært grunnløse – kunnskapssektoren har i perioder under pandemien vært mer utsatt for dataangrep og forsøk på datainntrenging enn andre sektorer.[50]

I andre og tilsvarende studier er ikke dette en like tydelig trend.[51] Heller ikke kartlegginger som Unit gjennomførte i 2021 tyder på at antallet brudd og hendelser har økt mer enn vanlig under det første pandemiåret.[52]

National Cyber Security Center (NCSC) i Storbritannia har gjennomført en egen trusselvurdering for høyere utdanning og forskning.[53] NCSC mener det er svært sannsynlig at universiteter vil være viktige mål for nettkriminelle grupper. Sannsynligheten vurderes som høy for at sektoren utsettes for statlig dataspionasje.

I 2021 har NCSC styrket sin støtte til informasjons- og personopplysningssikkerhet i høyere utdanning og forskning i Storbritannia.[54]

EDUCAUSE rangerer hvert år de viktigste IT-områdene i amerikansk UH-sektor.[55] I 2022 ble informasjonssikkerhet rangert som det viktigste området.[56] Dette er ikke noe nytt. EDUCAUSE har i flere år rangert informasjonssikkerhet som den viktigste utfordringen på IT-området i amerikansk høyere utdanning og forskning.[57]

---

48 Se «Risiko- og tilstandsvurdering 2021», kapittel 3. https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

49 Se for eksempel Kaspersky (2021): «Digital Education: the Cyberrisks of the Online Classroom». https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/03172621/education_report_04092020.pdf. Sist besøkt 25.05.2022.

50 Se for eksempel Check Point (2021): «Education Sector Sees 29 % Increase in Attacks Against Organizations Globally». https://blog.checkpoint.com/2021/08/18/check-point-research-education-sector-sees-29-increase-in-attacks-against-organizations-globally/. Sist besøkt 25.05.2022.

51 Se for eksempel Mandiant: «M-Trends 2021». https://www.mandiant.com/resources/m-trends-2021. Sist besøkt 25.05.2022.

52 Se «Temarapport 2021: Pandemihåndteringen – betydningen for informasjonssikkerhet og personvern hos universiteter og høgskoler». https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

53 National Cyber Security Center (2019): «The Cyber Threat to Universities». https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities. Sist besøkt 25.05.2022.

54 Se https://www.ncsc.gov.uk/news/support-for-uk-education-sector-after-growth-in-cyber-attacks. Sist besøkt 25.05.2022.

55 Se for eksempel EDUCAUSE (2021): «Top 10 IT Issues, 2022: The Higher Education We Deserve». https://er.educause.edu/articles/2021/11/top-10-it-issues-2022-the-higher-education-we-deserve. Sist besøkt 25.05.2022.

56 I tillegg har EDUCAUSE laget scenarioer for hvordan utfordringer knyttet til informasjonssikkerhet i høyere utdanning og forskning kan tenkes å utvikle seg. Se for eksempel «2021 EDUCAUSE Horizon Report, Information Security Edition». https://library.educause.edu/resources/2021/2/horizon-reports. Sist besøkt 25.05.2022.

57 Se for eksempel «Top 10 IT Issues, 2020». https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2020. Sist besøkt 25.05.2022.

Informasjonssikkerhet – brudd og hendelser i 2021

Det nasjonale og internasjonale trusselbildet avspeiler seg i de brudd og hendelser som de 21 universitetene og høgskolene rapporterte om i 2021.

Alle de 21 institusjonene opplyste om brudd eller hendelser – det totale antallet var omkring 2250. Dette tallet inkluderer brudd og hendelser som gjelder personopplysningssikkerheten. Det inkluderer ikke personvernsaker som gjaldt andre forhold enn sikkerheten til personopplysninger.

Av totalen på omkring 2250, utgjorde brudd på informasjons- eller personopplysningssikkerheten ca. 17 prosent. Dette var tilfeller hvor informasjonsverdier enten hadde blitt kompromittert, skadet, ødelagt eller gjort utilgjengelige. Det betyr at over 80 prosent av rapporterte tilfeller ikke førte til reelle sikkerhetsbrudd.

Om rapporteringen

Institusjonene ble ikke bedt om å rapportere på forhåndsdefinerte brudd eller hendelser. Det eneste vi ba om var at de ga en oversikt over hvilke brudd og hendelser de hadde vært utsatt for, og som de selv mente det var verdt å nevne.

Totaltallet på ca. 2250 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 oppgitt 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».

Skjevfordeling blant institusjonene

I 2021 som i tidligere år, var antallet registrerte brudd og hendelser ujevnt fordelt mellom universitetene og høgskolene.

Variasjonene skyldes i noen grad ulikheter i institusjonsstørrelse og -kompleksitet: institusjoner med mange ansatte og studenter, mange grunnenheter og en omfattende IT-portefølje, registrerer flere brudd og hendelser enn hva de mindre institusjonene vanligvis gjør.

Men variasjoner i registrerte brudd og hendelser skyldes også andre institusjonelle forhold enn størrelse og kompleksitet. Her ser vi en tydelig forskjell mellom institusjoner som har opprettet spesialiserte IT-sikkerhetsmiljøer og institusjoner som ikke har slike miljøer. Registrerte brudd og hendelser avspeiler derfor tilsvarende ulikheter i kapasitet og ekspertise: jo mer spesialisert og bedre bemannet de lokale IT-sikkerhetsmiljøene er, desto flere brudd og hendelser oppdages og håndteres.

Endringer sammenliknet med 2020

Det totale antallet brudd og hendelser er høyere enn det som ble rapportert for 2020. Økningen skyldes i hovedsak at enkelte av de største institusjonene rapporterte om noen flere brudd eller hendelser enn tidligere.

Det var særlig én institusjon som rapporterte om flere brudd og hendelser i 2021 enn i 2020. Hos denne institusjonen ble det registrert en økning på 31 prosent. Vi fikk opplyst at dette var en noe større årlig økning enn det som har vært vanlig de siste årene. Institusjonen mente at økningen trolig skyldes styrket oppdagelseskapasitet og et mer utfordrende trusselbilde. Hos de øvrige institusjonene ble det rapportert om mindre endringer fra i fjor.

Det ble også rapportert om flere brudd eller hendelser som skyldes sårbarheter (sikkerhetshull) i dataprogrammer enn hva som tidligere har vært vanlig.

Det er verdt å legge merke til at flere universiteter og høgskoler rapporterte om nedgang i enkelte typer brudd og hendelser i 2021. Det gjaldt primært kompromitterte brukerkontoer (brukernavn og passord på avveie). Hos ett av universitetene ble det for eksempel opplyst om at totrinnsinnlogging og skjerpede krav til passord hadde ført til en nedgang i antallet kompromitterte brukerkontoer på over 80 prosent jamført med 2020.

Universitetene og høgskolene rapporterte om færre alvorlige brudd på informasjonssikkerheten i 2021 enn i 2020. Med alvorlige brudd mener vi datainntrenging som har hatt eller kunne medført betydelige skader på viktige informasjonsverdier, og hvor oppdagelses- og reparasjonstiden[58] er lang.

Alvorlige brudd og hendelser

De mest alvorlige bruddene og hendelsene som universitetene og høgskolene rapporterte om i 2021, gjaldt målrettede dataangrep mot enkeltpersoner eller mot institusjonene som sådan. Dette inkluderer bekreftede eller mistenkte tilfeller av statlig hacking (se drøftelse nedenfor).

Hos en institusjon ble det for eksempel registrert 10 brudd eller hendelser som ble vurdert som alvorlige. Det omfattet blant annet ett tilfelle av løsepengevirusangrep (forberedelsene hadde kommet relativt langt, men angrepet ble oppdaget før skadevaren ble aktivert). Det omfattet også enkelte alvorlige sårbarheter (sikkerhetshull) i IT-tjenester, blant annet i epostsystemet.

Hos én av de andre institusjonene utgjorde kompromitterte brukerkontoer og målrettede forsøk på nettfiske drøyt 26 prosent av antallet brudd eller hendelser som ble vurdert som alvorlige.

Ut over dette, handlet de mest alvorlige tilfellene om sårbarheter (sikkerhetshull) i IT-tjenester, to-tre avanserte forsøk på fakturasvindel og enkelte andre typer saker, for eksempel datalekkasje og tyveri av IT-utstyr. Det ble også rapportert om datainnbrudd på en viktig IT-tjeneste (utvinning av kryptovaluta). Innbruddet er anmeldt til politiet.

Nettkriminalitet

Økonomisk motivert datainntrenging og -angrep – nettkriminalitet – utgjorde den største kategorien brudd og hendelser i 2021. Også i 2020 var nettkriminalitet den største kategorien.

Dette stemmer relativt godt overens med funn fra internasjonale studier. I den mest anerkjente av studien oppgis det at 95 prosent av det totale antall tilsiktede brudd på informasjonssikkerheten i kunnskapssektoren internasjonalt er økonomisk motivert.[59]

Kompromitterte brukerkontoer og ulike typer nettsvindel, spesielt direktør- eller fakturasvindel, var de vanligste formene for nettkriminalitet i 2021. Kontoene ble vanligvis benyttet til utsendelse av søppel-epost til andre virksomheter. I et fåtall tilfeller ble kontoene anvendt til mer alvorlige forhold, for eksempel som springbrett til å ta seg videre inn i institusjonenes datanettverk eller til spredning av skadevare (blant annet løsepengevirus).

I løpet av de siste to årene har vi registrert en viss nedgang i forsøk på direktør- og fakturasvindel. I 2021 ble det rapportert om en håndfull saker hvor medarbeidere utbetalte penger på bakgrunn av falske fakturaer eller fiktive eposter fra ledere.

Menneskelige og tekniske feil eller uhell

Mens nettsvindelsaker gikk noe ned i 2021, økte antallet brudd og hendelser som skyldtes menneskelige og tekniske feil eller uhell.[60]

Slike saker handlet om eposter med sensitivt/beskyttelsesverdig innhold som ble sendt til feil mottakere, og lagring av dokumenter (personopplysninger) på områder i datanettverket hvor de var tilgjengelige for uvedkommende.

Det gjaldt i tillegg uautorisert eksponering av personopplysninger ved feil bruk av digitale eksamensløsninger eller studentadministrative systemer (FS). Feil publisering av personopplysninger, enten på intranett eller i elektronisk postjournal, hadde også

58 Oppdagelses- og reparasjonstid definerer vi som antall dager fra første indikasjon på kompromittering av datanettverket til (i) sikkerhetsbruddet oppdages, enten av virksomheten selv eller av en tredjepart, og (ii) skader er reparert og normal driftstilstand er gjenopprettet. I 2020, ble det rapportert om flere brudd hvor oppdagelses- og reparasjonstiden var over tre måneder. I ett tilfelle var den minst ett år. Internasjonalt er trenden at oppdagelsestiden – antall dager fra kompromittering til bruddet oppdages – blir kortere. Se for eksempel Mandiant: «M-Trends 2022», side 9-17. https://www.mandiant.com/m-trends. Sist besøkt 27.05.2022.

59 Verizon: «2022 Data Breach Investigations Report», side 57. https://www.verizon.com/business/resources/reports/dbir/. Sist besøkt 27.05.2022.

60 Denne kategorien utgjorde omkring 12 prosent av det samlede antallet rapporterte brudd og hendelser i 2020.

i enkelte tilfeller ført til uautorisert eksponering av opplysningene.

Tekniske feil handlet primært om at systemer eller tjenester hadde vært utilgjengelige i perioder. I noen tilfeller hadde slike feil ført til uautorisert eksponering av personopplysninger.

Ut over dette, ble det rapportert om tekniske sårbarheter som enten hadde eller kunne blitt utnyttet av trusselaktører til å bryte informasjonssikkerheten. Det var sårbarheter som rammet relativt bredt i sektoren, spesielt sikkerhetshull i epostsystemer (Exchange-servere) og i vanlig brukt programvarefunksjonalitet (Log4j[61]).

I tillegg til har vi en restkategori – andre brudd og hendelser – med noen få saker som ikke passer inn i de øvrige kategoriene, for eksempel tyveri av IT-utstyr og nedlasting av piratkopiert programvare.

Bekreftet statlig hacking

Universitetene og høgskolene ble spurt om de hadde vært utsatt for bekreftede eller mistenkte tilfeller av statlig hacking.[62]

I 2021 rapporterte seks institusjoner om bekreftede saker gjeldende statlig hacking, det vil si brudd eller hendelser hvor kjente statlige hackergrupper var involvert. Dette er flere enn i 2020, men sakene var likevel ikke like alvorlige. I de fleste sakene hadde institusjonene fått bistand fra Nasjonal sikkerhetsmyndighet og sektorens responsmiljø (tidligere Uninett CERT).

De rapporterte tilfellene handlet om forsøk på å ta seg inn i institusjonenes datanettverk («brute force-angrep»[63]). Enkelte institusjoner opplyste om jevnlige forsøk på datainntrengning fra statlige hackere. Det ble også opplyst om at nye sikringstiltak hadde blitt innført som følge av inntrengingsforsøkene, blant annet totrinnsinnlogging.

Det ble i tillegg rapportert om rekognoseringsaktivitet fra statlige hackergrupper. Med rekognosering menes at trusselaktører kartlegger institusjonene via internettet, trolig med tanke på å utnytte sårbarheter i datamaskiner for deretter å ta seg videre inn i datanettverket. Statlige hackergrupper hadde for eksempel vist interesse for driftsmeldinger i forbindelse med aktivering av totrinnsinnlogging og annen offentlig tilgjengelig informasjon om arbeidet med informasjonssikkerhet.

Mistenkt statlig hacking

I mars 2021 ble det kjent at en statlig kinesisk hackergruppe utnyttet sårbarheter i enkelte av Microsoft sine epostsystemer – virksomhetenes egen-driftede Exchange-servere.[64] Microsoft ga hackergruppen navnet «Hafnium».[65] Sårbarhetene ga trusselaktører tilgang til alle kontopassord, inkludert til administratorkontoer, og til andre datamaskiner tilknyttet det samme datanettverket.

Åtte universiteter og høgskoler rapporterte om at de var berørt av disse sårbarhetene. Hos to av institusjonene ble det opplyst om at sårbarhetene ble utbedret uten at det var registrert forsøk på datainntrenging. Hos de seks andre ble det gjort forsøk på inntrenging. Minst to av forsøkene lyktes.

I de to tilfellene hvor det hadde skjedd datainntrenging, ble det oppgitt at oppryddingskostnader var den viktigste skadevirkningen. Hos den ene var kostnaden på omkring 100 000 kr., mens det hos den andre dreide det som om ca. 500 000 kr. I tillegg ble det innført nye sikringstiltak i kjølvannet av hendelsene, for eksempel bruk av skybasert epostløsning og totrinnsinnlogging på epostkontoer.

Én eller flere av disse sakene kan gjelde statlig hacking, men det kan også ha vært nettkriminelle aktører som sto bak. Vi kategoriserer derfor bruddene og hendelsene som mistenkt statlig hacking, men hvor attribusjonen er uavklart.

---

61 Log4j logger aktivitet i webapplikasjoner og -tjenester. Sårbarheten i Log4j kan blant annet utnyttes til datainnbrudd, stjele brukernavn og passord, hente ut data fra IT-systemer og distribusjon av skadevare. Se for eksempel https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/samleside-for-log4j/. Sist besøkt 25.05.2022.

62 I fjorårets risiko- og tilstandsvurdering rapporterte vi om fire tilfeller hvor slike trusselaktører hadde skaffet seg tilgang til lokale datanettverk eller forskningsinfrastruktur (laboratorier, publikasjonsløsninger og tungregneanlegg). Se «Risiko- og tilstandsvurdering 2021», kapittel 3. https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

63 «Brute force-angrep» innebærer at trusselaktører forsøker å skaffe seg tilgang til brukerkontoer ved å prøve mange mulige kombinasjoner av brukernavn og passord. https://www.kaspersky.com/resource-center/definitions/brute-force-attack. Sist besøkt 25.05.2022.

64 Se for eksempel https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/. Sist besøkt 25.05.2022.

65 Se for eksempel https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/. Sist besøkt 25.05.2022.

Hendelser registrert av sektorens responsmiljø

Sektorens responsmiljø hos Sikt (tidligere Uninett CERT) har ansvaret for å oppdage og varsle om uønsket aktivitet i forskningsnettet. Som tidligere år, har vi innhentet statistikk fra sektorens responsmiljø om slik aktivitet.

Responsmiljøet rapporterte om 632 saker (brudd og hendelser) i 2021. Antallet er noe lavere enn for de foregående fire årene. I 2018 rapporterte responsmiljøet om 965 saker. Tilsvarende tall for 2019 og 2020 var henholdsvis 792 og 867.

Om statistikken fra sektorens responsmiljø

Det vil være en viss overlapp mellom de sakene (brudd og hendelser) som ble rapportert av institusjonene og de som sektorens responsmiljø opplyste om. Alle saker rapportert av responsmiljøet kommer derfor ikke i tillegg til de som institusjonene rapporterte om – det vil være noe dobbelrapportering. Vi har ikke mulighet til å avgjøre graden av dobbelrapportering.

Hovedtyper saker

I 2021 var sårbare systemer den vanligste sakskategorien registrert hos sektorens responsmiljø. Dette var datamaskiner som var eksponert mot internett og som manglet nødvendige sikkerhetsoppdateringer. Maskinene var derfor sårbare for datainntrenging og misbruk.

Den nest mest vanlige sakskategorien, var «DDoS amplifiers». Dette handlet om datamaskiner som kunne misbrukes av trusselaktører til å gjennomføre tjenestenektangrep.

Disse to kategoriene – sårbare systemer og «DDoS amplifiers» – utgjorde 60 prosent av sakene registrert hos sektorens responsmiljø i 2021.

Videre rapporterte responsmiljøet om følgende vanlige brudd og hendelser:

- Skanning og innloggingsforsøk: lokale datamaskiner som ble misbrukt av trusselaktører til å (i) skanne etter sårbarheter hos andre virksomheter og (ii) gjennomføre «brute force»-angrep (automatisert passordgjetting).
- Uønsket eksponering av datamaskiner: IT-tjenester som ikke burde vært eksponert mot internettet, men som likevel kan nås via nettet.
- Kompromitterte administrasjonskontoer: uautorisert tilgang til én eller flere kontoer med administrative rettigheter.
- Skadevare: IT-systemer som hadde blitt infisert med ulike typer «ondsinnet kode», for eksempel skadevare for utvinning av kryptovaluta.

Sektorens responsmiljø hadde registrert en viss nedgang i forsøk på nettsvindel i 2021 (direktør- og fakturasvindel). Samtidig ble det også her rapportert om større aktivitet fra statlige hackergrupper.

Leverandørkjedeangrep ble vurdert å være en større trussel enn tidligere. Dette er sikkerhetsbrudd som skjer via tredjeparter, spesielt leverandører av IT-tjenester eller -systemer. Også løsepengevirus ble vurdert som en alvorlig trussel. Her viste responsmiljøet blant annet til et finsk universitet som nylig hadde blitt rammet av løsepengevirus.[66]

66 Se https://twitter.com/cyber_etc/status/1490614380031102976. Sist besøkt 25.05.2022.

Saker meldt til Datatilsynet

Brudd på personopplysningssikkerheten som innebærer risiko for krenkelser av personvernet, skal meldes til Datatilsynet.[67] Figuren nedenfor viser hvor mange sikkerhetsbrudd som universitetene og høgskolene meldt til Datatilsynet i 2021 sammenliknet med de to foregående årene.

Vi ser at antallet sikkerhetsbrudd som ble meldt har økt for hvert år. I 2019 ble det rapportert om 14 slike saker. Antallet hadde økt til 30 i 2020 og videre til 44 i 2021.

Åtte av 21 universiteter og høgskoler oppga i 2021 at de hadde meldt brudd på personopplysningssikkerheten til Datatilsynet. Dette er færre enn i 2020 (12 institusjoner). Økningen fra 2020 til 2021 skyldes derfor at færre institusjoner meldte om flere saker enn tidligere.

Variasjonen mellom institusjoner i antallet meldte saker kan skyldes at ulike institusjoner har forskjellige vurderinger av hvilke sikkerhetsbrudd som er meldepliktige – noen legger listen for melding til Datatilsynet høyere enn andre. En annen årsak har være at enkelte institusjoner har bedre løsninger for intern varsling av brudd på personopplysningssikkerheten enn andre. Antallet meldte saker til Datatilsynet kan derfor avhenge av hvor godt institusjonene har tilrettelagt for intern varsling av slike brudd.

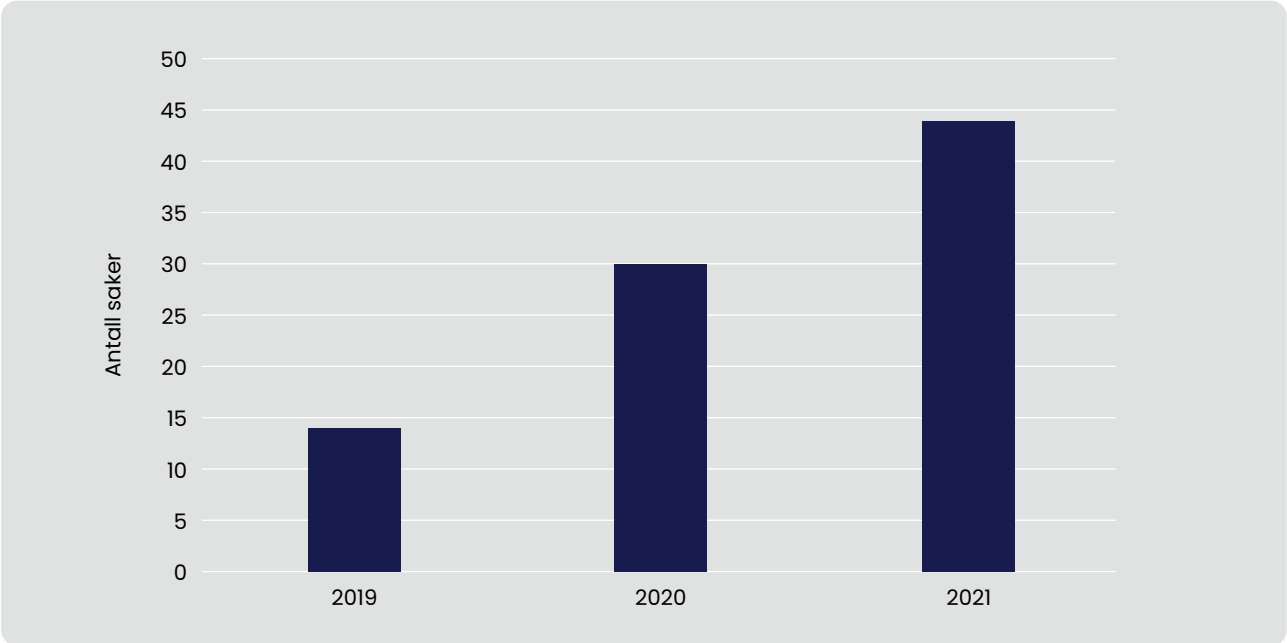
Meldingsinnhold

34 av 44 meldinger til Datatilsynet i 2021 omhandlet brudd på konfidensialiteten til personopplysninger. Enkelte av datainntrengingene i epostsystemer drøftet ovenfor ble for eksempel meldt.

De vanligste årsakene til meldinger var imidlertid feilsending av epost, feil publisering av personopplysninger og lagring av opplysninger på lagringsområder som var tilgjengelige for uvedkommende (egne ansatte eller studenter). Det ble også rapportert om meldinger som gjaldt uautorisert eksponering av innholdet i enkeltvedtak, for eksempel resultater av klagesensur.

Det ble ikke opplyst om saker som berørte et stort antall registrerte eller store mengder personopplysninger. Et par saker gjaldt særlige kategorier personopplysninger, som hadde blitt tilgjengeliggjort for uvedkommende.

Figur 3: Saker meldt til Datatilsynet, 2019-2021



67 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.

Andre personvernsaker i 2021

Universitetene og høgskolene ble bedt om å oppgi hvilke personvernsaker de hadde registrert i 2021 som ikke gjaldt brudd på sikkerheten til personopplysninger.

19 av de 21 universitetene og høgskolene opplyste om at de hadde registrert andre typer personvernhendelser i 2021 enn sikkerhetsbrudd. Totalt dreide det seg om ca. 380 slike saker. Dette er en økning sammenliknet med tidligere år. I 2020 ble det for eksempel rapportert om ca. 200 personvernsaker. Det tilsvarende antallet for 2019 var 140.

Antall og typer personvernsaker

Den klart største kategorien saker, gjaldt feil eller mangler ved registrering av forsknings- og studentprosjekter i NSD (nå Sikt) sitt meldingsarkiv. I 2021 utgjorde meldinger om slike feil og mangler drøyt 64 prosent av det totale antallet rapporterte personvernsaker. Her handlet det om to typer mangler.

For det første at påbegynte registreringer i NSD (nå Sikt) sitt meldingsarkiv ikke ble sluttført. I slike tilfeller måtte institusjonene undersøke om manglende sluttføring skyldtes at forsknings- eller studentprosjektene ikke ble gjennomført, eller om prosjektene ble gjennomført uten gyldig registrering.

For det andre manglende bekreftelse på at forsknings- og studentprosjekter var avsluttet og at opplysningene enten er slettet eller anonymisert (sluttmelding). Ved manglende sluttmelding, måtte institusjonene sjekke hva som hadde skjedd med opplysningene – om de var slettet, anonymisert eller ikke. Flere institusjoner opplyste om at de hadde noe etterslep med hensyn til oppfølging av forsknings- og studentprosjekter hvor det ikke forelå sluttmelding.

De resterende personvernsakene omhandlet forskjellige andre forhold knyttet til feil behandling av personopplysninger og brudd på interne rutiner (avvik). Det inkluderte manglende oppdatering av behandlingsprotokollen ved bruk av nye applikasjoner, behandling av personopplysninger uten lovlig grunnlag og manglende gjennomføring av personvernvurderinger (DPIA).

Det ble også rapportert om manglende overholdelse av rutiner for kontroll med overføringer av opplysninger til tredjeland (land utenfor EU/EØS). Enkelte institusjoner opplyste om at de ikke hadde oppdatert rutinene for slike overføringer i kjølvannet av Schrems II-dommen.[68]

68 Se for eksempel https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/. Sist besøkt 25.05.2022.

Oppsummering og anbefalinger

EOS-tjenestene fremhever i sine årlige vurderinger at trusselbildet i kunnskapssektoren er mer utfordrende enn tidligere. Det advares mot at norske forskningsmiljøer innen en rekke fagområder kan være mål for cyberoperasjoner.

Vår kartlegging av statlige universiteter og høgskoler speiler i noen grad dette trusselbildet: institusjonene rapporterte om noen flere uønskede brudd på informasjonssikkerheten og krenkelser av personvernet enn i 2020. Sektorens responsmiljø (tidligere Uninett CERT) opplyste om en viss nedgang i antallet registrerte brudd og hendelser sammenliknet med 2020.

Nettkriminalitet utgjorde fortsatt den klart største kategorien brudd og hendelser. Deretter fulgte utilsiktede menneskelige og tekniske feil eller uhell. Det ble rapportert om flere bekreftede eller mistenkte tilfeller av statlig hacking enn hva som tidligere har vært vanlig.

Videre ser vi en økning i antallet brudd på personopplysningssikkerheten som meldes til Datatilsynet. Vi ser også at antallet rapporterte meldinger fordeler seg på færre institusjoner enn i 2020. Det kan bety at oppdagelseskapasiteten og kvaliteten på varslingsrutiner er noe ujevnt fordelt i sektoren.

Vi anbefaler at sektoren fortsatt styrker sin evne til å håndtere brudd på informasjonssikkerheten og krenkelser av personvernet. Kapasiteten til å oppdage inntrengingsforsøk og å begrense skadevirkninger bør videreutvikles, både på sektor- og institusjonsnivå.

Videre anbefaler vi at følgende tiltak iverksettes:

- sektorens deteksjons- og responskapasitet videreutvikles,
- det gjennomføres sårbarhets- og inntrengingstesting i sektoren,
- det gis veiledning til sektoren om håndtering av IKT-sikkerhetshendelser,
- det gjennomføres kurs for operativt sikkerhetspersonell i sektoren (IRT),
- det gis bistand for å styrke beredskaps- og kontinuitetsarbeidet i sektoren,
- VDI innføres hos institusjoner som ønsker det.

Kapittel 3

Universiteter og høgskoler – sårbarheter, forbedringer og status

Kapittel 3

Universiteter og høgskoler – sårbarheter, forbedringer og status

Innledning

Bruddene og hendelsene drøftet i forrige kapittel viser at statlige universiteter og høgskoler kan være sårbare for trusler mot sine informasjonsverdier. I dette kapitlet drøftes hvilke sårbarheter som arbeidet med informasjonssikkerhet og personvern har til hensikt å utbedre.

Sårbarheter er mangler eller svakheter hos institusjonene som kan føre til at informasjonsverdier blir stjålet, skadet, ødelagt eller gjort utilgjengelige. Eksempler på sårbarheter er sikkerhetshull i programvare, manglende personvernkompetanse, lav brukerbevissthet eller uklar sikkerhetsorganisering (fordeling av ansvar og oppgaver).

I dette kapitlet drøftes tre hovedspørsmål:

1) Hvilke sårbarheter mente universitetene og høgskolene at de har behov for å utbedre?
2) Hvilke forbedringstiltak iverksatte universitetene og høgskolene i 2021 for å utbedre sårbarheter og håndtere trusler mot informasjonssikkerheten og personvernet?
3) I hvilken grad hadde iverksatte tiltak styrket etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern?

Resten av kapitlet

I første del av kapitlet gis en oversikt av de viktigste sårbarhetene som universitetene og høgskolene rapporterte om.

Deretter gis en oversikt av de viktigste forbedringstiltakene som universitetene og høgskolene hadde iverksatt i 2021.

Til slutt oppsummeres status for institusjonenes etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

Rapporterte sårbarheter i 2021

Som tidligere år, spurte vi de 21 universitetene og høgskolene om hvilke sårbarheter som måtte utbedres for å styrke arbeidet med informasjonssikkerheten og personvernet.

Figur 4 oppsummerer institusjonenes svar – hvilke sårbarheter som ble nevnt av flest og færrest institusjoner. Figuren viser derfor sårbarhetsprofilen for denne delen av sektoren.

Sårbarhetsprofilen for 2021 er litt forskjellig fra de profilene vi har sett tidligere år. Nedenfor kommenterer vi stabilitet og endring sammenliknet med 2020 og 2019.

Stabilitet

I 2020 og 2019 rapporterte universitetene og høgskolene om at ledere og ansattes kompetanse om informasjonssikkerhet og personvern var den viktigste sårbarheten. Bevissthet om utfordringer knyttet til informasjonssikkerhet og personvern ble oppgitt å være den nest viktigste sårbarheten.[69]

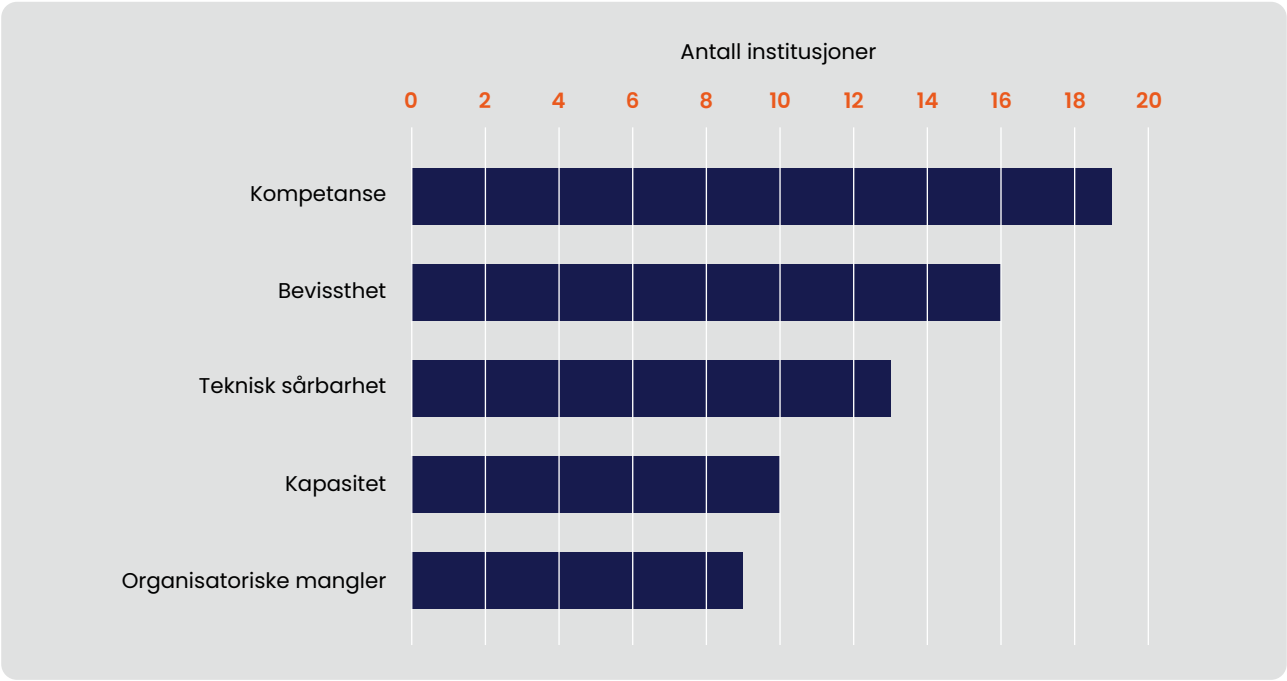
Vi ser at dette ikke har endret seg i 2021 – kompetanse og bevissthet oppgis fortsatt å være de viktigste sårbarhetene. 19 institusjoner oppga at informasjonssikkerhets- og personvernkompetanse er viktige sårbarheter, mens 16 mente det samme om bevissthet.[70]

Endring

Det som overrasker denne gangen, er at institusjonene oppga at både tekniske sårbarheter og kapasitet (årsverksinnsats) var viktigere sårbarheter enn hva tilfelle var for ett og to år siden. I 2021 mente 13 institusjoner at tekniske sårbarheter (sikkerhetshull i programvare) var en viktig sårbarhet. 10 institusjoner mente det samme om egen manglende kapasitet til å utføre informasjonssikkerhets- og personvernoppgaver. Dette er vesentlig flere enn for et par år siden.

Samtidig er det overraskende at organisatoriske sårbarheter, for

Figur 4: Sårbarhetsprofil, 2021



69 «Risiko- og tilstandsvurdering 2021» (side 31-33), og «Risiko- og tilstandsvurdering 2020» (side 19-22). https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

70 Kompetansemangel er ikke spesielt for UH-sektoren, se for eksempel Stortingsmelding 38 (2016-2017): «IKT-sikkerhet – et felles ansvar». https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/. Her fremheves det at sikkerhetskompetanse er en knapp ressurs. Stortingsmeldingen ble derfor fulgt opp med en nasjonal strategi for digital sikkerhetskompetanse. https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf. Begge ble sist besøkt 25.05.2022.

eksempel uklar fordeling av ansvar og oppgaver eller manglende rutiner for behandling av personopplysninger, har falt utenfor pallen. Slike sårbarheter ble i 2021 relegert til femte og sisteplass, mens de tidligere har innehatt en sikker tredjeplass.

Tekniske sårbarheter

Den økte oppmerksomheten om tekniske sårbarheter som institusjonene rapporterte om i 2021, skyldes trolig flere forhold:

For det første, det generelt skjerpede trusselbildet. For det andre, flere brudd og hendelser i UH-sektoren hvor utnyttelse av tekniske sårbarheter har vært en viktig angrepsmetode (se kapittel 2).

For det tredje, sikkerhetstesten (sårbarhetsskannet) som Uninett gjennomførte i UH-sektoren i mai 2021. Skannet avdekket tekniske sårbarheter i internetteksponerte datamaskiner (tjenester).

Organisatoriske mangler

Færre rapporter om organisatoriske sårbarheter indikerer at institusjonene har forbedret systematikken i eget arbeid.

Det ble for eksempel opplyst om at fordelingen av ansvaret for informasjonssikkerhets- og personvernoppgaver, var avklart og kjent i større grad enn i 2020 og 2019.

Kapasitetsutfordringer

I 2021 oppga dobbelt så mange institusjoner at kapasitet til å utføre informasjonssikkerhets- og personvernoppgaver var en viktig sårbarhet sammenliknet med 2020 (10 i 2021 mot fem i 2020).

Noe av årsaken til denne endringen er trolig knyttet til pandemihåndteringen. I 2020 ble det rapportert fra enkelte institusjoner at pandemihåndteringen hadde ført til at planlagte oppgaver ble satt på vent.[71] Når dette etterslepet skulle tas inn i 2021, kan det ha synliggjort behovet for å styrke kapasiteten.

Samtidig er det trolig at oppfølging av resultatene fra Uninett sin sikkerhetstest og håndtering av forsøkene på datainntrenging i epostsystemer, også har synliggjort at kapasiteten til å utføre viktige oppgaver bør styrkes.

71 Se «Temarapport 2021 – pandemihåndteringen og betydningen for arbeidet med informasjonssikkerhet og personvern i UH-sektoren». https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

Tiltaksaktiviteten i 2021

Vi spurte institusjonene om hvilke tiltak de hadde iverksatt i 2021 for å utbedre sårbarheter og styrke arbeidet med informasjonssikkerhet og personvern.

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? Var selvmedisineringen tilpasset egendiagnostiseringen?

Kapasitetstiltak – årsverksendringer

Figur 5 viser hvor mange universiteter og høgskoler som opplyste om at det ble iverksatt kapasitetstiltak – styrking av årsverksinnsatsen – i 2021.

Vi ser at åtte institusjoner hadde økt antallet årsverk øremerket for arbeidet med informasjonssikkerhet og personvern i 2021. Dette er den største samlede årsverksveksten siden 2019.

13 institusjoner rapporterte om at årsverksinnsatsen ikke hadde endret seg. Ingen institusjoner rapporterte om at årsverksinnsatsen var redusert.

Hvordan årsverkene fordeler seg hos den enkelte institusjon, er gjort rede for i tidligere risiko- og tilstandsvurderinger.[72] De er i hovedsak knyttet til rollen for informasjonssikkerhetsansvarlig/-rådgiver (CISO), og til institusjonenes IT-avdelinger, inkludert hendelseshåndteringsteam (IRT).

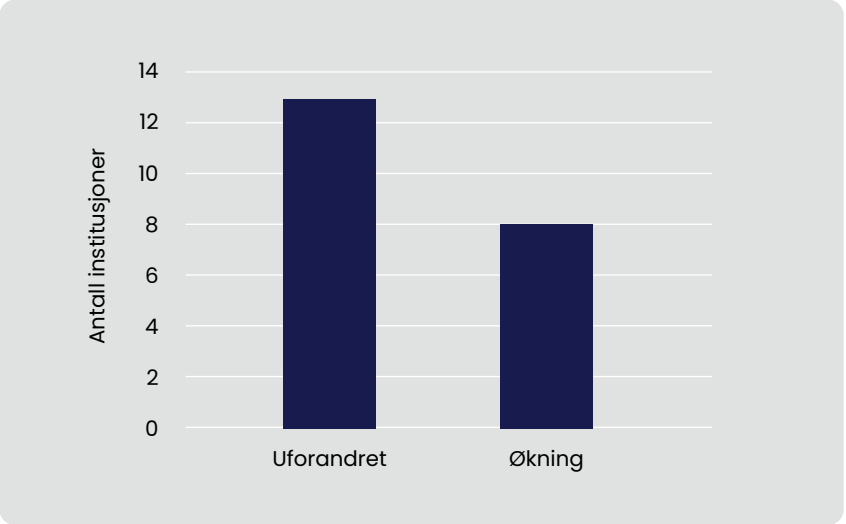
I tillegg er det øremerkede årsverk i HR- og økonomiavdelingene, avdelinger med ansvar for virksomhetsstyring og i studie- og forskningsadministrasjonen. Hos enkelte institusjoner inkluderer det også sikkerhets- og beredskapsledere (CSO).

De vitenskapelig ansatte

Årsverksanslagene omfatter i liten grad arbeidet med informasjonssikkerhet og personvern blant vitenskapelig ansatte, for eksempel søknader om godkjenning av eller meldinger om forskningsprosjekter, særlig til de regionale forskningsetiske komiteene og NSD (nå Sikt). I dette arbeidet inngår både informasjonssikkerhet og personvern som viktige elementer.

Det er grunn til å tro at årsverksanslagene ville blitt noe høyere dersom innsatsen til de vitenskapelige ansatte hadde blitt inkludert i rapporteringen.

Figur 5: Endringer i antall årsverk, 2020–2021



72 Se for eksempel «Risiko- og tilstandsvurdering 2020», side 17. https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

Om tiltakene

Enkelte av tiltakene i figur 6 nedenfor, er konkrete informasjonssikkerhets- eller personverntiltak, for eksempel innføring av totrinnsinnlogging eller kurs for ansatte i GDPR.

Enkelte andre tiltak er systemtiltak. Dette er tiltak som har til hensikt å etablere eller videreutvikle et systematisk informasjonssikkerhets- eller personvernarbeid. Eksempler på systemtiltak er revisjon av ledelsessystemer for informasjonssikkerhet eller etablering av rutiner for risikostyring.

Innleid kapasitet

Oversikten over årsverk inkluderer kun institusjonenes egne ansatte. Innleid kapasitet inngår ikke i oversikten.[73]

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

Det vi spesielt har merket oss i år er antallet universiteter og høgskoler som oppga at de hadde benyttet tjenester fra kommersielle konsulent- og sikkerhetsselskaper og advokatfirmaer.

20 av 21 institusjoner opplyste om at de hadde kjøpt informasjonssikkerhets- eller personverntjenester fra slike aktører i 2021. 11 institusjoner opplyste om at de hadde kjøpt assistanse fra to eller flere kommersielle selskaper.

Institusjonene leide inn kapasitet fra kommersielle aktører for å løse en rekke oppgaver. Det gjaldt i særlig grad revisjoner av arbeidet med informasjonssikkerhet og personvern, etablering av beredskaps- og kontinuitetsplaner, gjennomføring av kriseøvelser og håndtering av digitale sikkerhetshendelser.

Det var også vanlig at innleid kapasitet ble benyttet til videreutvikling eller kvalitetssikring av internkontrollen for personvern (GDPR), innføring av ledelsessystemer for informasjonssikkerhet, etablering av behandlingsprotokoller og risikovurderinger av IT-tjenester.

Andre viktige tiltak i 2021

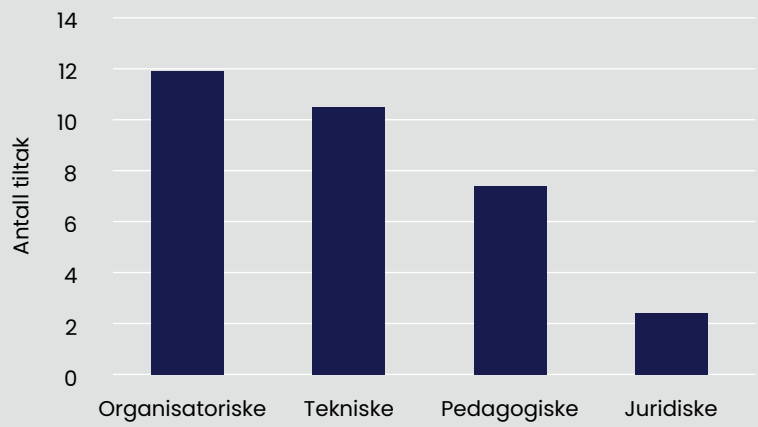
Vi spurte institusjonene om hva egne årsverk og den innleide kapasiteten hadde jobbet med i 2021: hvilke og hvor mange tiltak ble iverksatt for å utbedre sårbarheter og styrke arbeidet med informasjonssikkerhet og personvern?

Figur 6 gir en oversikt over antall og hovedtyper tiltak som universitetene og høgskolene opplyste om.

Figuren viser at universitetene og høgskolene totalt rapporterte om 322 tiltak i 2021. Til sammenlikning ble det i 2020 rapportert om 220 tiltak. Det betyr at tiltaksaktiviteten har økt vesentlig fra 2020 til 2021.

Tiltaksprofilen – hvordan tiltakene fordeler seg på de ulike tiltakskategoriene – var omtrent den samme i 2021 som i 2020: flest organisatoriske tiltak (119), tekniske tiltak (105) som en god nummer to og pedagogiske tiltak (74) på tredjeplass. Det ble rapportert om færrest juridiske tiltak (24).

Figur 6: Informasjonssikkerhets- og personverntiltak, 2021



73 Med ett unntak: hos én institusjon ble 1,5 konsulentårsverk inkludert i årsverksinnsatsen. Dette fordi avtalen om bistand strekker seg over flere år.

Definisjoner

Organisatoriske tiltak: Utarbeidelse, innføring eller praktisering av ledelsessystemer for informasjonssikkerhet og internkontroll for personvern (GDPR). Eksempler på slike tiltak kan være fordeling av ansvar og oppgaver, 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 kan inkludere publisering av informasjon på hjemmesider, kurs i risikovurderinger, grunnleggende opplæring i GDPR, utarbeidelse av veiledere eller maler 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 tekniske tiltak inkluderer totrinnsinnlogging, segmentering av datanettverk, anskaffelse av brannmur, kryptering av elektronisk kommunikasjon eller forbedret nettverksovervåkning.

Juridiske tiltak: Tiltak som forutsetter juridisk kompetanse og som gjelder rettslige vurderinger av krav til informasjonssikkerhet og personvern. Eksempler på dette kan være gjennomgang eller endring av vilkår i databehandleravtaler eller kontroll av at avtalte vilkår for behandling av personopplysninger ivaretas av databehandleren.

Organisatoriske tiltak

De viktigste organisatoriske tiltakene handlet om systemtiltak. Mer konkret dreide det seg om innføring og praktisering av ledelsessystemer for informasjonssikkerhet og internkontroll for etterlevelse av personvernlovgivningen (personopplysningsloven og personvernforordningen). Tydeliggjøring av rollene i sikkerhetsorganisasjonen og revisjoner av sikkerhetsstrategier/-policyer er eksempler på dette. Anskaffelser av digitale verktøy for strukturering av arbeidet med etterlevelse av personvernkrav (GDPR) var et annet viktig systemtiltak som det ble opplyst om.

I tillegg ble det opplyst om tiltak for å styrke institusjonenes hendelseshåndteringsteam (IRT). Dette handlet spesielt om tydeliggjøring av mandatet for teamene og utarbeidelse av retningslinjer for håndtering av digitale sikkerhetshendelser.

Videre ble det rapportert om gjennomføring av enkeltaktiviteter som inngår i ledelsessystemer for informasjonssikkerhet eller internkontrollen for personvern (GDPR). Dette handlet typisk om utarbeidelse av nye rutiner, blant annet med hensyn til de registrertes rettigheter, og etablering av retningslinjer for sikker forvaltning av informasjonsverdier, for eksempel klassifiserings- og lagringsguider. Det handlet også om kartlegging av systemer og tjenester, utarbeidelse av behandlingsprotokoller for personopplysninger og gjennomføring av risikovurderinger.

Beredskap og kontinuitet – planverk for håndtering av alvorlige informasjonssikkerhets- og personvernhendelser – er et annet organisatorisk område hvor det i 2021 ble rapportert om viktige forbedringer. Mens det i 2020 var 10 institusjoner som opplyste om svært mangelfulle eller utdaterte beredskaps- og kontinuitetsplaner, var antallet redusert til fire i 2021. Det var likevel bare én institusjon som hadde etablert et fullverdig og oppdatert planverk som jevnlig ble øvd og revidert.

Tekniske tiltak
Hovedformålet med denne typen tiltak er å hindre at institusjonenes datamaskiner utfører oppgaver som det ikke er meningen at de skal gjøre: gi fra seg sensitiv informasjon, slette verdifulle data, blokkere viktige arbeidsoppgaver, osv. Tiltakene skal også sørge for at tekniske eller menneskelige feil og uhell ikke skader kjernevirksomheten.

Figur 7 viser hvor mange universiteter og høgskoler som rapporterte om at de i 2021 hadde eller var i ferd med å innføre åtte grunnleggende tiltak for å styrke den tekniske sikkerheten.[74]

Enkelte av tiltakene i figuren er organisatoriske snarere enn tekniske. Det gjelder for eksempel sikkerhets-oppdatering og tjenestekontroll. Vi har likevel valgt å kategorisere dem som tekniske ettersom de er viktige for å styrke den tekniske sikkerheten.

Figuren viser at tre tiltak peker seg ut. Dette er tiltak som halvparten eller flere av de 21 institusjonene opplyste om at de hadde eller var i ferd med å innføre.

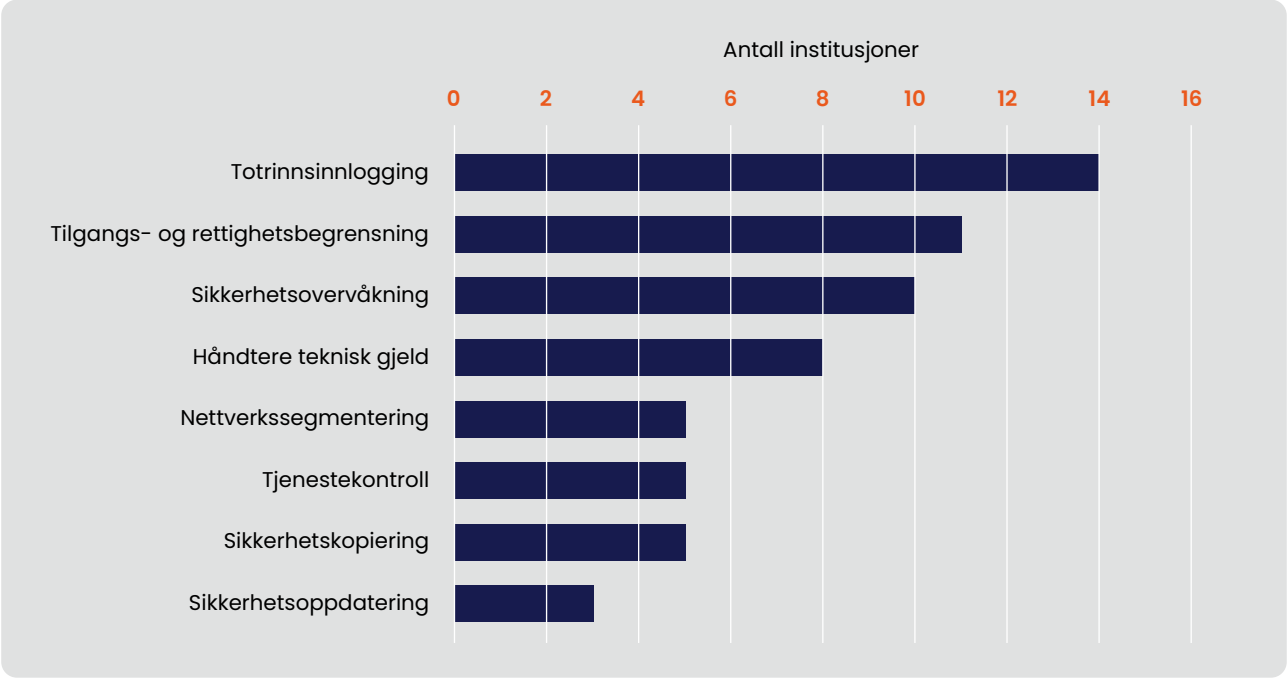
14 institusjoner rapporterte om innføring av totrinnsinnlogging. Dette beskytter mot datainntrenging og -angrep som følge av at trussel-aktører, spesielt nettkriminelle grupper og statlige hackere, skaffer seg tilgang til ansatte eller studenters brukernavn og passord.

11 universiteter og høgskoler opplyste om tilgangs- og rettighetsbegrens-ning: styrket kontroll med hvilke IT-systemer som brukerne får tilgang til og hva brukerne får lov til å gjøre i IT-systemene. Dette beskytter mot at brukerne får vite om opplysninger som de ikke har tjenestelige behov for å kjenne til. Det begrenser også hva trusselaktører kan gjøre – hvor mye skade de kan anrette – dersom de skaffer seg tilgang til institusjonenes datamaskiner.

10 institusjoner hadde forbedret sikkerhetsovervåkingen, spesielt bruk av funksjonalitet i skytjenester som kan oppdage og varsle om uønsket aktivitet. Det begrenser skade-virkningene dersom aktører med «skumle hensikter» lykkes med å ta seg inn i institusjonenes datanettverk.

I tillegg oppga litt under halvparten av institusjonene at et fjerde tiltak

Figur 7: Tiltak for å styrke teknisk sikkerhet



74 Tiltakene anbefales blant annet av NSM, se for eksempel https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt. Sist besøkt 25.05.2022.

i figuren – håndtere teknisk gjeld – hadde blitt prioritert i 2021. Med dette menes at bruken av eldre og sårbare IT-systemer enten avsluttes, oppgraderes til nyere versjoner eller skjermes bedre mot angrip via internettet.

De øvrige tiltakene i figur 7 ble rapportert av fem eller færre institusjoner. Det gjelder følgende tiltak:

- fiksing av sikkerhetshull i programvare (sikkerhetsoppdatering),
- godkjenning av ny programvare (tjenestekontroll),
- kopiering av data og programvare (sikkerhetskopiering),
- styrking av interne sikkerhetsbarrierer i datanettverket (nettverkssegmentering).

11 institusjoner oppga at de i 2021 hadde jobbet med fire eller flere av tiltakene i figur 7. Disse institusjonene hadde derfor hatt relativt stor aktivitet med hensyn til mange av tiltakene.

De resterende 10 institusjonene oppga at de hadde jobbet med to eller færre av tiltakene. Disse institusjonene har derfor hatt mer begrenset tiltaksaktivitet når det gjelder teknisk sikkerhet, for eksempel fordi de ikke har kapasitet til å gjennomføre mange krevende tiltak hvert år. Men det kan også bety at enkelte av institusjonene har valgt å prioritere organisatoriske, pedagogiske eller juridiske tiltak i 2021.

Pedagogiske tiltak

Pedagogiske tiltak har som formål å styrke kompetanse og bevissthet om informasjonssikkerhet og personvern. Som ved tidligere kartlegginger, var det to hovedtyper tiltak det ble opplyst om i 2021.

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

For det andre, allmenn bevisstgjøring («folkeopplysning»). Dette var primært informasjon eller informasjonskampanjer rettet mot den jevne student eller ansatt. Det kunne handle om informasjon om vanlige sikkerhetstrusler på internett, for eksempel nettfiske eller svindelepost, eller grunnleggende informasjon om personvern (formidlet i møter med studenter og ansatte, på digitale informasjonstavler eller på hjemmesider). Deltakelse i nasjonal sikkerhetsmåned, og bruk av de nanolæringskursene som inngår i denne årlige kampanjen, var et annet vanlig bevisstgjøringstiltak.[75]

Et siste viktig pedagogisk tiltak var øvelser på håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser. I 2020 ble slike øvelser nedprioritert til fordel for håndtering av pandemien. I 2021 ble det opplyst om at øvelsesaktiviteten hadde økt noe.

Juridiske tiltak

Den siste tiltakskategorien – juridiske tiltak – er ny av året. Dette handler primært om kontroll med og oppfølging av vilkår i avtaler med leverandører at IT-tjenester.

Ovenfor har vi sett at det ble rapportert om relativt få slike tiltak, og at de i hovedsak gjaldt oppfølging av Schrems II-dommen. Det kunne derfor dreie seg om gjennomgang og revisjon av databehandleravtaler med tjenesteleverandører og kontroll med hvorvidt at personopplysninger ble overført til land hvor vernet av personopplysninger ikke tilsvarer det som følger av GDPR.

75 Se https://sikkert.no/. Sist besøkt 27.05.2022.

Sårbarhetsprofil og tiltaksaktivitet

Dersom vi sammenlikner sektorens sårbarhetsprofil i figur 4 med tiltaksaktiviteten i figur 5 og 6, ser vi at det er enkelte forskjeller mellom institusjonenes egendiagnostisering og selvmedisinering: tiltaksaktiviteten overlapper ikke fullt ut med rapporterte sårbarheter.

Forskjellen synes å være størst når det gjelder kompetanse og bevissthet. For mens institusjonene vurderte kompetanse og bevissthet som de to viktigste sårbarhetene, var tiltaksaktiviteten klart størst med hensyn til organisatoriske og tekniske tiltak. Tiltak for å styrke kompetansen og bevisstheten hos ledere og medarbeidere – pedagogiske tiltak – var den tredje største tiltakskategorien.

Dette ble også kommentert av institusjonene selv. Flertallet av dem mente det var utfordrende å gi det opplærings- og kompetansetilbudet de hadde behov for.

Vi ser den motsatte tendensen når det gjelder organisatoriske sårbarheter og tiltak. Organisatoriske mangler var den sårbarheten som færrest institusjoner opplyste om, men det ble likevel rapportert om flest organisatoriske tiltak. Det er mulig at forskjellen nettopp skyldes at mange organisatoriske tiltak ble iverksatt i 2021, og at disse sårbarhetene derfor ble vurdert som tilfredsstillende håndtert.

På den annen side opplyste institusjonene om at praktisering av ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR) var mangelfull. Det kan tyde på at organisatoriske sårbarheter fortsatt utgjør en viktig utfordring, og at det er behov for å opprettholde eller styrke aktiviteten innen denne tiltakskategorien.

Forbedring og status

Neste spørsmål er om tiltaksaktiviteten i 2021 har endret etterlevelsen av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.[76] Har tiltakene forbedret graden av etterlevelse?

Forbedret etterlevelse

Figur 8 oppsummerer våre vurderinger av endringer i etterlevelsen av departementets policy fra 2020 til 2021. Vurderingene gjelder både informasjonssikkerhet og personvern.

Vår vurdering er at 16 av 21 universiteter og høgskoler hadde forbedret sin etterlevelsen av departementets policy i 2021 sammenliknet med 2020. Hos halvparten av disse 16 institusjonene var forbedringene tydeligere enn hos den andre halvparten. Den andre halvparten hadde derfor forbedret seg i noen grad sammenliknet med 2020.

Vår vurdering er at fem institusjoner verken hadde forbedret eller svekket sin etterlevelse av policyen – de befant seg på omtrent samme nivå som i 2020. Slik vi ser det, hadde ingen institusjoner svekket sin etterlevelse av policyen i løpet av fjoråret.

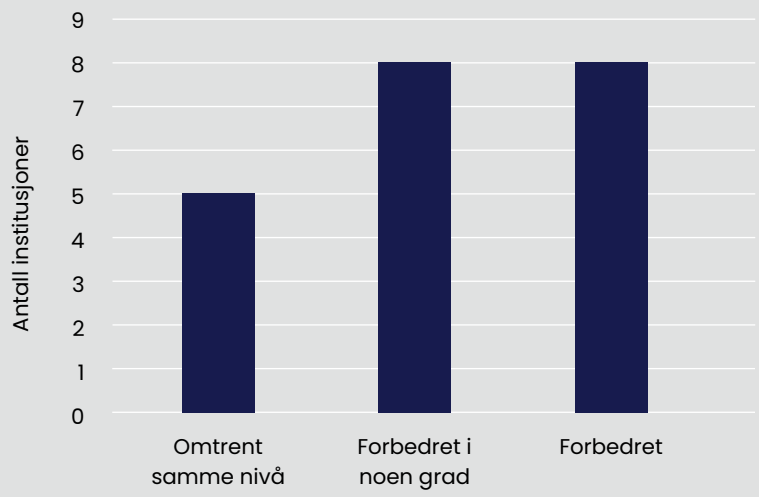
Forbedringene i etterlevelse var noe større fra 2020 til 2021 enn de var fra 2019 til 2020. Da mente vi halvparten av universitetene og høgskolene (10) ikke hadde forbedret sin etterlevelse av policyen jamført med året før. Vi antar at styrket etterlevelse i 2021 skyldes tiltaksaktiviteten drøftet

Policyetterlevelse – forbedringer og status

Vurderinger av etterlevelsen av kravene som departementets policy stiller til informasjonssikkerhet, inkludert sikring av personopplysninger, er basert på punktene 1-5 og 11-12 i policyen. Det legges særlig vekt på vurderinger av det forebyggende sikkerhetsarbeidet (risikostyring), involvering av toppledelsen og styret, og etablering og øving av beredskaps- og kontinuitetsplaner. Vi har også vurdert i hvilken grad øvrige oppgaver i ledelsessystemet for informasjonssikkerhet praktiseres i hele organisasjonen.

Vurderinger av etterlevelsen av kravene som departementets policy stiller til personvern (GDPR), er basert på punktene 6-12 i policyen. Det legges særlig vekt på vurderinger av arbeidet med protokoller over behandlingsaktiviteter, rutiner for ivaretakelse av de registrertes rettigheter og tiltak for å styrke kompetansen om personvernregelverket (personopplysningsloven og GDPR). Vi har også vurdert i hvilken grad øvrige deler av internkontrollen for GDPR (som ikke direkte gjelder sikring av personopplysninger) praktiseres i hele organisasjonen.

Figur 8: Forbedringer i etterlevelse av policy, 2020-2021



76 Se «Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

ovenfor. Vi har for eksempel bemerket at flere institusjoner rapporterte om styrket kapasitet (årsverksinnsats og innleid assistanse). Det er trolig at dette har bidratt til økt fremdrift i arbeidet med etterlevelse.

Hos enkelte institusjoner er det også trolig at styrket etterlevelse skyldes at ressurser har blitt tilbakeført til arbeidet med informasjonssikkerhet og personvern som følge av nedskalering av ekstraordinære tiltak for å håndtere pandemien.

Hvor var forbedringene størst?

Forbedringene i etterlevelse av policyen var størst når det gjelder kravene som omhandler informasjonssikkerhet (punktene 1-5 og 11-12 i policyen[77]). Hos åtte av de 16 institusjonene som rapporterte om forbedret etterlevelse, hadde forbedringene hovedsakelig skjedd innen informasjonssikkerhet.

Hos fire institusjoner var forbedringene størst når det gjelder krav til behandling av personopplysninger som omhandler andre forhold enn sikring av opplysningene.

De fire siste institusjonene hadde forbedret seg noe innen begge områder – både informasjonssikkerhet og personvern.

Status – etterlevelse av kravene til personvern (GDPR)

Figur 9 oppsummerer om forbedringene skissert ovenfor hadde ført til endringer i status når det gjelder personvernkravene i departementets policy (punktene 6-10 og 11-12 i policyen[78]). Ga forbedringene grunnlag for statusoppgradering med hensyn til personvern?

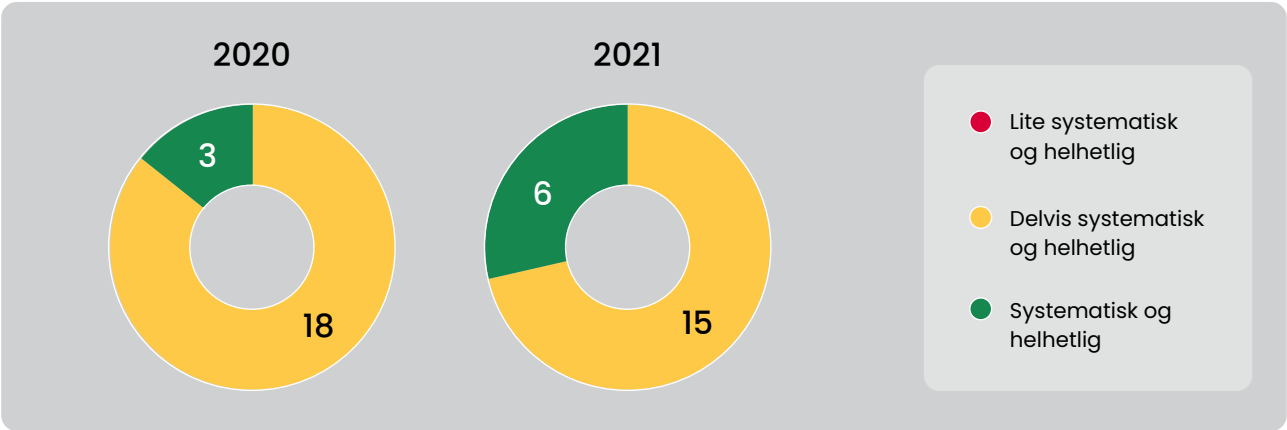
Statusvurderingen i figuren omfatter ikke kravene som stilles til sikring av personopplysninger. De inngår i statusen for arbeidet med informasjonssikkerhet i figur 10.

Figuren viser at i 2021 hadde seks institusjoner etablert et systematisk og helhetlig arbeid med personvern (internkontroll) som ivaretok policyens krav på tilfredsstillende måter. Dette er en dobling sammenliknet med 2020. Det betyr at disse seks institusjonene jobber langsiktig og planmessig med personvern. Samtidig er prinsippet om kontinuerlig forbedring godt institusjonalisert, og arbeidet har tydelig støtte fra toppledelsen og styret.

Hos de resterende 15 institusjonene var personvernarbeidet delvis systematisk og helhetlig. Disse institusjonene rapporterte derfor om enkelte avvik fra policyens personvernkrav som de har behov for å lukke. Avvikene gjaldt i særlig grad vanskeligheter med å gjøre interne rutiner og retningslinjer for behandling av personopplysninger kjent i hele organisasjonen. Dernest ble det opplyst om utfordringer med praktiseringen av rutinene og retningslinjene.

Ingen institusjoner ble vurdert til å jobbe lite systematisk og helhetlig – ad hoc og tilfeldig – med policyens personvernkrav. Heller ikke i 2020 fant

Figur 9: Status for etterlevelse av personvernkrav, 2020 og 2021



77 Se https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 27.05.2022.

78 Se https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 27.05.2022.

vi institusjoner som i svært liten grad etterlevde kravene til personvern.

Status – etterlevelse av kravene til informasjonssikkerhet

Figur 10 oppsummerer om forbedringene drøftet ovenfor hadde ført til statusoppgraderinger på informasjonssikkerhetsområdet, inkludert sikring av personopplysninger.

Av figuren ser vi at forbedringene i 2021 ikke hadde ført til endringer i status med hensyn til etterlevelse av krav til sikring av informasjonsverdier. Som i 2020, var det tre institusjoner som hadde et systematisk og helhetlig informasjonssikkerhetsarbeid. Det innebærer at arbeidet omfatter alle deler av kjernevirksomheten, det er tydelig forankret hos toppledelsen og styret, og prinsippet om kontinuerlig forbedring er tilfredsstillende institusjonalisert.

De resterende 18 universitetene og høgskolene beholdt sin 2020-status: de jobber delvis systematisk og helhetlig med informasjonssikkerhet, men har enkelte viktige avvik fra policyens krav. De største utfordringene for disse institusjonene er å ferdigstille innføringen av ledelsessystemer for informasjonssikkerhet, spesielt at ledere og medarbeidere med sentrale roller i arbeidet er kjent med og har den nødvendige kompetansen til å ivareta sine oppgaver og ansvar.

Hos flere av institusjonene kan det også være behov for å forbedre kapasiteten (årsverksinnsatsen) slik at arbeidet med informasjonssikkerhet får tilstrekkelig tyngde.

Forbedringer uten statusendring

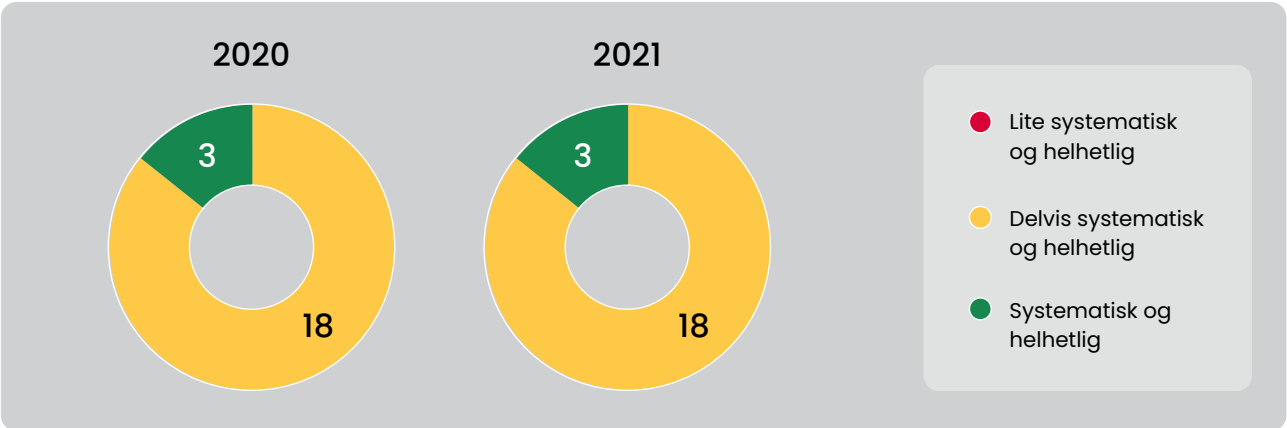
Selv om vi ikke finner grunnlag for statusendringer på informasjonssikkerhetsområdet, er det likevel innen dette området at forbedringene i policyetterlevelse var størst i 2021. Vår vurdering er derfor at veien mot målet (tilfredsstillende etterlevelse av kravene til informasjonssikkerhet) er blitt kortere i 2021, men at flertallet av institusjonene enda ikke har brutt mållinjen.

Forskjellen mellom rapporterte sårbarheter og iverksatte tiltak kan bidra til å forklare hvorfor mange institusjoner hadde forbedret arbeidet med informasjonssikkerhet, men uten at status for etterlevelse av departementets policy hadde endret seg like mye. Institusjonene gjør viktige fremskritt, men spørsmålet er om fremskrittene alltid skjer på de områder hvor etterlevelsen er mest utfordrende.

Forbedringer uten statusendring indikerer også at utviklingspotensialet er størst innen informasjonssikkerhet. I kapittel 2 så vi for eksempel at reglene om sikring av informasjonsverdier som er undergitt eksportkontroll, kan være utfordrende for mange institusjoner.

Dessuten ble viktige oppgaver innen informasjonssikkerhet satt på vent i 2020 på grunn av pandemien. Deler av forbedringene i 2021 handlet derfor om at etterslepet fra 2020 ble tatt igjen – utsatte oppgaver ble gjennomført.

Figur 10: Status av krav til informasjonssikkerhet, 2020 og 2021



Forventninger til 2022

To institusjoner etterlevde alle kravene i departementets policy for informasjonssikkerhet og personvern på en tilfredsstillende måte i 2021. Det gjorde de også i 2020. Vi forventer oss at disse to vil opprettholde og styrke sin etterlevelse av policyen i 2022.

I det følgende vurderer vi sannsynligheten for at også de øvrige universitetene og høgskolene vil kunne etterleve departementets policy i 2022. Vi har delt de 19 institusjonene inn i tre sannsynlighetskategorier. Hver kategori indikerer hvor trolig vi mener det er at tilfredsstillende etterlevelse kan oppnås i løpet av 2022.

- **Etterlevelse sannsynlig:** Vi mener det er sannsynlig at fem universiteter og høgskoler kan etterleve policyens krav på tilfredsstillende måter i 2022. Forutsetningen er at disse institusjonene har minst like stor fremgang i arbeidet med informasjonssikkerhet og personvern i 2022 som i 2021.

- **Etterlevelse mulig:** Vi mener det er mulig at seks universiteter og høgskoler vil kunne etterleve kravene i policyen på tilfredsstillende måter i 2022. For disse institusjonene vil det imidlertid kreve større forbedringer i arbeidet med informasjonssikkerhet og personvern enn hva vi har sett hos dem tidligere. Vi regner det derfor som noe mer usannsynlig enn sannsynlig at de vil kunne etterleve policyen allerede i 2022.

- **Etterlevelse lite sannsynlig:** Vi mener det er lite sannsynlig at de resterende åtte universitetene og høgskolene vil kunne etterleve policyens krav på tilfredsstillende måter i 2022. Vår vurdering er at disse institusjonene vil trenge noe lengre tid enn de øvrige på å oppnå tilfredsstillende etterlevelse.

Enkelte av institusjonene i den siste kategorien (etterlevelse lite sannsynlig) regnet med at tilfredsstillende etterlevelse var to-tre år unna. Her ble det spesielt pekt på at det vil ta tid å innføre ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR) på fakultets- og instituttnivå.

Om sannsynlighetskategoriene

Vi benytter følgende sannsynlighetsverdier i vurderingen av om tilfredsstillende etterleve av kravene i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern vil kunne oppnås i 2022:

- **Sannsynlig:** det er sannsynlighetsovervekt for at institusjonen vil kunne overholde kravene i policyen ved utgangen av 2022 (mer enn 50 prosent sannsynlighet).

- **Mulig:** det er mer usannsynlig enn sannsynlig at institusjonen vil kunne overholde kravene i policyen ved utgangen av 2022 (mer enn 30 prosent og 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 2022 (mindre enn 30 prosent sannsynlighet).

Oppsummering og anbefalinger

De 21 universitetene og høgskolene oppga at kompetanse og bevissthet var de viktigste sårbarhetene i arbeidet med informasjonssikkerhet og personvern. Dette ble vurdert å være de viktigste sårbarhetene også i 2020, 2019 og 2018.

Tekniske sårbarheter (sikkerhetshull i programvare) og kapasitetsmangler (for få «hender i arbeid») ble nevnt som viktige av flere institusjoner i 2021 enn tidligere. Årets kartlegging tyder på at begge sårbarhetene prioriteres ved valg av tiltak.

Det var likevel noen forskjeller mellom rapporterte sårbarheter og iverksatte tiltak hos de 21 universitetene og høgskolene. Det kommer særlig til uttrykk ved at kompetanse og bevissthet ble vurdert som de klart viktigste sårbarhetene, mens tiltak som adresserer disse sårbarhetene – pedagogiske tiltak – utgjorde det tredje største tiltaksområdet (tredje flest rapporterte tiltak). Samtidig var organisatoriske mangler den sårbarheten som færrest institusjoner mente var viktig. Organisatoriske tiltak var likevel det største tiltaksområdet (flest rapporterte tiltak).

Vår vurdering er at to institusjoner etterlevde departementets policy på tilfredsstillende måter i 2021. Vi mener det er sannsynlig at ytterligere fem institusjoner vil kunne etterleve kravene i policyen i løpet av 2022. For de øvrige institusjonene er dette mindre eller lite sannsynlig.

Med bakgrunn i kartleggingsfunnene presentert i dette kapitlet, vil vi fremheve betydningen av kompetanse og opplæring. Vi mener at sektortiltak innen disse områdene vil gjøre størst forskjell både med hensyn til (i) etterlevelse av departementets policy og (ii) redusere risikoen for brudd på informasjonssikkerheten og krenkelser av personvernet.

Vi anbefaler derfor at det iverksettes sektortiltak som bidrar til å redusere forskjellen mellom tilbudet av og etterspørselen etter opplæring og kompetanseheving. Slike tiltak inngår allerede i gjeldende sektorinitiativ,[79] men gjennomføringen av tiltakene bør styrkes. Det bør også vurderes om dagens kompetanse- og opplæringstilbud svarer godt nok på institusjonenes behov.

79 Se for eksempel https://www.uninett.no/cybersikkerhetssenteret. Sist besøkt 25.05.0222.

Kapittel 4

Øvrige virksomheter – forvaltningsorganer og selskaper

Kapittel 4

Øvrige virksomheter – forvaltningsorganer og selskaper

Innledning

Sju øvrige virksomheter – forvaltningsorganer og selskaper – omfattes av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern. Det er følgende virksomheter:

- Sikt – kunnskapssektorens tjenesteleverandør.
- Norges forskningsråd (NFR).
- Nasjonalt organ for kvalitet i utdanningen (NOKUT).
- Simula.
- Norsk utenrikspolitisk institutt (NUPI).
- De nasjonale forskningsetiske komiteene (FEK).
- Universitetssenteret på Svalbard (UNIS).[80]

Disse virksomhetene hadde til sammen omkring 1100 ansatte i 2021. Flest ansatte hadde NFR (ca. 450[81]) og færrest var det hos FEK (11[82]). Sektorens nye tjenesteleverandør – Sikt – hadde omkring 370 ansatte.[83]

Enkelte av virksomhetene driver forskning og undervisning. UNIS hadde for eksempel 299 studenter i 2020.[84] Ved Simula og NUPI deltar studenter og ph.d.-kandidater i prosjekter og mottar veiledning.

Resten av kapitlet

Nedenfor følger først en kort drøftelse av digitale avhengigheter og informasjonsverdier i denne delen av UH-sektoren.

Så følger en oversikt over (i) brudd og hendelser hos virksomhetene i 2021, (ii) sårbarheter som virksomhetene rapporterte om i arbeidet med informasjonssikkerhet og personvern, og (iii) tiltak som de hadde iverksatt i 2021 for å utbedre sårbarhetene.

Til slutt gis en vurdering av status for etterlevelse av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.

Spesielt om Sikt – kunnskapssektorens tjenesteleverandør

Sikt ble opprettet 1. januar 2022. Men ettersom årets kartlegging gjelder for 2021, var det ikke aktuelt med en ordinær gjennomgang av arbeid med informasjonssikkerhet og personvern denne gangen. Vi ba derfor om en foreløpig status fra Sikt om arbeidet innen disse områdene. Det betyr at Sikt ikke inngår i drøftelsene og vurderingene som presenteres i dette kapitlet.

---

80 I tillegg omfattes Direktoratet for høyere utdanning og kompetanse (HK-dir) av departementets styringsmodell. Kunnskapsdepartementet er ansvarlig for styringen av HK-dir sitt arbeid med informasjonssikkerhet og personvern.

81 NFR årsrapport 2020, side 12. https://www.forskningsradet.no/siteassets/publikasjoner/2021/arsrapport-2020_endelig.pdf. Sist besøkt 25.05.2022.

82 FEK årsrapport 2020, side 5. https://www.forskningsetikk.no/globalassets/dokumenter/arsrapporter/fek/2020/arsrapport-2020.pdf. Sist besøkt 25.05.2022.

83 Se https://sikt.no/om-sikt. Sist besøkt 25.05.2022.

84 UNIS Annual Report, side 6. https://www.unis.no/wp-content/uploads/2021/05/UNIS_Annual_Report_2020_web.pdf. Sist besøkt 25.05.2022.

Informasjonsverdier og avhengigheter

De sju øvrige forvaltningsorganene og selskapene forvalter viktige informasjonsverdier. Sikt forvalter for eksempel informasjonsverdier på vegne av hele sektoren, inkludert forskningsnettet i Norge, i tillegg til andre digitale tjenester og infrastruktur, blant annet tungregneanlegg.[85] Datterselskapet Sigma2 er sentral i denne forbindelse.

Enkelte av virksomhetene forvalter i tillegg informasjonsverdier innenfor viktige kunnskapsområder. Det dreier seg blant annet om områder som kryptologi, sikkerhets- og forsvarsstudier og utenrikspolitikk. UNIS gjennomfører forskning innenfor områder som biologi, geologi, geofysikk og arktisk teknologi.[86]

Oversikt over informasjonsverdier

Størrelsen på de øvrige forvaltningsorganene og selskapene gjør likevel at de forvalter færre informasjonsverdier enn universitets- og høgskoledelen av sektoren. Samtidig er «verdilandskapet» mindre komplekst. Det innebærer for eksempel at omfanget av personopplysninger som behandles er begrenset sammenliknet med mange av universitetene og høgskolene.

Organisasjonsstørrelse og «verdilandskapets» struktur fører til at disse virksomhetene har en enklere jobb med å få oversikt over hvilke informasjonsverdier de forvalter. Hos enkelte av virksomhetene ble det likevel opplyst om utfordringer med etablering av fullstendige oversikter over behandlinger av personopplysninger (protokoll). Som hos universitetene og høgskolene, handlet dette delvis om mangel på egnede arbeidsverktøy for registrering og vedlikehold av slike oversikter.

Digitale avhengigheter

Årsrapportene til de seks virksomhetene gir indikasjoner på at «verdilandskapet» blir mer komplekst og at avhengigheten av digitale løsninger øker.

NOKUT sier for eksempel i årsrapporten for 2020 at digitalisering og forbedringer på IKT-området, er en viktig del av arbeidet med å utvikle og effektivisere organisasjonen. Søknads- og saksbehandlingssystemet eSam står sentralt i dette arbeidet.[87] NOKUT uttrykker videre at manglende kompetanse og kapasitet til forvaltning av nye IKT-systemer vil kunne føre til svakere informasjonssikkerhet og driftssikkerhet. Dette kan svekke måloppnåelsen innenfor andre kjerneområder.[88]

NFR opplyser om «(…) vedvarende og omfattende digitalisering» i sin årsrapport.[89] Blant annet er deler av søknadsbehandlingen digitalisert ved hjelp av robotteknologi og kunstig intelligens. Også andre prosesser er digitalisert (anskaffelsesprosessen). NFR oppgir at dette har gitt gevinster, blant annet i form av bedre utnyttelse av kompetanse og ressurser.

NUPI, UNIS og FEK fremhever i sine årsrapporter betydningen av digitalisering innen utdanning og formidling. Dette handler særlig om nettbasert publisering og annen utadrettet virksomhet, digital undervisning og veiledning, og digitale eksamener og disputaser.[90]

85 Se Sikt sin tjenesteoversikt. https://sikt.no/tjenesteoversikt. Sist besøkt 25.05.2022.

86 UNIS Strategy 2025. https://www.unis.no/wp-content/uploads/2019/04/UNIS_Strategy_2025_web.pdf. Sist besøkt 25.05.2022.

87 NOKUT årsrapport 2020, side 72. https://www.nokut.no/siteassets/om-nokut/arsrapporter-og-tildelingsbrev/2020/nokut-arsrapport-2020.pdf. Sist besøkt 25.05.2022.

88 NOKUT årsrapport 2020, side 61. https://www.nokut.no/siteassets/om-nokut/arsrapporter-og-tildelingsbrev/2020/nokut-arsrapport-2020.pdf. Sist besøkt 25.05.2022.

89 NFR årsrapport 2020, side 11. https://www.forskningsradet.no/siteassets/publikasjoner/2021/arsrapport-2020_endelig.pdf. Sist besøkt 25.05.2022.

90 Se for eksempel NUPI årsrapport 2020, side 12-14. https://www.nupi.no/om-nupi/aarsrapporter-og-revisjonsberetninger. Sist besøkt 25.05.2022. Se også UNIS Annual Report, side 5-6. https://www.unis.no/wp-content/uploads/2021/05/UNIS_Annual_Report_2020_web.pdf. Sist besøkt 25.05.2022.

Brudd og hendelser

Virksomhetenes informasjonsverdier er i utgangspunktet utsatt for de samme truslene som beskrevet i kapittel 2. Det er likevel noen forskjeller med hensyn til typer brudd og hendelser sammenliknet med universitetene og høgskolene. Vi kommer tilbake til dette nedenfor.

På grunn av omorganiseringen av denne delen av UH-sektoren i 2021, har vi opplysninger om saker – brudd og hendelser – fra færre virksomheter enn i 2020. Det var derfor seks virksomheter som rapporterte om brudd og hendelser i 2021 mot ni i 2020.

Nedgangen i antallet kartlagte virksomheter, bidrar trolig til å forklare nedgangen i antallet rapporterte brudd og hendelser fra 2020 til 2021. I 2020 ble det til sammen opplyst om 95 brudd og hendelser. Det samlede antallet saker for 2021 var 23. Én av virksomhetene hadde ikke registrert brudd eller hendelser i 2021.

I tillegg ble det rapportert om hendelser som det var vanskelig å anslå omfanget av. Disse hendelsene inngår ikke i det totale antallet rapporterte saker.

Hendelsesprofilen

Brudd og hendelser som ble registrert i denne delen av sektoren i 2021, gjaldt i all hovedsak

(i) menneskelige eller tekniske feil og uhell,
(ii) avvik fra egne informasjonssikkerhets- eller personvernrutiner, og
(iii) forsøk på nettsvindel.

Eksempler på saker hvor feil og uhell ble oppgitt å være årsaken, var lagring av personopplysninger på usikre lagringsområder, feilsending av brev med skjermverdig informasjon eller nedetid på IT-systemer på grunn av maskinvarefeil. Manglende eller mangelfulle databehandleravtaler, manglende oppdatering av oversikter over personopplysninger (behandlingsprotokoll) og manglende avslutning av brukerkontoer ved opphør av ansettelsesforhold, var eksempler på rapporterte avvik fra virksomhetenes egne rutiner. Forsøk på nettsvindel handlet primært om faktura- og direktørsvindel.

Det ble også rapportert om enkelte saker som gjaldt sårbarheter i datatjenester, og nye IT-tjenester som ble tatt i bruk uten at risikoen for brudd på informasjonssikkerheten var vurdert.

Ingen av virksomhetene rapporterte om løsepengevirus, tjenestenekt (DDoS) eller misbruk av datamaskiner til utvinning av kryptovaluta (Bitcoin, Monero, osv.).

Statlig hacking og datainntrenging

Det ble ikke rapportert om bekreftede eller mistenkte tilfeller av statlig hacking eller forsøk på datainntrenging i epostsystemer (slik som hos en del av universitetene og høgskolene). Det ble heller ikke opplyst om rekognoseringsaktivitet, for eksempel at virksomhetenes datanettverk hadde vært skannet for sårbarheter. Det ble imidlertid rapportert om ett forsøk på datainntrenging. Forsøket mislyktes, og hendelsen ble rapportert til NSM.

Vi har sett at universitetene og høgskolene meldte flere brudd på personopplysningssikkerheten til Datatilsynet i 2021 enn tidligere. Det står i kontrast til hva de øvrige forvaltningsorganene og selskapene rapporterte om. Her hadde én av virksomhetene vært i dialog med Datatilsynet om et sikkerhetsbrudd som gjaldt manglende tilgangsstyring. Andre saker enn dette ble ikke meldt til Datatilsynet. Heller ikke i 2020 ble det meldt saker til Datatilsynet fra disse virksomhetene.

Skadevirkninger

Virksomhetene mente at hendelsene og avvikene ikke hadde ført til alvorlige skadevirkninger. Det innebar for eksempel at sakene som gjaldt faktura- og direktørsvindel ikke hadde ført til urettmessige utbetalinger.

I saker som omhandlet feilaktig lagring eller feilsending av personopplysninger, var det imidlertid snakk om mindre krenkelser av personvernet. Her dreide det seg likevel om få og lite sensitive opplysninger. Bruddene ble ikke vurdert som så alvorlige at de var meldepliktige til Datatilsynet.

I tillegg ble det rapportert om noe ekstraarbeid og tapt arbeidstid i forbindelse med håndtering av rutineavvik og nedetid på systemer.

Sårbarheter

Virksomhetene ble bedt om å vurdere hvilke sårbarheter som påvirket deres arbeid med informasjonssikkerhet og personvern. Figuren nedenfor gir en samlet oversikt over hovedtyper sårbarheter som det ble rapporterte om.

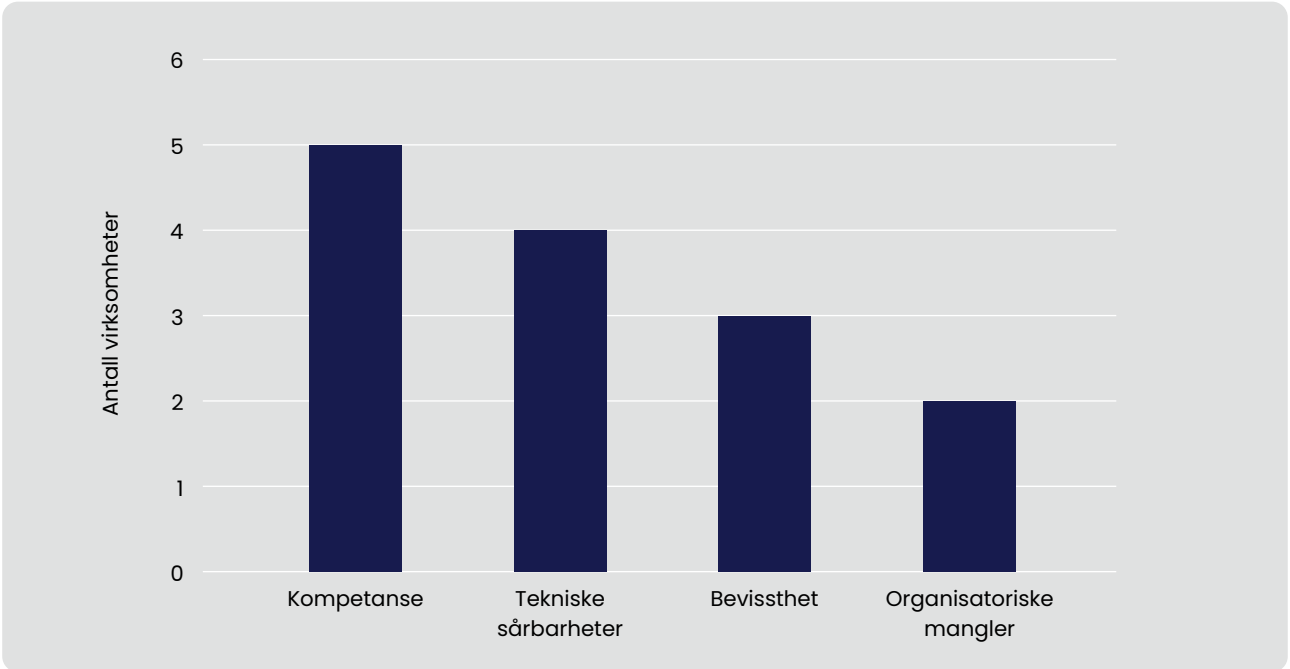
Stolpene i figuren viser antallet virksomheter som opplyste om at sårbarhetene var viktige utfordringer i arbeidet med informasjonssikkerhet og personvern.

Kompetanse ble vurdert som den viktigste sårbarheten også hos disse forvaltningsorganene og selskapene. Det handlet om at ledere eller medarbeidere som var ment å spille sentrale roller i arbeidet med informasjonssikkerhet og personvern, spesielt system- eller tjenesteeiere, ikke hadde tilstrekkelig praktisk kunnskap om de oppgavene de var forventet å løse.

Tekniske sårbarheter – særlig sikkerhetshull i programvare og ustabile IT-systemer – ble vurdert som den nest viktigste sårbarheten. Manglende brukerbevissthet (grunnleggende kunnskap om informasjonssikkerhet og personvern blant ledere og medarbeidere) ble vurdert som tredje viktigst. Organisatoriske mangler, spesielt uklar ansvars- og oppgavefordeling og manglende rutiner for sikker og lovlig behandling av personopplysninger, ble oppgitt som viktige sårbarheter av færrest virksomheter.

Ingen av virksomhetene oppga at kapasitet (årsverksinnsats) var en viktig sårbarhet. Dette avviker fra rapporteringen i 2020. Da var det flere virksomheter som mente at dette var en viktig utfordring. Det skiller seg også fra vurderingene til universitetene og høgskolene (se kapittel tre).

Figur 11: Virksomhetenes sårbarhetsprofil, 2021



Kapasitetstiltak

Kapasitet (årsverksinnsats) ble altså ikke oppgitt å være en vesentlig sårbarhet. Det ble likevel rapportert om at den samlede årsverksinnsatsen hos virksomhetene hadde økt med drøyt to årsverk i 2021.

Det var én av virksomhetene som sto for mesteparten av økningen. Økningen hadde skjedd i form av innleie, det vil si advokatbistand og avtale med et sikkerhetsselskap om levering av tjenester for deteksjon av digitale sikkerhetshendelser.

Hos de øvrige virksomhetene hadde antallet årsverk i arbeidet med informasjonssikkerhet og personvern endret seg lite.

Andre viktige tiltak i 2021

Virksomhetene ble spurt om hvilke andre tiltak enn kapasitetstiltak de hadde iverksatt i 2021 for å styrke arbeidet med informasjonssikkerhet og personvern.

Figur 12 gir en oversikt over antall og hovedtyper[91] tiltak som virksomhetene opplyste om.

Figuren viser at det totalt ble rapportert om 58 informasjonssikkerhets- og personverntiltak i 2021. Det er noen færre enn i 2020. Da var det totale antallet rapporterte tiltak 66. I 2021 ble imidlertid seks virksomheter kartlagt mot ni i 2021. Sett i lys av dette, kan vi si at tiltaksaktiviteten hadde økt noe sammenliknet med 2020.

Virksomhetene rapporterte om flest organisatoriske tiltak (22), mens tekniske tiltak var den nest største tiltakskategorien (18). Deretter fulgte pedagogiske (15) og juridiske tiltak (3).

Dette er omtrent den samme rangeringen som i 2020. Forskjellen er at i 2021 hadde pedagogiske og tekniske tiltak byttet plass sammenliknet med året før. I 2020 var pedagogiske tiltak den nest største tiltakskategorien, mens tekniske tiltak inntok tredjeplassen.

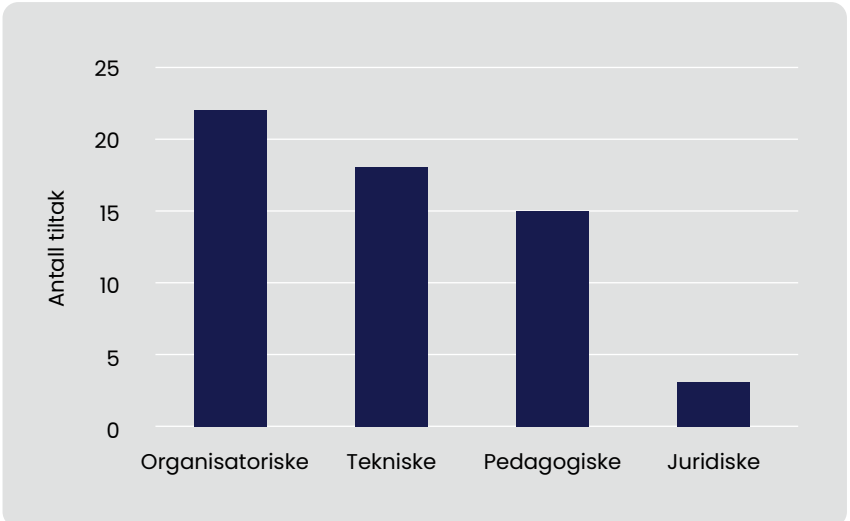
Sikkerhetstest og tekniske tiltak

Plassbyttet i rangordningen mellom tekniske og pedagogiske tiltak, kan skyldes sikkerhetstesten (sårbarhetsskannet) som Uninett gjennomførte i sektoren i mai 2021 (testen er omtalt tidligere i denne rapporten).

Fire av virksomhetene fikk positive evalueringer i rapportene som de mottok fra Uninett. De hadde, ifølge Uninett, enten gjort en gjennomgående god jobb eller hadde et lite fotavtrykk av sårbare maskiner som kunne nås via internettet.

Den siste virksomheten fikk kritiske merknader. Virksomheten hadde svart på kritikken ved å iverksette en rekke tekniske sikringstiltak for

Figur 12: Informasjonssikkerhets- og personverntiltak, 2021



91 Tiltakskategoriene er definert i kapittel tre.

å styrke den digitale sikkerheten. Også de øvrige virksomhetene hadde iverksatt tekniske tiltak som følge av resultatene fra testen.

Tiltaksprofil

De fleste virksomhetene hadde iverksatt eller var i ferd med å gjennomføre både organisatoriske, tekniske og pedagogiske tiltak. Det var bare én virksomhet som ikke hadde gjennomført pedagogiske tiltak i 2021. Tre virksomheter rapporterte om juridiske tiltak.

De viktigste organisatoriske tiltakene gjaldt ferdigstillelse eller revisjon av ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR). I tillegg var det stort fokus på utarbeidelse av rutiner for sikring og behandling av personopplysninger, og kartlegging av slike behandlinger (utarbeidelse av behandlingsprotokoller). Sikkerhetsorganisering – fordeling av ansvaret for viktige oppgaver – ble fremhevet av flere virksomheter som prioriterte tiltak i 2021.

Som antydet ovenfor, gjaldt de vanligste tekniske tiltakene lukking av sikkerhetshull avdekket under Uninett sin sikkerhetstest (sårbarhetsskann). To virksomheter rapporterte i tillegg om at sikring av mobile dataenheter var et viktig tiltaksområde. Like mange virksomheter opplyste om at forbedring av nettverks- og epostsikkerheten – anskaffelse av ny brannmurløsning og epostfilte – ble prioritert. Det ble også rapportert om tiltak for å styrke evnen til å oppdage digitale sikkerhetshendelser.

Pedagogiske tiltak handlet primært om grunnleggende opplæring av ledere og medarbeidere i informasjonssikkerhet og personvern, vanligvis i form av e-læring. Hos én av virksomhetene ble effekten av opplæringen målt og evaluert. Det ble i liten grad opplyst om særskilt opplæring av ansatte med sentrale roller i arbeidet med informasjonssikkerhet og personvern. Dette hadde skjedd hos én virksomhet.

Alle de juridiske tiltakene gjaldt oppfølging av Schrems II-dommen.

Tiltakene dreide seg derfor om gjennomgang av avtaler med leverandører av digitale tjenester som overførte personopplysninger til land utenfor EU/EØS, inkludert kartlegginger av slike overføringer.

Sårbarheter og tiltak

Dersom vi sammenlikner rapporterte sårbarheter og iverksatte tiltak, ser vi at fem av virksomhetene mente at pedagogiske sårbarheter (bevissthet og kompetanse) var viktige utfordringer i arbeidet med informasjonssikkerhet og personvern. Likevel ble det rapportert om flest organisatoriske og tekniske tiltak. Pedagogiske tiltak var noe mindre vanlig.

Som blant universitetene og høgskolene, var det derfor et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak. Forskjellen var imidlertid mindre enn hos universitetene og høgskolene. Iverksatte tiltak synes derfor å sammenfalle noe bedre med rapporterte sårbarheter i denne delen av sektoren enn i universitets- og høgskoledelen.

Status – etterlevelse av kravene til personvern (GDPR)

I figur 13 nedenfor gir vi vår vurdering av om tiltakene drøftet ovenfor hadde ført til endringer i status når det gjelder etterlevelsen av de særskilte personvernkravene i departementets policy for informasjonssikkerhet og personvern (punktene 6-10 og 11-12 i policyen[92]).

Statusvurderingen i figuren omfatter ikke kravene som stilles til sikring av personopplysninger. De inngår i statusen for arbeidet med informasjonssikkerhet i figur 14.

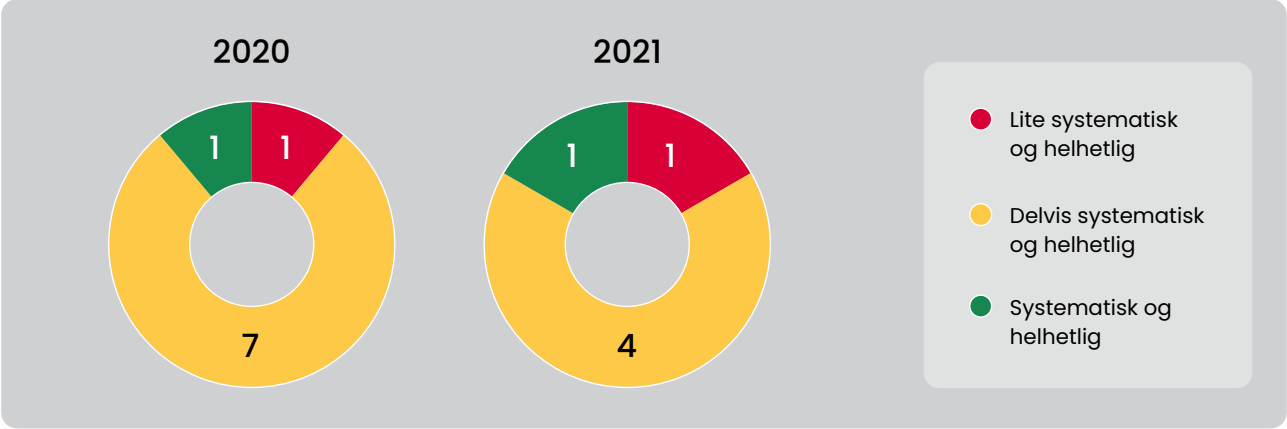
Om statusvurderingene

Sammenlikning av status for 2021 og 2020 i figur 13 og 14, er noe haltende. Årsaken til dette er konsekvensene av omorganiseringen i denne delen av sektoren i 2021. Omorganiseringen innebærer at nye virksomheter har kommet til og andre har forsvunnet siden 2020. Sammenlikningen er derfor bare meningsfull for de seks virksomhetene som ble videreført – NFR, NOKUT, Simula, NUPI, UNIS og FEK.

Uninett og NSD ble vurdert i 2020, men var avviklet da årets kartleggingsrunde ble gjennomført.

Kriteriene for vurdering av status i figur 13 og 14 er de samme som for universitetene og høgskolene. Kriteriene er gjort rede for i kapittel 3.

Figur 13: Status for etterlevelse av personvernkrav, 2020 og 2021



Figuren viser at vi ikke har endret status for etterlevelse av policyens krav til arbeidet med personvern (GDPR) for de virksomhetene som ble videreført etter omorganiseringen i sektoren. Det betyr at én virksomhet vurderes å ha et systematisk og helhetlig personvernarbeid. Denne virksomheten jobber langsiktig og planmessig med personvern (GDPR), prinsippet om kontinuerlig forbedring er tilfredsstillende institusjonalisert, og arbeidet har tydelig støtte fra toppledelsen og styret.

Vår vurdering er at ytterligere fire virksomheter var i ferd med å tilfredsstille kravene i policyen i 2021: personvernarbeidet var delvis systematisk og helhetlig. Det betyr at disse virksomhetene hadde enkelte avvik fra departementets policy som de har behov for å lukke. Alle fire var imidlertid kommet såpass langt i etterlevelsesarbeidet at vi mener det er sannsynlig at de kan endre status fra «gul» til «grønn» i løpet av 2022.

Når det gjelder den sjette og siste virksomheten, mener vi at etterlevelsen av personvernkravene i policyen er lite systematisk og helhetlig.

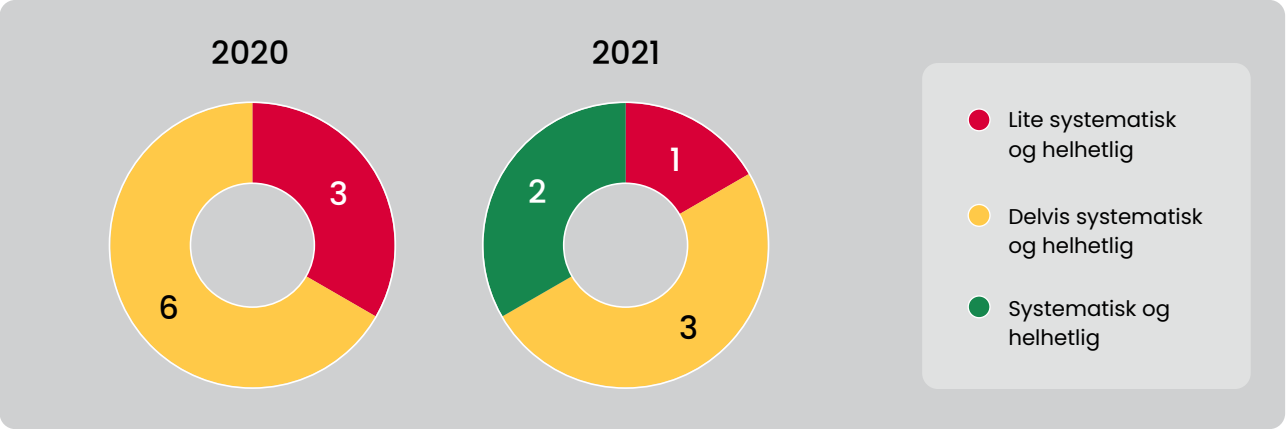
92 Se https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 27.05.2022.

Status – etterlevelse av kravene til informasjonssikkerhet

Figur 14 gir en oversikt over hvor virksomhetene sto i relasjon til kravene som departementets policy stiller til arbeidet med informasjonssikkerhet (punktene 1-5 og 11-12 i policyen[93]).

Statusvurderingen omfatter også kravene til sikring av personopplysninger.

Figur 14: Status for etterlevelse av krav til informasjonssikkerhet, 2020 og 2021



Figuren viser positiv endring fra 2020 til 2021. Det skyldes at to virksomheter, som begge lå godt an i 2020, hadde styrket sitt arbeid med informasjonssikkerhet i 2021. Begge har derfor endret status fra «gul» til «grønn». Som nevnt ovenfor, innebærer dette at de to virksomhetene jobber langsiktig og planmessig med informasjonssikkerhet, prinsippet om kontinuerlig forbedring er institusjonalisert, og arbeidet har støtte fra toppledelsen.

Én av de andre virksomhetene har også endret status med hensyn til etterlevelse, men her er det snakk om en mer beskjeden forbedring – fra «rød» til «gul» (fra lite systematisk og helhetlig til delvis systematisk og helhetlig). På «gult» nivå finner vi ytterligere to virksomheter. Begge disse har beholdt sin status sammenliknet med 2020.

Hos den siste virksomheten hadde det ikke skjedd vesentlige forbedringer i etterlevelsen av kravene til informasjonssikkerhet. Virksomheten har derfor beholdt sin «røde» status fra 2020.

Vi mener at to av de «gule» virksomhetene var kommet såpass langt i sin etterlevelse av kravene til informasjonssikkerhet at det er sannsynlig med statusoppgradering i 2022 (fra «gul» til «grønn»). For de to siste virksomhetene er vurderingen at statusendring er mindre sannsynlig.

93 Se https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 27.05.2022.

Oppsummering og anbefalinger

De øvrige forvaltningsorganene og selskapene har et mindre omfattende og komplekst «verdilandskap» enn universitetene og høgskolene. Det avspeiler seg i de bruddene og hendelsene som virksomhetene rapporterte om i 2021. Sakene gjaldt i hovedsak feil og uhell, avvik fra egne rutiner og forsøk på nettsvindel. Det ble ikke rapportert om bekreftet eller mistenkt statlig hacking.

De seks virksomhetene opplyste om de samme sårbarhetene i arbeidet med informasjonssikkerhet og personvern som universitetene og høgskolene. Kompetanse ble vurdert som den største utfordringen, fulgt av tekniske sårbarheter og organisatoriske mangler.

Det var et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak, spesielt at det var gjennomført færre pedagogiske tiltak enn hva sårbarhetsprofilen i denne delen av sektoren skulle tilsi. Sårbarheter og tiltak korresponderte likevel bedre enn hos universitetene og høgskolene.

Selv om vi ikke fant at andre enn én virksomhet hadde tilfredsstillende etterlevelse av personvernkravene i departementets policy i 2021, mener vi det er sannsynlig at fire andre kan oppnå det samme i 2022.

To av virksomhetene har, slik vi vurderer det, tilfredsstillende etterlevelse av kravene til informasjonssikkerhet i departementets policy. Vi mener det er sannsynlig at to andre virksomheter kan oppnå samme status i 2022.

Vi kan ikke se at det er behov for særskilte sektortiltak rettet mot de øvrige forvaltningsorganene og selskapene. Våre anbefalinger for universitetene og høgskolene gjelder derfor også for disse virksomhetene. Det betyr, etter vår oppfatning, at det også i denne delen av sektoren er spesielt viktig med sektortiltak innen opplæring og kompetanseheving.

Kapittel 5

Risiko, mål og anbefalinger

Kapittel 5

Risiko, mål og anbefalinger

Innledning

I dette kapitlet følger først en vurdering av risikoen for konkrete hendelser som kan føre til at sektorens informasjonsverdier ødelegges, går tapt, eksponeres for uvedkommende eller at personopplysninger håndteres på uforsvarlige måter. Vurderingene av risiko baserer seg på drøftelsene i de tidligere kapitlene.

Deretter drøfter vi mulighetene for oppnåelse av hovedmålene for informasjonssikkerhet og personvern i Kunnskapsdepartementets strategi for digital omstilling, 2021-2025.[94] En forutsetning for å nå målene, er tilfredsstillende etterlevelse av departementets policy for informasjonssikkerhet og personvern.[95] Graden av policyetterlevelse gir derfor en indikasjon på mulighetene for måloppnåelse.

Til slutt oppsummerer vi våre anbefalinger til sektortiltak for å styrke arbeidet med informasjonssikkerhet og personvern i UH-sektoren.

Før vi vurderer risiko for konkrete brudd på informasjonssikkerheten og krenkelser av personvernet, vil vi også denne gangen gi vår vurdering av generelle risiko i sektoren. Dette er en overordnet vurdering av hvordan sentrale utviklingstrekk på informasjonssikkerhets- og personvernområdet drøftet i tidligere kapitler, påvirker risiko på sektornivå.[96]

Generelle risiko i sektoren

Vi mener at risiko i sektoren er omtrent den samme som i 2020. Risikonivået er derfor, slik vi ser det, fortsatt høyt i viktige deler av sektoren.[97]

Vår begrunnelse for denne konklusjonen handler om følgende forholdet:

Informasjonsverdier

Sektoren mangler tilfredsstillende oversikt over alle sine informasjonsverdier: data, opplysninger, datamaskiner og IT-systemer. Samtidig er avhengigheten av disse verdiene økende i alle deler av kjernevirksomheten.

Verdioversikter er mest dekkende når det gjelder behandling av personopplysninger i forskning. Her er det etablert fellestjenester hos Sikt hvor forsknings- og studentprosjekter som behandler personopplysninger skal registreres. Tilsvarende oversikter

94 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 25.05.2022.

95 Policyen er kommunisert til sektoren i rundskriv F-04-20. Se https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 25.05.2022.

96 Vurderingen av generelle risiko gjelder for de deler av sektoren som inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern. Den gjelder ikke for de delene av sektoren som vi ikke har kartlagt. Vi antar likevel at vurderingen også vil ha en viss relevans der.

97 Se «Risiko- og tilstandsvurdering 2021», kapittel 5, side 61-62. https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning. Sist besøkt 20.05.2022.

finnes i mindre grad i administrasjon og i forskning hvor andre informasjonsverdier enn personopplysninger behandles.

Flere institusjoner opplyste om at de har iverksatt eller planla initiativ for å få oversikt over forskning som omfattes av krav til eksportkontroll og internasjonal kunnskapsoverføring.

Arbeidet med å fremskaffe verdioversikter er utfordrende, men blir gradvis bedre. Utfordringene er større hos universitetene og høgskolene enn hos øvrige forvaltningsorganer og selskapene.

Trusselbildet

EOS-tjenestene mener at trusselbildet i samfunnet er skjerpet. Spesielt NSM mener det har skjedd et taktskifte med hensyn til digitale trusler siden 2019. Vi har sett noe av det samme i UH-sektoren de siste to-tre årene.

I 2021 rapporterte universitetene og høgskolene om noen flere brudd og hendelser enn i 2020, men antallet alvorlige brudd og hendelser var lavere enn året før. Samtidig hadde tilstedeværelsen av statlige hackergrupper økt: flere institusjoner var utsatt for forsøk på datainntrenging fra slike grupper i 2021 enn tidligere. Det ble ikke rapportert om tilsvarende trusselaktivitet fra de øvrige forvaltningsorganene og selskapene.

Nettkriminell aktivitet utgjorde fortsatt den største kategorien brudd og hendelser. Ulike typer feil og uhell – menneskelige og tekniske – var den nest største kategorien.

Sårbarheter og tiltak

Sårbarhetene som kan føre til brudd og hendelser, er i hovedsak de samme som institusjonene og virksomhetene rapporterte om i 2020 og tidligere år. Kompetanse om informasjonssikkerhet og personvern var derfor den viktigste sårbarheten. Tekniske sårbarheter (sikkerhetshull i programvare) ble oppgitt å være en større utfordring i 2021 enn ved tidligere kartlegginger.

Antallet tiltak for å utbedre sårbarheter var høyere hos universitetene og høgskolene i 2021 enn i 2020. Det ble blant annet rapportert om flere tiltak for å styrke kapasiteten (årsverksinnsatsen) og den tekniske sikkerheten. Det virket likevel å være et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak, spesielt at pedagogiske tiltak (kompetanseheving og bevisstgjøring) ble iverksatt i mindre grad enn hva det syntes å være behov for. Også hos de øvrige forvaltningsorganene og selskapene virket det å være et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak, særlig med hensyn til kompetanse.

Oppsummert – pluss og minus

Gradvis forbedret oversikt over informasjonsverdier og økt tiltaksaktivitet, indikerer at risikoen i sektoren for brudd på informasjonssikkerheten og krenkelser av personvernet er noe redusert: kunnskapen om hva som skal beskyttes er økende og det iverksettes flere forbedringstiltak enn tidligere. Færre alvorlige brudd på informasjonssikkerheten og krenkelser av personvernet sammenliknet med 2020 trekker i samme retning.

Et mer utfordrende trusselbilde og økt statlig trusselaktivitet i sektoren, trekker i motsatt retning – risikoen for brudd og hendelser er noe skjerpet. Den noe manglende korrespondansen mellom rapporterte sårbarheter og iverksatte tiltak antyder at håndteringen av risiko for brudd og hendelser kan forbedres ytterligere. Også det trekker i motsatt retning.

Til sammen mener vi at disse pluss- og minusfaktorene taler for at generell risiko i sektoren ikke har forandret seg vesentlig siden forrige kartlegging. At risikoen for brudd på informasjonssikkerheten og krenkelser av personvernet er på omtrent samme nivå som i 2020, innebærer at den fortsatt er høy. Som tidligere år, kan risikoen være noe lavere for øvrige forvaltningsorganer og selskapene enn for universitetene og høgskolene.

Selv om den generelle risikoen i sektoren ikke er vesentlig endret, kan risikoen for ulike risikoscenarier – konkrete brudd på informasjonssikkerheten og krenkelser av personvernet – likevel ha endret seg. Nedenfor vurderer vi risiko for slike brudd og hendelser.

Rammeverket for vurdering av risiko

Risikoscenarier vurderes langs to dimensjoner: (i) sannsynligheten for at brudd og krenkelser skjer og (ii) mulige skadevirkninger dersom brudd og krenkelser skulle skje.

Vi operasjonaliserer sannsynlighet som forventet hendelsesfrekvens – hvor ofte antar vi at bestemte brudd og krenkelser kan skje. Vurderinger av frekvens skjer med utgangspunkt i trusselbildet og rapporterte brudd og krenkelser i kapittel 2.

Skadevirkninger handler om mulige negative konsekvenser som brudd og krenkelser kan medføre. Skadevirkninger kan ramme ulike aktører og interesser. De kan derfor ha negative konsekvenser for institusjonene og virksomhetenes kjerneoppgaver, ansatte eller studenter og deltakere i forskningsprosjekter. For enkelte typer brudd eller krenkelser kan det være snakk om negative konsekvenser for nasjonale myndigheter og interesser.

Både sannsynlighet og skadevirkninger beror på sårbarhetene i sektoren, tiltakene som er iverksatt og informasjonsverdiene som skal beskyttes. Dette ble drøftet i kapittel 1, 3 og 4.

Nærmere presentasjon av rammeverket for vurdering av risiko, gis i vedlegg 3.

Sannsynlighet og skadevirkninger

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

Vi benytter følgende verdier for skadevirkning (konsekvensverdier):

- **Personvernkrenkelser:** eksempler på dette er at den registrerte ikke får tilgang til egne personopplysninger; opplysninger lagres lengre enn fastsatt; det registreres flere opplysninger enn behandlingsformålet tillater; uautorisert eksponering av personopplysninger; opplysninger mangler eller er feil; personopplysninger er utilgjengelige.
- **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; tap av data/opplysninger; gjenkjøp av IT-utstyr; kompromittering av immaterielle verdier (opphavsrett, patenter); 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.

Vurdering av risikoscenarier

Flere av risikoscenariene nedenfor ble vurdert i fjorårets rapport. Vi angir derfor endringer i risikonivå sammenliknet med fjorårets vurdering.

Scenario 1: skadevare, spesielt løsepengevirus – høy risiko

Skadevarehendelser, særlig større løsepengevirusangrep, ble i fjorårets rapport oppgradert fra middels til høy risiko. Løsepengevirus er skadelig programvare som kan gjøre datamaskiner i et datanettverk ubrukbare. Ofret vil vanligvis bli bedt om å betale en løsepengesum til angriperne, primært nettkriminelle grupper. Dersom utbetaling skjer, lover angriperne at de vil sørge for at datamaskinene – og arbeidsprosessene som er avhengig av dem – igjen skal fungere.

Heller ikke i år rapporterte institusjonene og virksomheter om alvorlige tilfeller med løsepengevirus. Det taler for at sannsynligheten er forholdsvis lav.

Men også i 2021 har vi sett at mange norske virksomheter i ulike bransjer og sektorer har vært utsatt for større løsepengevirusangrep (se kapittel 2). At store løsepengevirus-angrep ikke har rammet institusjoner eller virksomheter i UH-sektoren kan derfor være tilfeldig.[98]

Dette gjør det krevende å vurdere sannsynligheten for at slike brudd i 2022. Usikkerheten, og at løsepengevirus har skapt problemer for virksomheter i UH-sektorens omland, gjør likevel at vi vurderer scenariet som sannsynlig. Det understøttes av at løsepengevirus også i år ble fremhevet som en viktig bekymring blant institusjonene og virksomhetene og av sektorens responsmiljø.

Skadevirkningene som følge av løsepengevirus kan være store og sammensatte.[99] Det kan blant annet dreie seg om omfattende tjenesteavbrudd – kjerneoppgaver blir umulig å utføre for en kortere eller lengre periode. Samtidig kan medieoppslag påvirke omdømme til enkelt-institusjoner eller til sektoren som sådan. Medieoppslag kan også få politiske følgeskader, for eksempel kritikk av departementet.

Videre kan angriperne stjele informasjon fra institusjonenes datamaskiner, typisk personopplysninger, og true med å offentliggjøre dem dersom løsepenger ikke betales. Dette vil i så fall krenke personvernet til de som informasjonen gjelder. Vi antar at dette vil kunne påvirke omdømme og tilliten til enkelt-institusjoner eller til sektoren som sådan.

Løsepengevirus-angrep kan i tillegg føre til store direkte og indirekte økonomiske tap i form av opprydningskostnader og tjenesteavbrudd (oppgaver som ikke utføres[100]). Det kan også dreie seg om andre økonomiske tap, for eksempel knyttet til permanent tap av viktige forskningsdata eller andre typer data. I enkelte tilfeller kan skadene derfor være irreversible.

Skadevirkningene kan bli omfattende for hele sektoren dersom viktige fellestjenester rammes av løsepengevirus.[101]

Risikoen for løsepengevirus kan reduseres ved iverksetting av ulike typer tiltak, for eksempel rask innføring av nye sikkerhetsoppdateringer, bedre kontroll med tjenester som eksponeres mot internett, totrinnsinnlogging, sikring av back-up og økt brukerbevissthet. Det ble rapportert om at slike tiltak hadde blitt gjennomført i sektoren i 2021.

Vi mener likevel at risikonivået når det gjelder skadevare, spesielt løsepengevirus, bør opprettholdes. Dette fordi skadevirkningene kan bli svært omfattende, og forringe evnen til å utføre kjerneoppgaver i lang tid.

Scenario 2: statlig kunnskapsspionasje (APT)

I fjorårets rapport fremhevet vi at risikoen for statlig hacking – etterretning og kunnskapsspionasje – er vanskelig å vurdere, men at visse institusjoner og virksomheter kan være mer utsatt

98 I Storbritannia har for eksempel antallet løsepengevirusangrep mot institusjoner i kunnskapssektoren økt betydelig de siste par årene. Se https://www.jisc.ac.uk/blog/latest-cyber-impact-report-underlines-ransomware-as-a-huge-threat-20-apr-2022. Sist besøkt 27.05.2022.

99 Se for eksempel analyse av løsepengevirusangrepet mot Østre Toten kommune i januar 2021. https://www.ototen.no/aktuelt/ny-versjon-av-sikkerhetsrapporten.13134.aspx. Sist besøkt 25.05.2022.

100 Se for eksempel https://www.theregister.com/2022/03/24/heriot_watt_outage/?&web_view=true. Sist besøkt 25.05.2022.

101 «Et vellykket utpressingsangrep – konsekvensanalyse». Oversendt Kunnskapsdepartementet 31.01.2022 som svar på bestilling i brev 21/2063-28 av 10.12.2021 fra Kunnskapsdepartementet til HK-dir

for dette enn andre. Videre mente vi at variasjoner i risiko blant annet kan bero på faglig profil – hvilke typer forskning som bedrives.[102]

Vår vurdering er at sannsynligheten for at institusjoner og (i mindre grad) virksomheter i UH-sektoren blir utsatt for statlige nettverksoperasjoner er forhøyet sammenliknet med tidligere.[103] Det begrunner vi med at statlige hackergrupper har drevet til dels omfattende kartlegging av universiteter og høgskoler i 2021, og at flere institusjoner enn tidligere rapporterte om bekreftede eller mistenkte forsøk på datainntrenging fra slike grupper.

Det ble også rapportert om rekognosering og forsøk på datainntrenging hos institusjoner hvor dette tidligere ikke hadde vært registrert.

Skadevirkningene ved slike operasjoner er i prinsippet mange av de samme som ved løsepengevirusangrep. Én viktig forskjell er at det her handler om innhenting av informasjon og data, ikke om å blokkere bruken av datamaskiner og hindre tilgangen til viktige data. Selv om de økonomiske kostnadene kan bli store, vil de vanligvis være mindre enn ved omfattende løsepengevirusangrep.

Vi regner heller ikke med at krenkelser av personvernet vil være like store som i enkelte typer løsepengevirusangrep. Dette fordi statlige hackere vanligvis ikke har intensjoner om å offentliggjøre personopplysninger. Likevel kan personvernkrenkelser måtte påregnes, spesielt dersom statlige hackere er ute etter å kartlegge utvalgte enkeltpersoner.

De mest alvorlige skadevirkningene av vellykket kunnskapsspionasje, vil trolig handle om nasjonale interesser og omdømme/tillit. Nasjonale interesser kan for eksempel bli skadelidende dersom statlige hackere får tilgang til kunnskap som er undergitt eksportkontroll. Brudd på slike reguleringer vil være alvorlig i seg selv. Hvilke andre skadevirkninger som ulovlig tilgang til kunnskap med militære anvendelsesområder kan medføre, er vi ikke i stand til å vurdere. Vi regner imidlertid med at skadevirkningene kan være betydelige.

Omdømme og tillit handler også i denne sammenheng om medial oppmerksomhet. Slik oppmerksomhet kan innebære svekket tillit til enkelt-institusjoner, offentlig kritikk av sektoren som sådan eller av departementet.

Scenario 3: kompromitterte brukerkontoer – høy risiko

Kompromitterte brukerkontoer handler om at nettkriminelle grupper eller statlige hackere skaffer seg tilgang til ledere eller ansattes datamaskiner og IT-tjenester. Det kan for eksempel skje ved hjelp av nettfiske eller automatisk passordgjetting («brute force»). Deretter kan angriperne misbruke datamaskinen eller IT-tjenestene til sine formål, eventuelt å skaffe seg tilgang til andre og mer interessante datamaskiner i det samme datanettverket, for eksempel maskiner som inneholder verdifulle data.

Risikoen for slike brudd på informasjonssikkerheten ble i fjorårets rapport vurdert som høy. Innføring av totrinnsinnlogging hos flertallet av institusjonene og virksomhetene har ført til en nedgang i antallet kompromitterte brukerkontoer i 2021. Vi mener derfor at sannsynligheten er redusert sammenliknet med 2020. Etter hvert som stadig flere institusjoner og virksomheter ferdigstiller innføringen av totrinnsinnlogging, regner vi med at sannsynligheten reduseres ytterligere.

Det ble likevel rapportert om over 200 kompromitterte brukerkontoer i 2021. Vår vurdering er derfor at sannsynligheten for slike sikkerhetsbrudd fortsatt (og inntil videre) er relativt høy.

Skadevirkningene av kompromitterte brukerkontoer vil avhenge av hva kontoene brukes til. Dersom de brukes til utsendelse av søppel-epost, som er det vanlige, er der ikke snakk om alvorlige skadevirkninger. Men risikoscenariene drøftet ovenfor – løsepengevirus og statlig kunnskapsspionasje – starter ofte med at brukerkontoer kompromitteres. Skadevirkningene kan derfor bli de samme som skissert i risikoscenario 1 og 2: tjenesteavbrudd, personvernkrenkelser, økonomisk tap, tap av omdømme/tillit eller skader på nasjonale interesser.

Vår vurdering er derfor at risikoen knyttet til kompromitterte kontoer fortsatt er høy selv om sannsynligheten er noe redusert. Kompromitterte brukerkontoer var også blant de hendelsene som institusjonene og virksomhetene i sektoren var mest bekymret for.

102 I kapittel 2 har vi sett at det kan gjelde forskningsmiljøer innen en lang rekke fagområder: kjernefysikk, fysikk, kjemi, biologi, medisin, undervanns- og dypvannsteknologi, kontrollsystemer, styringssystemer, autonome fartøy, mønstergjenkjenning (maskinlæring), ingeniørdesign, nanoteknologi, satellitt- og missilteknologi og teknologi tilpasset arktiske forhold.

103 Internasjonale undersøkelser antyder at mange virksomheter og organisasjoner har eller mistenker at de har vært utsatt for statlig eller statsstøttet datainntrenging. Se for eksempel https://www.infosecurity-magazine.com/news/organizations-faced-nationstate/?&web_view=true. Sist besøkt 25.05.2022.

Scenario 4: utilsiktede feil og uhell – middels risiko

Risikoen for utilsiktede brudd eller krenkelser – menneskelige eller tekniske feil og uhell som ikke er fremprovosert av trusselaktører – ble i fjorårets rapport vurdert som middels. Også i 2021 ble det opplyst om forholdsvis mange slike brudd og hendelser. Disse utgjorde i tillegg en høy andel av de bruddene på personopplysningssikkerheten som ble meldt til Datatilsynet. Sannsynligheten for brudd og krenkelser som følge av menneskelige eller tekniske feil og uhell er derfor, slik vi vurderer det, på omtrent samme nivå som i 2020.

Skadevirkningene handlet om tapt arbeidstid på grunn av kortere avbrudd i tjenesteleveranser fra eksterne leverandører og krenkelser av personvernet. Her dreide det seg i hovedsak om at ansatte fikk tilgang til personopplysninger som de ikke hadde tjenstlige behov for å kjenne til, for eksempel som følge av at opplysninger ble feilsendt på epost. I enkelte tilfeller handlet det også om at allmennheten kunne hatt tilgang til opplysninger på grunn av feil publisering på internett.

Det var likevel snakk om feil og uhell som rammet få personer og som bare i noen tilfeller gjaldt særlige kategorier personopplysninger. Skadevirkningene var derfor nokså identiske med de som ble rapportert i 2020.

Ettersom sannsynligheten for og skadevirkningene er omtrent de samme som ved forrige kartlegging, mener vi at risikoen for menneskelige eller tekniske feil og uhell fortsatt er middels.

Scenario 5: direktør- og fakturasvindel – lav risiko

Risikoen for nettsvindel, spesielt faktura- og direktørsvindel, ble vurdert som middels i fjorårets rapport. I år mener vi at sannsynligheten for utbetaling av større beløp som følge av direktør- eller fakturasvindel, er redusert. Det skyldes at det ble rapportert om færre forsøk på slik nettsvindel enn tidligere, og at det ble rapportert om økt bevissthet om direktør- og fakturasvindel, særlig blant økonomimedarbeidere.

I tillegg ble det oppgitt at svært få svindelforsøk hadde lyktes. Der hvor utbetaling hadde skjedd, handlet det om kjøp av gavekort som ble betalt av egen lomme.

Tidligere har det vært hendelser i sektoren som har medført urettmessig utbetaling av millionbeløp. I slike tilfeller kan medieoppslag skade omdømmet til den aktuelle institusjonen eller virksomheten.

Vi mener likevel at risikoen for direktør- eller fakturasvindel er noe mindre enn tidligere. Vi nedgraderer derfor risikoen fra middels til lav.

Det er imidlertid fortsatt behov for årvåkenhet i sektoren når det gjelder nettsvindel.

Scenario 6: tjenestenekt (DDoS) – lav risiko

I fjorårets rapport ble risikoen for større tjenestenektangrep i UH-sektoren vurdert som lav. Heller ikke i 2020 ble det rapportert om større tjenestenektangrep. Sektorens responsmiljø hos Sikt opplyste om at antallet slike angrep har vist en nedadgående trend i flere år. Sannsynligheten for tjenestenekt fremstår derfor som lav. Sannsynligheten kan være noe større for at datamaskiner i UH-sektoren misbrukes til å gjennomføre tjenestenektangrep mot virksomheter i andre sektorer.

Skadevirkningene av tjenestenektangrep kan variere noe, for eksempel at hjemmesiden er midlertidig nede eller at eksamen må utsettes fordi den digitale eksamensløsningen er utilgjengelig. Vi er ikke kjent med at tjenestenektangrep har ført til alvorlige skadevirkninger i UH-sektoren.

Vi mener derfor at risikoen for denne typen sikkerhetsbrudd fortsatt er lav.

Risikomatrisen

De seks scenariene vurdert ovenfor, oppsummeres i risikomaterien nedenfor.
Scenariene benevnes S1 – S6:

- S1 = skadevare, spesielt løsepengevirus.
- S2 = statlig hacking (kunnskapsspionasje).
- S3 = kompromitterte brukerkontoer.
- S4 = utilsiktede feil og uhell.
- S5 = direktør- og fakturasvindel.
- S6 = tjenestenekt (DDoS).

Skadevirkning					
	Meget alvorlig			S1, S2, S3	
	Alvorlig				
	Mindre alvorlig		S6		S4
	Lite alvorlig			S5	
		Svært lite sannsynlig	Lite sannsynlig	Sannsynlig	Svært sannsynlig
		Sannsynlighet			

Muligheter for måloppnåelse

Risiko for brudd på informasjonssikkerheten og krenkelser av personvernet påvirker sektorens evne til å oppnå målene i strategien for digital omstilling. Her omtales informasjonssikkerhet og personvern som én av seks forutsetninger for arbeidet med digital omstilling.[104] Det sies blant annet at forvaltning av data i sektoren stiller store krav til forsvarlig behandling av personopplysninger og til informasjonssikkerheten.[105] Hovedmålene om informasjonssikkerhet og personvern er følgelig at:

«Institusjonenes arbeid med informasjonssikkerhet og personvern skal sikre at alle aktiviteter innenfor utdanning, forskning, formidling og administrasjon gjennomføres på en sikker og tillitsvekkende måte. Viktige informasjonsverdier og personopplysninger skal beskyttes. Både vitenskapelig og administrativt ansatte må ha god kunnskap om informasjonssikkerhet og personvern, slik at de er i stand til å skape, bruke, lagre og dele data på en sikker måte.»[106]

Vi kan ikke se at målene i strategien innebærer strengere eller andre krav til informasjonssikkerhet og personvern enn hva som følger av departementets policy for informasjonssikkerhet og personvern. Slik vi ser det, operasjonaliserer policyen hovedmålene i strategien. Det betyr at graden av policyetterlevelse er en god indikator på mulighetene for måloppnåelse.

Etterlevelse og måloppnåelse

Vi forventer at hovedmålene i strategien vil kunne nås hos 13 av de 21 universitetene og høgskolene. Dette gjelder de to universitetene som i dag etterlever kravene i policyen. Det gjelder også de 11 institusjonene hvor tilfredsstillende etterlevelse vurderes som sannsynlig eller mulig i 2022 (se kapittel 3).

Vi er mer usikre på om hovedmålene kan nås for de åtte universitetene og høgskolene hvor etterlevelse vurderes som lite sannsynlig i 2022 (se igjen kapittel 3). Vi regner det likevel som realistisk at flertallet av dem vil kunne etterleve policyen og oppfylle hovedmålene ved strategiperiodens utløp (2025).

Når det gjelder de sju øvrige forvaltningsorganene og selskapene, forventer vi at samtlige vil etterleve policyen og oppnå hovedmålet i strategien før 2025. Disse virksomhetene har jevnt over kommet noe lengre med arbeidet enn universitetene og høgskolene (se kapittel 4). Det skyldes i stor grad at de er mindre organisasjoner enn flertallet av universitetene og høgskolene. De har derfor en enklere jobb med å ivareta policykrav og sikre måloppnåelse.

Oppnå og opprettholde

Vellykket måloppnåelse forutsetter at institusjonene og virksomhetene er i stand til å opprettholde tilfredsstillende policyetterlevelse over tid. Etterlevelse og måloppnåelse er derfor en tilstand og ikke et øyeblikksbilde ved slutten av en strategiperiode. Følgelig er det viktig at sektoren evner å videreføre en ønsket tilstand etter at den først er oppnådd.

Vi har i dag ikke grunnlag for å vurdere sektorens opprettholdelsesevne. Dette vil være en prioritert oppgave etter hvert som stadig flere institusjoner og virksomheter forbedrer kvaliteten på arbeidet.

---

104 «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 25.05.2022.

105 Ibid., side 22.

106 Ibid., side 32.

Forslag til oppfølging på sektornivå

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. Vi anbefaler derfor følgende sektortiltak:

Anbefaling 1 – risikoreduksjon

I risikoscenariene S1 – S3 vurderes risikoen for brudd på informasjonssikkerheten og krenkelser av personvernet som høyere enn hva departementet tidligere har akseptert. Risikoen for løsepengevirus og statlig kunnskapsspionasje vurderes som høy. Det samme gjelder risikoen knyttet til kompromittering av brukerkontoer.

Vi mener at anbefalingene 2 – 6 nedenfor bør innrettes slik at risikoen for scenariene S1 – S3 reduseres. Scenariene og hvordan risikoen for dem kan reduseres bør blant annet være sentrale tema i kompetansehevende aktiviteter i sektoren, og i rådgivings- og veiledningsarbeidet til Sikt (Cybersikkerhetssenteret).

Anbefaling 2 – verdioversikter

Universitetene og høgskolene mangler tilfredsstillende oversikter over enkelte av sine informasjonsverdier som skal beskyttes mot brudd på sikkerheten og krenkelser av personvernet.

Det anbefales derfor at universitetene og høgskolene tilbys rådgiving og veiledning om

- hvordan kartlegging av verdier best kan gjennomføres, inkludert hvilke arbeidsverktøy som kan benyttes,
- hvordan oversikter over informasjonsverdier bør være, spesielt innholdselementer og detaljeringsgrad.

Anbefaling 3 – oppdagelse og hendelseshåndtering

Flere brudd på informasjonssikkerheten og krenkelser av personvernet de siste to årene, indikerer at universitetene og høgskolene har behov for ytterligere å styrke evne til å oppdage og håndtere brudd og hendelser.

Vi anbefaler derfor følgende tiltak:

- videreutvikling av sektorens deteksjons- og responskapasitet,
- gjennomføring av sårbarhets- og inntrengingstesting i sektoren,
- veiledning til sektoren om håndtering av IKT-sikkerhetshendelser,
- kurs for operativt sikkerhetspersonell i sektoren (IRT),
- bistand for å styrke til beredskaps- og kontinuitetsarbeidet i sektoren,
- tilbud om bruk av VDI for de institusjoner og virksomheter som ønsker dette.

Anbefaling 4 – opplæring og kompetanseheving

Både institusjonene og virksomhetene opplyste om at manglende kompetanse innen informasjonssikkerhet og personvern er deres viktigste utfordring (sårbarhet). Slik kompetanse kan være vanskelig å skaffe gjennom rekruttering og nyansettelser. Kompetansen må derfor i stor grad bygges opp internt i sektoren.

Vi anbefaler derfor følgende tiltak:

- videreutvikle møteplassene i sektoren for informasjonsutveksling og erfaringsdeling (CISO- og personvernombudsforum),
- tilby rådgiving og veiledning tilpasset den enkelte institusjon eller virksomhet,
- gjennomføre revisjoner av arbeidet med informasjonssikkerhet og personvern hos den enkelte institusjon eller virksomhet,
- styrke veiledning om innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet,
- tilby kurs for ledere i informasjonssikkerhet og personvern.

Anbefaling 5 – sektortjenestene
Virksomheter som anskaffer eller forvalter sektortjenester, enten i rollen som databehandler eller ved å inngå rammeavtaler med andre leverandører, har et særlig ansvar for at krav til informasjonssikkerhet og personvern ivaretas.

Vi anbefaler at departementet stiller tydelige forventninger til at hensynet til informasjonssikkerhet og personvern ivaretas ved utvikling av sektortjenester og inngåelse av avtaler med leverandører. Det inkluderer rettslige avklaringer knyttet til eventuelle overføringer av personopplysninger til land utenfor EU/EØS.

Anbefaling 6 – samarbeid med NSM
HK-dir har behov for informasjon om trusselaktivitet for å kunne vurdere trusselnivået i UH-sektoren og risiko for brudd på informasjonssikkerheten og krenkelser av personvernet.
I samarbeid med departementet, planlegges et samarbeid med Nasjonal sikkerhetsmyndighet (NSM) med tanke på utveksling av trusselinformasjon.

Vi anbefaler at samarbeid og informasjonsutveksling mellom departementet, HK-dir og Nasjonal sikkerhetsmyndighet etableres slik som planlagt. Samarbeidet bør videreutvikles og utdypes over tid.

Anbefaling 7 – øvrige virksomheter
De øvrige forvaltningsorganene og selskapene har kommet noe lengre i arbeidet med informasjonssikkerhet og personvern enn universitetene og høgskolene. Samtidig har disse virksomhetene mange av de samme utfordringene (sårbarhetene) som universitetene og høgskolene. Det gjelder særlig behovet for kompetanse og opplæring.

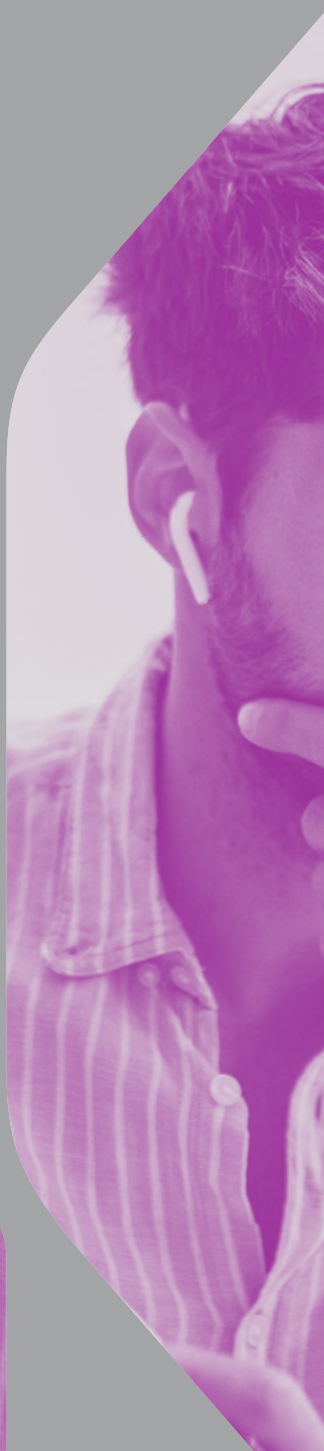
Vår anbefaling er derfor at det ikke iverksettes egne sektortiltak for øvrige forvaltningsorganer og selskaper. Anbefalingene som gjelder for universitetene og høgskolene vil også møte behovene til disse virksomhetene.

Oppfølging av den enkelte virksomhet

Den enkelte institusjon og virksomhet har også i år mottatt anbefalinger om hva vi mener de bør prioritere i 2022.

Departementet følger opp anbefalingene fra HK-dir i styringsdialogen med den enkelte institusjon og virksomhet.

Vedlegg



VEDLEGG

Vedlegg 1:

Datagrunnlaget og arbeidet med rapporten

Denne 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 de til sammen 28 institusjonene og virksomhetene ble gjennomført i perioden 8. november 2021 til 16. februar 2022.

Forberedelse og kontakt

Virksomhetene mottok først et brev fra HK-dir om kartlegging. Brevene til de 12 første institusjonene og virksomhetene ble sendt ut i oktober 2021. Brevene til de siste 16 institusjonene og virksomhetene ble sendt ut i november 2021.

I brevene ble det opplyst om at HK-dir ville gjennomføre møter med den enkelte institusjon eller virksomhet for å kartlegge statusen i arbeidet med informasjonssikkerhet og personvern (GDPR).

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

Deltakelse og deltakere

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

HK-dir stilte vanligvis med tre deltakere, men på enkelte møter med to.

Gjennomføring og datainnsamling

Det var satt av 1,5-2 timer til besvarelse av spørsmålene i kartleggingsskjemaet.

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

Med unntak av hos én virksomhet, ble kartleggingsmøtene avholdt som videokonferanser. Hos den siste ble det gjennomført fysisk møte.

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

Hos de øvrige institusjonene og virksomhetene ble svarene på spørsmålene i kartleggingsskjemaet 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 institusjonene og virksomhetenes svar på spørsmålene i skjemaet. Referatene ble sendt tilbake til den enkelte institusjon og virksomhet for kommentarer og kvalitetssikring. Vi mottok tilbakemeldinger – korreksjoner og utfyllende kommentarer – fra 21 av institusjonene og virksomhetene.

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

De 12 institusjonene og virksomhetene som det ble gjennomført kartleggingsmøter med i november og desember 2021, mottak anbefalingsbrev fra HK-dir tidlig i januar 2022. De øvrige 16 institusjonene og virksomhetene mottok sine brev i mars og april 2022.

Andre datakilder

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

- statistikk om IT-sikkerhetshendelser i forskningsnettet fra sektorens responsmiljø hos Sikt (tidligere Uninett CERT),
- årsrapportene til institusjonene og virksomhetene for 2020,
- 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 institusjonene og virksomhetenes hjemmesider,
- risiko- eller trusselvurderinger fra internasjonale aktører,
- forskningslitteratur innen informasjonssikkerhet og personvern.

I tillegg inngår annen informasjon i datagrunnlaget. Det gjelder informasjon om trusler, sårbarheter og tiltak innhentet i møter mellom HK-dir og (i) sektorens responsmiljø hos Sikt og (ii) rådgivingstjenesten i Cybersikkerhetssenteret. Disse møtene gjennomføres hvert kvartal og ved behov.

Metodiske begrensninger

Den primære datakilden var svarene som institusjonene og 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 institusjonene og virksomhetene rapporterte om at de hadde iverksatt, 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.

Nærmere kvalitetssikring av arbeidet med informasjonssikkerhet må skje gjennom sikkerhetstester og revisjoner.

VEDLEGG

Vedlegg 2:

Kartleggingsskjemaet som ble benyttet

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

2. Hvilke brudd på informasjonssikkerheten, inkludert personopplysningssikkerheten, og avvik fra egne sikkerhetsrutiner har virksomheten registrert i 2021?
   - 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.

3. Hvilke andre typer personvernhendelser og rutineavvik enn brudd på personopplysningssikkerheten og avvik fra sikkerhetsrutiner har virksomheten registrert i 2021?
   - 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.

4. Hva er de viktigste årsakene til at brudd på informasjonssikkerheten eller uønskede personvernhendelser oppsto i 2021 (eventuelt årsaker til at uønskede hendelser kan skje i fremtiden)?
   - Noen eksempler på årsaker til brudd og hendelser: uhell, teknisk svikt, mangelfull brukerkompetanse/bevissthet, begrensede ressurser (tid, personell, økonomi), uklar ansvars- eller oppgavefordeling, vanskelig regelverk, feil hos leverandør eller manglende sikkerhetsoppdatering.

5. Hvilke initiativ/tiltak ble gjennomført i 2021 for å styrke/videreutvikle arbeidet med informasjonssikkerhet og ledelsessystemet for informasjonssikkerhet?
   - Eventuelle endringer i status for arbeidet med informasjonssikkerhet og ledelsessystemet siden forrige kartlegging.
   - Områder (forskning, utdanning, administrasjon og formidling) hvor virksomheten mener at arbeidet med informasjonssikkerhet og ledelsessystemet bør styrkes.

6. Hvilke initiativ/tiltak ble gjennomført i 2021 for å styrke/videreutvikle arbeidet med personvern og etterlevelsen av personopplysningsloven/GDPR?
   - Eventuelle endringer i status for innføring/drift av internkontrollen for personopplysningsloven/GDPR siden forrige kartlegging.
   - Områder (forskning, utdanning, administrasjon og formidling) hvor virksomheten mener at arbeidet med personvern og internkontrollen for personopplysningsloven/GDPR bør styrkes.

7. I hvilken grad ble det gjennomført risikovurderinger av informasjonssikkerheten i 2021? Ble vurderingene fulgt opp med nødvendige sikringstiltak?

8. Hvilke initiativ/tiltak ble gjennomført i 2021 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.

9. I hvilken grad har virksomheten en plan for håndtering av alvorlige informasjonssikkerhets- og personvernhendelser (kontinuitet og beredskap)? Ble det øvd på håndtering av slike hendelser i 2021?

10. Hvilke hovedtema/-problemstillinger ble diskutert på ledelsens gjennomgang i 2021?
    - Viktige initiativ/tiltak på informasjonssikkerhets- og personvernområdet som planlegges gjennomført i 2022.

Årets fokusområde – Schrems II-dommen:
EU-domstolens dom i Schrems II-saken innebærer at det blir mer utfordrende å ta i bruk databehandlingstjenester hvor personopplysninger overføres til enkelte land utenfor EØS-området (tredjeland). Vi har noen spørsmål om virkningene av dommen.

1. Hvilke konsekvenser (om noen) har Schrems II-dommen fått for digitaliseringsarbeidet hos dere?
   - Eksempler på konsekvenser kan være at anskaffelser av nye databehandlingstjenester er avlyst eller satt på vent, eventuelt at bruken av visse tjenester er avsluttet.

2. Hvilke tiltak har dere iverksatt for å håndtere kravene som dommen innebærer med hensyn til overføring av personopplysninger til tredjeland?
   - Eksempler på tiltak kan være kartlegginger av databehandlingstjenester som overfører personopplysninger til tredjeland eller endring i rutiner for anskaffelse av databehandlingstjenester.

3. Hva (om noe) kan gjøres på sektornivå for å bistå virksomhetene med håndteringen av de nye kravene til overføring av personopplysninger?

VEDLEGG

Vedlegg 3:

Rammeverket som ble benyttet ved vurdering av risiko

Sannsynlighetsverdier (hendelsesfrekvens)

Svært sannsynlig:	Det forventes at hendelsen kan skje mange ganger i året.
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 tilgangen til egne personopplysninger; enkelte opplysninger lagres litt lengre enn hva som er fastsatt; det registreres noen flere trivielle opplysninger enn hva behandlingsformålet strengt tatt krever.
- **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 på grunn av uønskede hendelser eller 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 aktører som følge av direktør- eller fakturasvindel.
- **Tap av omdømme og tillit:** misnøye blant viktige interne brukergrupper på grunn av uønskede hendelser eller 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 aktører som følge av direktør- eller 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 virksomheten; offentlig kritikk av virksomheten (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, for eksempel ulovlig kunnskapsoverføring, eller som innebærer brudd på internasjonale forpliktelser.

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 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, for eksempel ulovlig kunnskapsoverføring, eller større brudd på internasjonale forpliktelser.

VEDLEGG

Risikonivåer og oppfølging

Høy risiko:

Hendelser som medfører uakseptabel risiko:

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

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

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 sektortiltak, eventuelt om sektortiltakene bør revideres for å styrke den risikoreduserende effekten.

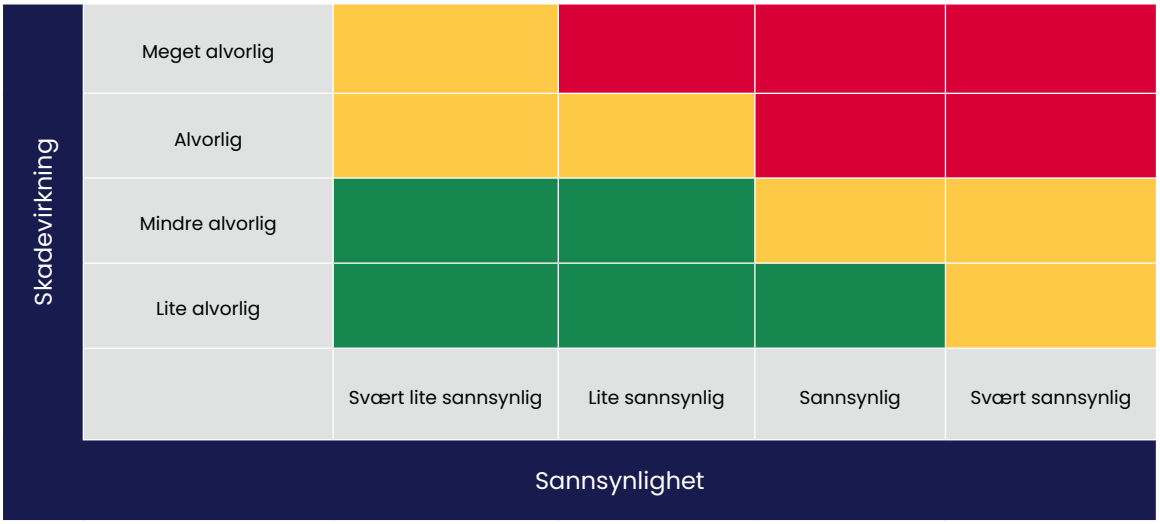
Lav risiko:

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; 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. Det betyr for eksempel at dersom en hendelse innebærer meget alvorlige personvernkrenkelser samtidig som tjenesteavbrudd og økonomisk tap vurderes som mindre eller lite alvorlig, vil konsekvensverdien for hendelsen bli meget alvorlig. Dersom også tjenesteavbrudd og økonomisk tap vurderes som meget alvorlig, vil konsekvensverdien være den samme (meget alvorlig). Hendelsen vil likevel innebære flere typer meget alvorlige konsekvenser. I slike tilfeller kan det være særlig aktuelt med risikoreduserende tiltak.

VEDLEGG

Vedlegg 4:

Institusjoner og virksomheter som omfattes av Kunnskaps-departementets styringsmodell

Statlige universiteter og høgskoler

- Arkitektur- og designhøgskolen i Oslo.
- Høgskolen i Innlandet.
- Høgskolen i Molde - Vitenskapelig høgskole i logistikk.
- Høgskulen i Volda.
- Høgskolen i Østfold.
- Høgskulen på Vestlandet.
- Kunsthøgskolen i Oslo.
- Nord universitet.
- Norges Handelshøyskole.
- Norges idrettshøgskole.
- Norges miljø- og biovitenskapelige universitet.
- Norges musikkhøgskole.
- Norges teknisk-naturvitenskapelige universitet.
- OsloMet – storbyuniversitetet.
- Samisk høgskole.
- Universitetet i Agder.
- Universitetet i Bergen.
- Universitetet i Oslo.
- Universitetet i Stavanger.
- Universitetet i Sørøst-Norge.
- Universitetet i Tromsø - Norges arktiske universitet.

Øvrige forvaltningsorganer og selskaper

- De nasjonale forskningsetiske komiteene.
- Nasjonalt organ for kvalitet i utdanningen.
- Norges forskningsråd.
- Norsk utenrikspolitisk institutt.
- Sikt – kunnskapssektorens tjenesteleverandør.
- Simula Research Laboratory.
- Universitetssenteret på Svalbard.
- Direktoratet for høyere utdanning og kompetanse (styringsansvaret ligger hos Kunnskapsdepartementet).