Tilstandsvurdering av informasjonssikkerhet og personvern blant de statlig eide universitetene og høgskolene

Rapport 2019

Innholdsfortegnelse

Sammendrag

I denne rapporten drøftes to hovedspørsmål: (1) Hva er tilstanden på informasjonssikkerhets- og personvernområdet hos statlig eide universiteter og høgskoler? (2) Hva sier tilstanden om oppnåelse av sektormålene for arbeidet med informasjonssikkerhet og personvern, slik de fremgår av *Digitaliseringsstrategi for universitets- og høyskolesektoren, 2017-2021*?

Datagrunnlaget for rapporten er de enkelte institusjonenes svar på 24 spørsmål vedrørende deres arbeid med informasjonssikkerhet og personvern. Spørsmålene ble besvart i kartleggingsmøter mellom den enkelte institusjon og Unit. Institusjonene mottok spørsmålene i forkant av kartleggingsmøtene. Fra institusjonene deltok ledere og medarbeidere med sentrale roller i det lokale informasjonssikkerhets- og personvernarbeidet, for eksempel informasjonssikkerhetsledere/-rådgivere, IT-ledere, andre ledere i sentraladministrasjonen og personvernombud. I etterkant av møtene utarbeidet Unit et kartleggingsreferat med sammendrag av institusjonenes svar på de enkelte spørsmålene. Referatene ble sendt til institusjonene for skriftlige kommentarer. Unit mottok slike kommentarer fra 16 institusjoner.

Vurderingene, konklusjonene og anbefalingene i denne rapporten bygger primært på informasjon innhentet av Unit i løpet av informasjons- og kartleggingsmøtene. Det innebærer at det ikke er bedt om tilgang til eller gjennomført gjennomganger av interne dokumenter som beskriver arbeidet med informasjonssikkerhet og personvern. Det er heller ikke gjennomført kontroller av hvilke tekniske, organisatoriske eller fysiske sikringstiltak som er iverksatt eller om tiltakene har hatt den tiltenkte effekten. Hensikten med undersøkelsen har isteden vært å kartlegge omfanget av og systematikken i institusjonenes arbeid med informasjonssikkerhet og personvern, det vil si i hvilken grad helhetlig risikostyring og internkontrollmetodikk strukturerer det daglige, praktiske arbeidet med informasjonssikkerhet og personvern i alle deler av virksomheten (forskning, undervisning, administrasjon og formidling).

Hovedkonklusjonene i rapporten er at det i sektoren er en relativt høy risiko for mangelfull måloppnåelse, slik målene for informasjonssikkerhet og personvern er definert i digitaliseringsstrategien for UH-sektoren. Dette gjelder følgende sektormål: (1) institusjonene skal etablere helhetlig styring og ledelse av arbeidet med informasjonssikkerhet og personvern, (2) institusjonenes arbeid med styrking av informasjonssikkerheten og personvernet skal være systematisk, (3) nivået på arbeidet med informasjonssikkerhet og personvern skal ligge høyere enn de nasjonale minstekravene (blant annet rettslige krav) og (4) studenter og ansatte skal bevisstgjøres problemstillinger knyttet til informasjonssikkerhet og personvern. Units samlede vurdering er at risikoen for mangelfull måloppnåelse er størst når det gjelder sektormål 1-3, men noe mindre når det gjelder sektormål 4.

Grunnlaget for disse konklusjonene er kombinasjonen av følgende forhold:

- Sektoren forvalter store, sammensatte og uoversiktlige informasjonsverdier, inkludert personopplysninger. Mange av verdiene er av sensitiv og til dels svært sensitiv karakter.
- Forskning og høyere utdanning virker ikke å være mindre utsatt for sikkerhetshendelser og avvik enn samfunnet for øvrig.
- Sektoren har gjennomført en rekke initiativ og tiltak på informasjonssikkerhets- og personvernområdet, men arbeidet preges likevel av viktige sårbarheter/utfordringer.

Med bakgrunn i hovedkonklusjoner anbefales det at følgende tiltak iverksettes på institusjonsnivå:

- Institusjonene med støtte fra den øverste ledelse prioriterer arbeidet med informasjonssikkerhet og personvern høyere enn i dag. Dette innebærer styrket personalinnsats, bedre samordning av ressursinnsatsen og økt fokus på kompetanseheving innenfor alle virksomhetsområder.
- Institusjonene iverksetter tiltak for innføring og praktisering av vedtatte ledelsessystemer for informasjonssikkerhet (internkontroll).
- Institusjonene skaffer seg bedre oversikter over sine informasjonsverdier, inkludert digitale systemer og tjenester.
- Institusjonene planlegger for hvordan normal drift skal gjenopprettes i etterkant av alvorlige sikkerhetshendelser (kontinuitetsplanlegging).

På nasjonalt nivå anbefales følgende tiltak:

- Det utarbeides tydelige og målbare sektormål for informasjonssikkerhet og personvern som innarbeides i en revidert versjon av Units handlingsplan for digitalisering av høyere utdanning og forskning.
- Det etableres en konsulent- og rådgivingstjeneste for informasjonssikkerhet og personvern som kan bistå sektoren.
- Det legges vekt på at krav til informasjonssikkerhet og personvern ivaretas ved utvikling eller anskaffelser av fellestjenester i sektoren.
- Det fokuseres på informasjonssikkerhet og personvern i forskning og undervisning. Dette inkluderer studentforskning og forskningsområder hvor det ikke behandles personopplysninger.

Det anbefales ikke at det iverksettes nasjonale initiativ for sertifisering av digitale løsninger eller prosesser med hensyn til informasjonssikkerhet og personvern.

Det anbefales heller ikke at det iverksettes et nasjonalt arbeid med utforming av atferdsnormer for behandling av personopplysninger (slik EUs personvernforordning åpner for og som er utarbeidet i helse- og omsorgssektoren).

Innledning

Statlige universiteter og høgskoler forvalter viktige informasjonsverdier og personopplysninger på vegne av samfunnet og den enkelte. For å ivareta informasjonssikkerheten til disse verdiene og personvernet til de som opplysningene gjelder, er det en forutsetning at institusjonene har oversikt over sine informasjonsverdier og personopplysninger. Institusjonene må også kjenne til hvilke trusler informasjonsverdier og personopplysninger utsettes for og hvordan verdiene og opplysningene er sårbare for disse truslene.

Denne rapporten gir et første innblikk i disse problemstillingene på sektornivå, og inngår som en del av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.[1] Rapporten legger et første grunnlag for departementets helhetlige risikostyring av informasjonssikkerhet og personvern på sektornivået. Den kan også være en av flere informasjonskilder som institusjonene i sektoren benytter i sitt eget arbeid med informasjonssikkerhet og personvern.

[1] Styringsmodellen ble presentert for Kunnskapsdepartementets underliggende virksomheter i brev fra statsråden av 7. januar 2019.

Høye ambisjoner

Kunnskapsdepartementet har høye ambisjoner om at digitaliseringen skal bidra til at informasjonsverdiene utnyttes på best mulig måte på alle nivåer i sektoren. For å kunne realisere ambisjonene, slik de blant annet er formulert i digitaliseringsstrategien for universitets- og høyskolesektoren, er det nødvendig å dimensjonere arbeidet med informasjonssikkerhet og personvern riktig. Det kommer til uttrykk i digitaliseringsstrategien gjennom ambisjonen om en målrettet styrking av informasjonssikkerheten*:*

> *«Universitetene og høyskolene er kunnskapsvirksomheter hvor forvaltning og foredling av informasjon/data er en del av kjernevirksomheten. Å videreutvikle denne kjernevirksomheten gjennom en strategisk satsing på digitalisering innebærer også at institusjonene må ha et aktivt forhold til styringen av informasjonssikkerheten, og ha en egen strategisk interesse i å løfte denne høyere enn de nasjonale minstekravene.»*[2]

Formålet med denne rapporten er derfor tredelt. For det første å gi et grunnlag for å vurdere de statlige universitetenes og høgskolenes evne til å håndtere risikoen for brudd på informasjonssikkerheten og til å etterleve personvernregelverket (personopplysningsloven og GDPR).[3] For det andre å vurdere risikoen i sektoren for manglende realisering av målene i digitaliseringsstrategien om styrking av informasjonssikkerheten og personvernet. For det tredje å gi anbefalinger om eventuelle sektortiltak som bør iverksettes for å styrke arbeidet med informasjonssikkerhet og personvern.

[2] Digitaliseringsstrategi for universitets- og høgskolesektoren, 2017-2021, side 22.

[3] Tilstanden hos Kunnskapsdepartementets øvrige underliggende virksomheter – direktorater, selskaper og forskningsvirksomheter – vil bli kartlagt i løpet av våren 2019.

Informasjonsverdier, trusler og sårbarheter

Drøftelsene og vurderingene i rapporten tar utgangspunkt i de viktigste prinsipper som ligger til grunn for tradisjonell risikovurderingsmetodikk.[4] Det betyr at rapporten er organisert med bakgrunn i tre hovedelementer – informasjonsverdier, trusler og sårbarheter.

Mer konkret innebærer dette at fokuset i rapporten rettes mot følgende forhold:

Informasjonsverdier: Det som sektoren skal beskytte. Når det gjelder personvern vil dette være personopplysninger og tekniske løsninger (systemer, tjenester, datanettverk, osv.) hvor slike opplysninger behandles. Når det gjelder informasjonssikkerhet vil det også omfatte andre typer opplysninger, data og tekniske løsninger. Her kan det for eksempel dreie seg om viktige forskningsdata som ikke er personopplysninger og elektronisk forskningsinfrastruktur for lagring, deling eller analyse av slike data.

Trusler: Det eller de som kan utsette informasjonsverdiene i sektoren for sikkerhetshendelser eller personvernkrenkelser. Dette kan være trussel-aktører (enkeltpersoner, kriminelle grupper, nasjonalstater, osv.) som opererer på internett, og som har ulike motiver for å kompromittere informasjonsverdiene i sektoren. Det kan også være studenter, medarbeidere eller tjenesteleverandører som mangler kompetanse til å håndtere viktige informasjonsverdier på en sikker, forsvarlig eller lovlig måte.

Sårbarheter: Sektorens manglende evne til å beskytte sine informasjonsverdier mot sikkerhetshendelser eller personvern-krenkelser. Dette kan inkludere evnen til å gi studenter eller medarbeidere tilstrekkelig kompetanse i forsvarlig og lovlig håndtering av personopplysninger. Det kan også omfatte andre typer ressursprioritering, for eksempel personalressurser som er avsatt til arbeidet med informasjonssikkerhet og personvern, eller om det er iverksatt et systematisk arbeid for å forebygge, oppdage og håndtere hendelser eller avvik. I tillegg kan det omfatte en rekke andre forhold, blant annet tekniske sårbarheter i programvare eller IT-utstyr.

Rapporten gir en overordnet gjennomgang av disse momentene på sektornivå. Den gir derfor et grunnlag for å vurdere risikoforhold knyttet til informasjonssikkerhet og personvern i forskning og høyere utdanning.

[4] Se for eksempel Nasjonal sikkerhetsmyndighet (2016): Risikovurdering for sikring. Tilgjengelig på https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf. Se også Håkon Bergsjø og Ronny Windvik (2018): Datasikkerhet for ledere. Hvordan beskytte din virksomhet. Oslo: Universitetsforlaget.

Risikovurdering

Risikoen for hendelser og for mangelfull måloppnåelse er produktet av informasjonsverdier, trusler og sårbarheter. Det betyr at risikoen for at sektormålene og nasjonale føringer ikke oppnås kan sies å være relativt stor dersom:

- Forskning og høyere utdanning forvalter store og viktige informasjonsverdier.
- Evne til å ivareta informasjonsverdiene er mangelfull fordi arbeidet med informasjonssikkerhet og personvern er lite systematisk og risikobasert, mangler helhet og er lavt prioritert.
- Forskning og høyere utdanning er like mye eller mer utsatt for trusler som mange andre samfunnssektorer.

Motsatt kan risikoen sies å være liten dersom:

- Forskning og høyere utdanning forvalter store og viktige informasjonsverdier.
- Evne til å ivareta informasjonsverdiene er godt utviklet fordi arbeidet med informasjonssikkerhet og personvern er risikobasert og systematisk, velfungerende, helhetlig og tilstrekkelig prioritert.
- Forskning og høyere utdanning er like mye eller mindre utsatt for trusler som mange andre samfunnssektorer.

Vurderinger av risiko – stor, liten eller middels – er ingen eksakt vitenskap. Vurderingene og konklusjonene må basere seg på god kjennskap til sektortilstanden og grundige faglige evalueringer av tilstanden sett i lys av sektormålene.

Kapitteloversikt

I kapittel 1 gis et tentativt omriss av hvilke informasjonsverdier som forvaltes i sektoren.

I kapittel 2 gis en oversikt over trusler og hendelser, det vil si hvilke typer sikkerhets- og personvernbrudd sektoren har opplevd, og hvilke trussel-aktører som står bak hendelsene.

I kapittel 3 gis en oversikt over viktige initiativ som sektoren har iverksatt for å redusere risikoen for brudd på informasjonssikkerheten og for mangelfull etterlevelse av personvernregelverket.

I kapittel 4 gis en oversikt over viktige sårbarheter/utfordringer som preger arbeidet med informasjonssikkerhet og personvern på sektornivået.

I det siste kapitlet – kapittel 5 – presenteres den samlede vurderingen av risiko basert på drøftelsene i de foregående kapitlene. Det inneholder også enkelte anbefalinger til tiltak.

Vedlegg

I vedlegg 1 gjøres det rede for datagrunnlaget som rapporten baserer seg på.

1. Informasjonsverdier i sektoren

Innledning

Dette kapittelet er et forsøk på å antyde hva som kan være de viktigste informasjonsverdiene i forskning og høyere utdanning.

Å beskrive informasjonsverdier i sektoren er en krevende oppgave fordi «verdilandskapet» er omfattende og uoversiktlig. Formålet med kapittelet er å gi en tentativ forståelse av hva informasjonsverdiene *kan være*. Poenget er altså å antyde et omriss av hvilke verdier som forvaltes for å kunne bedre forstå hva konsekvensene av risiko kan være.

Hva er informasjonsverdier?

I høyere utdanning og forskning er forsvarlig forvaltning av informasjonsverdier en fundamental forutsetning for at universiteter og høgskoler skal kunne fremstille og formidle kunnskap av høy kvalitet og ved bruk av vitenskapelige metoder. Sikker forvaltning av informasjonsverdier, og forsvarlig behandling av opplysninger om enkeltpersoner, er derfor avgjørende for at institusjonene skal kunne løse sitt samfunnsoppdrag på en god måte.

Med informasjonsverdier i høyere utdanning og forskning menes alle typer data, opplysninger og dataressurser (IT-utstyr, applikasjoner, systemer, datanettverk, osv.) som har betydning for hvordan universiteter og høgskoler utfører sine kjerneoppgaver. Eksempler på informasjonsverdier kan være ustrukturert informasjon (i form av notater, dokumenter, publikasjoner, video- og lydopptak, osv.) eller strukturert informasjon (studentdata i administrative systemer, data i forskningsdatabaser, svar i surveyundersøkelser, osv.). Det kan også være informasjon i form av rådata, typisk forskningsdata som enda ikke er systematisert og analysert, eller i form av bearbeidet informasjon (for eksempel forskningspublikasjoner og undervisningsmateriell).

Informasjonsverdier vil omfatte personopplysninger, det vil si informasjon eller vurderinger som kan knyttes til enkeltpersoner. Det vil også omfatte opplysninger eller data som ikke inneholder informasjon om enkeltpersoner.

Til sist vil informasjonsverdier omfatte de dataressurser – applikasjoner, systemer, databaser, datanettverk, osv. – som benyttes for behandling av data og opplysninger.

Dette betyr at informasjonsverdier kan deles inn i to hovedkategorier:

- Data og opplysninger i seg selv.
- Bærerne av data og opplysninger – dataressurser som håndterer eller genererer innhold. Dette inkluderer tekniske løsninger som institusjonene drifter selv, fellesløsninger som driftes av andre statlige aktører (for eksempel Unit) og tjenester levert av kommersielle virksomheter (Microsoft, Google, osv.).

I noen tilfeller kan verdien være tilgangen til ressurser, for eksempel e-infrastruktur for tungregning eller sensornettverk. Da er det tilgangen til å gjøre store beregninger eller målinger som er verdien og ikke informasjonen i seg selv.

Variasjonsbredde og verdier

Universiteter og høgskoler forvalter store mengder informasjonsverdier. Samtidig er det betydelig variasjoner i hvilke typer informasjonsverdier som institusjonene er ansvarlige for. Dette skyldes blant annet at universiteter og høgskoler forvalter data og opplysninger innenfor mange ulike fag- og forskningsområder.

Informasjonsverdiene i forskning og høyere utdanning kan spenne fra trivielle personopplysninger til svært sensitive opplysninger om studenter eller ansatte, for eksempel politiattester, skikkethetsvurderinger eller utestengelsesvedtak. I forskningsvirksomheten kan det dreie seg om alt fra lite sensitive studentprosjekter til store forskningsprosjekter, understøttet av kostbare digitale løsninger, hvor resultatene er underlagt eksportkontroll.

Verdi for hvem?

Variasjonsbredden i de informasjonsverdiene som forvaltes i sektoren innebærer at verdiene kan ha betydning for mange ulike aktører.

Forskningsdata kan for eksempel brukes som grunnlag for politikkutforming og forvaltning. Noen eksempler på dette er vær- og klimadata, maritime data, geologiske data og helsedata. Dersom man ikke kan bruke disse dataene til å treffe riktige beslutninger eller gjennomføre viktige forvaltningsoppgaver, nasjonalt eller internasjonalt, representerer dette utfordringer som vil merkes langt utenfor UH-sektorens grenser. Å forstå disse verdikjedene og avhengighetene er viktig når verdier skal vurderes.

Det kan også finnes informasjonsverdier som er av vesentlig verdi for den enkelte institusjon eller forsker, men som har mindre direkte betydning på sektor- og samfunnsnivå. Det vil også finnes andre aktører enn offentlig forvaltning, institusjonene selv og den enkelte forsker som har interesse av informasjonsverdiene i sektoren. Det kan for eksempel være private aktører (samarbeidspartnere) i privat sektor eller dataeiere i andre sektorer (for eksempel industriaktører eller registerforvaltere i andre sektorer).[5] Der hvor det behandles personopplysninger vil disse opplysningene ha særlig betydning for de som opplysningene gjelder (studenter, ansatte, deltakere i forskningsprosjekter, osv.).

Forskjellige verdidimensjoner

I tillegg til at informasjonsverdier har ulik betydning for forskjellige aktører, kan verdiene forstås i lys av ulike verdidimensjoner. Registerdata, for eksempel på helseområdet, illustrerer hvilke verdidimensjoner dette kan handle om:

- Kommersiell verdi – registerdata kan gi grunnlag for patenter.

[5] Samarbeidspartnere kan også være forskningsfinansiører. Institusjonene nevnte flere eksempler på slike partnere/finansiører, for eksempel Equinor, Huawei, Kongsberggruppen, Rolls Royce, Swiss Timing eller Ulstein-gruppen. Mange institusjoner hadde også samarbeid med offentlige virksomheter, f.eks. virksomheter i helsesektoren og grunnopplæringen som tilbyr praksisplasser for studenter.

- Samfunnsøkonomisk verdi – registerdata kan føre til nye medisinske behandlingsformer.
- Investeringsverdi – tap av registerdata kan medføre store gjenanskaffelseskostnader.
- Gjenbruksverdi – registerdata kan representere en ukjent fremtidig verdi.[6]

Særlig viktige verdier?

Enkelte typer informasjonsverdier kan sies å være mer betydningsfulle enn andre. Lovgiver har for eksempel vedtatt at personopplysninger om studenter, ansatte eller forskningsdeltakere har særlig verdi for den enkelte og samfunnet. Det samme gjelder opplysninger undergitt taushetsplikt eller helsedata om enkeltpersoner som benyttes i medisinsk og helsefaglig forskning.

Samtidig har universiteter og høgskoler egne strategier og utviklingsavtaler[7] som (i noen grad) identifiserer hvilke kunnskapsdomener som er særskilt viktige for den enkelte institusjon.

En første tilnærming til de viktigste informasjonsverdiene på sektornivået er at disse kan identifiseres gjennom:

- Nasjonale prioriteringer for forskning.
- Prosjekter for etablering av forskningsinfrastruktur.
- Felles dataressurser i forskning og høyere utdanning.
- Lange tidsserier (forskningsdata).

Nasjonale prioriteringer for forskning

Nasjonale prioriteringer for forskning er fastsatt i «Langtidsplan for forskning og høyere utdanning 2019-2029». De forskningsområdene som prioriteres i langtidsplanen er (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. Prioriteringen av disse fem områdene er en klar vektlegging av den verdien de representerer på nasjonalt nivå.

Forskningsinfrastruktur

Bærere av data og opplysninger – forskningsinfrastrukturer – er avgjørende for effektiv og innovativ kunnskapsproduksjon.[8] En nasjonal satsing på forskningsinfrastruktur gjøres av Norges forskningsråd gjennom «Norsk veikart for forskningsinfrastruktur». I veikartet tydeliggjøres det

---

[6] Se for eksempel Norges forskningsråd (2016): Enklere tilgang – mer forskning. Status og forbedringsmuligheter for norske persondata i helseforskning.

[7] Utviklingsavtalene er avtaler mellom departementet og et lærested. Avtalene inneholder mål og styringsparametre for prioriterte utviklingsområder for institusjonen. De gir rom for å løfte frem områder der institusjonene ser behov for særlig oppmerksomhet.

[8] Se for eksempel «Langtidsplan for forskning og høyere utdanning 2019–2028», side 14.

at fremtidige forskningsinfrastrukturer vil representere en betydelig verdi i norsk kunnskapsproduksjon og -formidling.

Uninett AS leverer og drifter forskningsnettet i Norge. Dette representerer en betydelig infrastrukturressurs for sektoren. I tillegg tilbyr Uninett en rekke andre datatjenester. Uninett sitt datterselskap – Sigma2 – tilbyr infrastrukturressurser i form av systemer for tungregning og for lagring og deling av data.

Av andre infrastrukturressurser i sektoren kan nevnes tjenester som leveres og driftes av Universitetet i Oslo, for eksempel «Tjenester for sensitive data».

Fellestjenester

Fellestjenester i administrasjon, forskning og undervisning representerer viktige informasjonsverdier. Mange av disse leveres, driftes eller forvaltes av Unit. Andre viktige fellestjenester driftes av kommersielle leverandører (skytjenesteleverandører) som Unit har inngått rammeavtaler med.

Fremover vil Unit (i samarbeid med andre aktører, for eksempel BOTT) tilby nye tjenester som vil være at betydelig verdi for sektoren. Det gjelder blant annet læringsanalyse, felles løsning for tilgangsstyring i sektoren og neste generasjons utdanningsplattform.

Arkivering og publisering av forskningsdata for gjenbruk i senere forskningsprosjekter representerer en viktig verdi i sektoren (åpne data). Løsninger for dette tilbys av flere aktører, blant annet Norsk senter for forskningsdata (NSD). Samtidig samler og forvalter NSD andre informasjonsverdier, for eksempel nøkkelinformasjon om sektoren som benyttes til styrings- og forskningsformål.[9]

Eksisterende, og ikke minst, fremtidige satsinger på tjenestekjeder vil også utgjøre viktige informasjonsverdier i sektoren. Effektiv saksbehandling og forbedret brukeropplevelse er blant gevinstene som slike tjenestekjeder kan gi.[10]

Lange tidsserier

Lange dataserier (tidsserier) representerer særlige beskyttelsesverdige informasjonsverdier. Dette er data som enten vil være svært kostbare eller umulige å gjenskaffe dersom de skulle gå tapt. Samtidig er verdien av tidsserier vanskelig å antyde fordi gjenbrukspotensialet (mulig fremtidig bruksverdi) i stor grad er ukjent.

Eksempler på lange tidsserier finnes blant annet på klima- og miljøområdet.[11] Norge har for eksempel noen av de lengste hydrologiske, oseanografiske og meteorologiske tidsseriene i

[9] Dette gjelder «Database for statistikk om høgre utdanning».

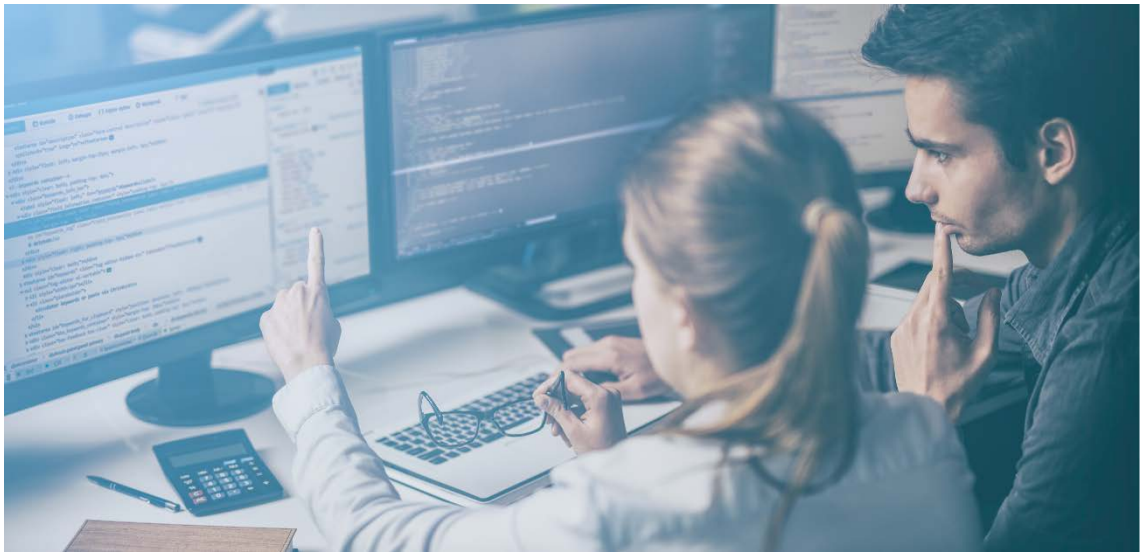
[10] Se Kunnskapsdepartementet (2018): Tjenestekjeder i kunnskapssektoren. Rapport fra «Arbeidsgruppen for flyt og deling av data».

[11] Norges forskningsråd (2004): Lange tidsserier for miljøovervåking og forskning. Viktige marien dataserier. Rapport nr. 3.

verden. Tilsvarende tidsserier finnes innenfor andre fagområder. Eksempler fra helseområdet inkluderer Helseundersøkelsen i Nord-Trøndelag og Tromsøundersøkelsen.[12]

Andre verdier i sektoren

I neste kapittel skal vi se at brudd på informasjonssikkerheten og krenkelser av personvernet ofte kan være økonomisk motivert. Her handler det om at eksterne aktører tar kontroll over lokale informasjonsverdier og benytter verdiene til egne formål. Eksempler på dette er, som vi skal se, misbruk av opplysninger om ansatte for å gjennomføre skreddersydde svindelforsøk (direktørsvindel), eller at tilgangen til lokale systemer og tjenester blokkeres for å presse institusjonene til å utbetale penger.



[12] Se https://www.ntnu.no/hunt og https://uit.no/forskning/forskningsgrupper/gruppe?p_document_id=367276.

2. Hendelser og trusler i sektoren

Innledning

Brudd på informasjonssikkerheten og krenkelser av personvernet forårsakes av trusler, det vil si ulike typer «kilder til fare».[13] Det kan dreie seg om eksterne trusler, for eksempel kriminelle grupper eller statlige aktører. Det kan også dreie seg om interne trusler, for eksempel studenter som behandler informasjonsverdier og personopplysninger på feil måte. I tillegg kan det finnes en rekke andre «kilder til fare» (mangelfull kompetanse hos tjeneste-leverandører; gjesteforskere som ikke kjenner sikkerhetspolicy, osv.).

I dette kapitlet følger først en kort oversikt over hvordan nasjonale sikkerhetsmyndigheter, og enkelte nasjonale og utenlandske sikkerhetseksperter/-organer, vurderer «kilder til fare» i forskning og høyere utdanning.

Deretter gis en oversikt over sikkerhetshendelser og skadevirkninger av disse som statlige universiteter og høgskoler rapporterte at de hadde vært utsatt for i 2017 og 2018. Det gis samtidig en kort oversikt over de viktigste trussel-aktørene.

Til slutt gis en kortfattet oversikt over avvik fra regler og interne rutiner for behandling av personopplysninger som institusjonene rapporterte at de hadde opplevd i løpet av samme tidsperiode (2017-18).

Generelt om trusler og trussel-aktører i sektoren

I USA har informasjonssikkerhet lenge vært ranket blant de aller viktigste fokusområdene i forbindelse med digitalisering i forskning og høyere utdanning. I 2019 ble komplekse informasjonssikkerhetsutfordringer vurdert som den mest betydningsfulle trenden i digitalisering av forskning og høyere utdanning i USA.[14] Samtidig hevdes det at høyere utdanning er den samfunnssektoren i USA som har størst problemer med å håndtere sikkerhetshendelser og dataangrep, for eksempel hacking eller skadevare.[15]

Andre sikkerhetsmiljøer, for eksempel sikkerhetsselskapet «FireEye», peker i sine globale trusselvurderinger på at utdanningssektoren er utsatt for trussel-aktører som søker tilgang til

---

[13] Denne definisjonen av trusler er hentet fra Direktoratet for forvaltning og IKT sin begrepsliste (tilgjengelig på https://internkontroll-infosikkerhet.difi.no/begrepsliste#Trusler%20eller%20trusselkilder).

[14] EDUCASE Center for Analysis and Research (2019): Higher Education's 2019 Trend Watch & Top 10 Strategic Technologies. Oppsummering av resultatene fra studien er tilgjengelig på https://library.educause.edu/resources/2019/1/higher-educations-2019-trend-watch-and-top-10-strategic-technologies.

[15] Foresite (2018): Higher Education One of the Worst at Handling Cyber Attacks. Tilgjengelig på https://foresite.com/higher-education-one-of-the-worst-sectors-at-handling-cyber-attacks/.

verdifull informasjon eller enkelt tilgjengelige dataressurser.[16] «FireEye» utga i 2015 en trusselrapport for de nordiske landene. I rapporten fremgår det at utdanningssektoren ble rammet av seks prosent av alle alvorlige og målrettede dataangrep i 2013-14.[17]

Nasjonale sikkerhetsmyndigheter

Nasjonal sikkerhetsmyndighet uttrykker i sin siste nasjonale (og åpne) risikovurdering bekymring for at forskning er potensielle mål for fremmede staters etterretningsvirksomhet.[18] I Politiets sikkerhetstjeneste sin årlige trusselvurdering legges det vekt på at risikoen for dataangrep og «kunnskapstyveri» fra fremmede staters myndigheter er særlig stor i «(…) forskningsmiljøer som jobber med undervannsteknologi, kompositttmaterialer, styringsteknologi og test- og måleutstyr».[19]

Også Politidirektoratet mener at forskningsinstitusjoner og akademia er attraktive for dataangrep og «kunnskapstyveri» fra fremmede stater. Direktoratet mener at forskningsmiljøer som jobber med fornybar energi, grønn teknologi, industrielle prosesser, medisin og romfart er spesielt utsatt.[20]

Etterretningstjenesten fremhever at forskningsinstitusjoner og akademia kan være utsatt for forsøk på uautorisert tilgang til kunnskap som er underlagt eksportkontroll (kunnskap som kan utnyttes til fremstilling av våpensystemer).[21]

I tillegg til de særskilte truslene som forskning og høyere utdanning er eksponert for, advarer nasjonale sikkerhetsmyndigheter mot kriminelle aktører. Det påpekes at disse trussel-aktørene blir stadig mer profesjonelle og bedre organisert. Metodene deres har blitt mer avanserte og målrettede.

---

[16] FireEye: M-Trends 2019. Tilgjengelig på https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

[17] FireEye (2015): Cyber Threats to the Nordic Region. Tilgjengelig på https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf.

[18] Nasjonal sikkerhetsmyndighet: Risiko 2019. Krafttak for et sikrere Norge. Side 11. Tilgjengelig på https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf.

[19] Politiets sikkerhetstjeneste: Trusselvurdering 2019. Side 9. Tilgjengelig på https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/.

[20] Politidirektoratet: Trusler og utfordringer innen IKT-kriminalitet (2017). Tilgjengelig på https://www.politiet.no/globalassets/dokumenter/pod/ikt_krim_pod.pdf.

[21] Etterretningstjenesten: Fokus 2019. Etterretningstjenestens vurderinger av aktuelle sikkerhetstrusler. Tilgjengelig på https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf. Se spesielt side 12, 15 og 95.

Sikkerhetshendelser og dataangrep

Det er ikke enkelt å estimere antallet sikkerhetshendelser og dataangrep som statlige universiteter og høgskoler utsettes for. Rapporter fra institusjonene selv indikerer imidlertid at sektoren utsettes for en god del hendelser/angrep hvert år. Samtidig rapporterte institusjonene at bare en liten del av hendelsene/angrepene kan beskrives som alvorlige.

Tilstanden i sektoren speiler dermed beskrivelsene som nasjonale sikkerhetsmyndigheter gir av tilstanden i samfunnet for øvrig: mange mindre hendelser, få store og alvorlige.[22]

Kategorisering: hendelser, angrep og skadevirkninger

Nedenfor følger en kategorisering av de vanligste hendelser, angrep, skadevirkninger og trussel-aktører som institusjonene rapporterte om.

Merk at kategoriene ikke er gjensidig utelukkende, det vil si at kategoriene i noen grad er overlappende. Det innebærer at samme hendelse kan plasseres i flere enn én av kategoriene. Vi har for eksempel en egen kategori for hendelser som omhandler direktørsvindel eller «kunnskapstyveri», men slike hendelser vil også ofte kunne havne under overskriften målrettet nettfisking. Hendelser som omhandler ID-tyveri kan havne i flere kategorier (nettfisking, målrettet nettfisking og brudd på personopplysningssikkerheten).

Dette kategoriseringsproblemet til tross – i sum mener vi oversikten gir et relativt dekkende bilde av de viktigste hendelser, angrep og skadevirkninger som sektoren rapporterte om.

Nettfisking (phishing)

Dette var den hyppigst forekommende sikkerhetshendelsen som institusjonene rapporterte om. Det var ofte enkeltpersoner eller kriminelle grupper med økonomiske motiver som sto bak hendelsene. I enkelte tilfeller kunne det være virksomheter eller stater som er ute etter å stjele kunnskap/forskningsresultater (se nedenfor).

Nettfisking går ut på at brukerne (studenter eller ansatte) lures til å gi fra seg brukernavn og passord til sin brukerkonto. Institusjonene opplyste at når slike angrep lyktes, kunne kaprede kontoer bli brukt til å masseutsendelse av epost (spam).[23] Masseutsendelsene førte blant annet til at enkelte institusjoner ble svartelistet hos sine leverandører av eposttjenester og av andre tjenesteleverandører som hadde blitt rammet av utsendelsene.

Institusjonene rapporterte også om at nettfisking kunne medføre at lokale brukere ble lurt til å besøke nettsider hvor deres datautstyr ble infisert med skadevare. Skadevaren kunne for eksempel overvåke brukernes atferd, hente ut data eller avbryte databehandlingen.

---

[22] Nasjonal sikkerhetsmyndighet: Risiko 2019. Krafttak for et sikrere Norge. Side 10. Tilgjengelig på https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf.

[23] Flere institusjoner som hadde vært utsatt for dette rapporterte at det var iverksatt sikringstiltak for å unngå gjentakelse. Det handlet om sperring av epostkontoer dersom det normerte antallet epostutsendelser for en gitt tidsperiode (for eksempel ett døgn) ble overskredet.

Skadevirkningen for institusjonene ble hovedsakelig rapportert å være ekstraarbeid, eventuelt noe omdømmetap på grunn av svartelistingen.

Målrettet nettfisking (spear phishing)

Dette ble rapportert å være en hyppig forekommende sikkerhetshendelse. Mange institusjoner mente at målrettet nettfisking var en tiltakende trend i sektoren.

Poenget med målrettet nettfisking er ofte det samme som for nettfisking. Forskjellen består i at angrepet er mer forseggjort: det sendes eposter til brukerne hvor det nevnes interne forhold eller navn på kolleger. Dette er ment å styrke troverdigheten til eposten og øke sannsynligheten for at brukerne lar seg lure til å oppgi brukernavn og passord, eller til å besøke internettsider som inneholder ulike typer skadevare.

Skadevirkningene og hvem som står bak disse angrepene (trussel-aktørene) ble rapportert å være det samme som når det gjaldt vanlig nettfiske.

Direktørsvindel

Direktørsvindel er en spesiell form for målrettet nettfisking som vanligvis retter seg mot økonomimedarbeidere. Også dette ble rapportert å være en hyppig forekommende sikkerhetshendelse i sektoren. Medarbeideren mottar typisk en epost som tilsynelatende kommer fra direktøren. I eposten oppgis det at det haster med å få betalt en regning, og det bes om at dette gjøres snarest. Dersom økonomimedarbeideren betaler overføres pengene til trussel-aktøren (enkeltpersoner eller kriminelle grupper) som står bak angrepet.

Ingen institusjoner rapporterte at penger hadde blitt utbetalt. Flere institusjoner oppga at det i enkelte tilfeller nesten hadde skjedd.

Skadevirkningen ble primært oppgitt å være ekstraarbeid og en viss grad av engstelse eller bekymring blant økonomimedarbeiderne.

Løsepengevirus

Flertallet av institusjonene rapporterte at de hadde vært utsatt for løsepengevirus – gjerne mange ganger – i løpet av de siste to årene. Løsepengevirusangrep er en form for datakidnapping. Angrepene skjer ofte ved at brukerne mottar en epost med lenke til tilsynelatende legitime nettsider (nettfiske-epost). Dersom brukeren klikker på lenken lastes det ned et program på datamaskinen som «låser ned» innholdet på maskinen. For å få tilgang til innholdet igjen blir brukerne bedt om å betale penger til den eller de som står bak (enkeltpersoner eller kriminelle grupper).

Flertallet av institusjonene som hadde vært utsatt for løsepengevirus rapporterte at de hadde sikkerhetskopier av innholdet på de rammede datamaskinene. Dermed ble innholdet reddet ved at dataene ble gjenopprettet fra sikkerhetskopien.

Skadevirkningene for disse institusjonene var primært ekstraarbeid. Enkelte institusjoner opplyste om flere tilfeller med tap av forskningsdata og vitenskapelige artikler/manus.

Brudd på personopplysningssikkerheten

Et flertall av institusjonene rapporterte at de hadde vært utsatt for brudd på konfidensialiteten til opplysninger om studenter eller ansatte. Det kunne for eksempel handle om at personlig informasjon ble publisert på nett eller hadde vært tilgjengelig fra internettet. Videre handlet det om feilsending av epost som inneholdt sensitive personopplysninger eller dokumenter i

personalsaker. Det forekom også tilfeller med mangelfull skjerming av opplysninger om student med hemmelig adresse.

Videre ble det rapportert om flere tilfeller hvor forskningsdata (helsedata, for eksempel lyd- og videoopptak av konsultasjoner) hadde blitt håndtert på måter som satte opplysningenes konfidensialitet i fare. Det ble i tillegg nevnt eksempler på tyveri av kredittkortopplysninger og uautorisert tilgang til eller eksponering av opplysninger om privat økonomi. Til sist rapporterte enkelte institusjoner at personopplysninger hadde kommet på avveie på grunn av stjålet eller mistet IT-utstyr (datamaskiner eller minnepinner).

De viktigste skadevirkningene som følge av disse sikkerhetshendelsene ble oppgitt å være ekstraarbeid, omdømmetap (negative medieoppslag), noe «intern støy» (fordeling av skyld og ansvar for det som hadde gått galt), et visst økonomisk tap (gjenkjøp av stjålet IT-utstyr) og krenkelser av personvernet til de som opplysningene gjaldt. I ett tilfelle hadde Datatilsynet ilagt overtredelsesgebyr for brudd på personopplysningsloven.

Trussel-aktørene i slike saker kan være enkeltpersoner eller kriminelle grupper med økonomiske motiver. I andre tilfeller ble hendelsene forårsaket av uhell, ubetenksomhet eller mangelfull kompetanse hos studenter eller ansatte.

Misbruk av dataressurser

Enkelte institusjoner rapporterte at de hadde vært utsatt for tilfeller med misbruk av lokale dataressurser. Det handlet dels om kriminelle grupper som utnyttet lokale datamaskiner og datakraft til utvinning av krypto-valuta (Bitcoin, Monero). Dels handlet det om at eksterne aktører benyttet datamaskiner og lokale datanettverk i angrep mot andre mål enn institusjonene selv, for eksempel Visma Software eller industrielle anlegg i utlandet.[24] Det ble også rapportert om at eksterne aktører hadde tatt kontroll over lokal IT-infrastruktur for å utføre tjenestenektangrep mot andre mål. Enkelte av angrepene ble beskrevet som avanserte, ressurskrevende, langvarige og sannsynligvis utført av fremmede lands myndigheter.

Det ble også rapportert om telefonsentraler som var blitt hacket. Uvedkommende hadde dermed kunne ringte på institusjonenes bekostning.

Skadevirkningene for institusjonene ble rapportert å være manglende tilgang til og legitim utnyttelse av lokale dataressurser og noe økonomisk tap. Samtidig vil andre enn institusjonene selv rammes når lokale dataressurser anvendes i angrep mot andre mål.

«Kunnskapstyveri» (spionasje)

Enkelte institusjoner rapporterte at de hadde vært utsatt for tilfeller av «kunnskapstyveri» og industrispionasje eller forsøk på dette. Her dreide det seg blant annet om trussel-aktører som handlet på vegne av utenlandske myndigheter. Disse aktørene skaffet seg tilgang til vitenskapelige publikasjonsdatabaser (hos disse institusjonene) og stjal tusenvis av

[24] Visma Software ble utsatt for et større datainnbrudd i februar 2019. Det ble hevdet at trussel-aktører med nære bånd til kinesiske myndigheter sto bak datainnbruddet. Se Reuters, 6. februar 2019: China Hacked Norway's Visma to Steal Client Information.

forskningsartikler. I andre tilfeller var det uklart hvilke aktører som sto bak «kunnskapstyveriene».

Det ble også rapportert at eksterne aktører hadde forsøkt å stjele forskningsresultater. Dette gjaldt innenfor forskningsområder som robotikk, data science, droneforskning, bio- og genteknologi. Det ble opplyst at tyveriforsøkene trolig ikke hadde lyktes.

Skadevirkningene ble primært vurdert å være omdømmetap. Det ble opplyst at omdømmetapet kunne skade tilliten til institusjonene blant offentlige og private samarbeidspartnere eller finansiører. Hendelsene kunne i tillegg få økonomiske konsekvenser for enkelt-forskere dersom de ble frastjålet intellektuelle hemmeligheter med kommersielt potensial.

Andre sikkerhetshendelser

Institusjonene rapporterte om en del sikkerhetshendelser som ikke lett lar seg passe inn i kategoriene ovenfor. Her dreide det seg om noen få tilfeller av tjenestenektangrep, blant annet rettet mot enkelte institusjoners hjemmesider og læringsplattformer, og hacking av studentserver (hacking skjedde trolig fra Kina).

Videre ble det rapportert om tilfeller med tap av forskningsdata på grunn av diskkrasj. Andre sikkerhetshendelser inkluderte bortfall av trådløst nettverk, perioder med ustabil tilgang til enkelte IT-tjenester, bortfall av IT-tjenester på grunn av strømbrudd og manipulasjon av innholdet på hjemmesider.[25]

Til slutt ble det rapportert om hendelser som ikke kan defineres som sikkerhetsbrudd eller dataangrep, for eksempel at ansatte hadde vært utsatt for forsøk på pengeutpressing via epost.[26]

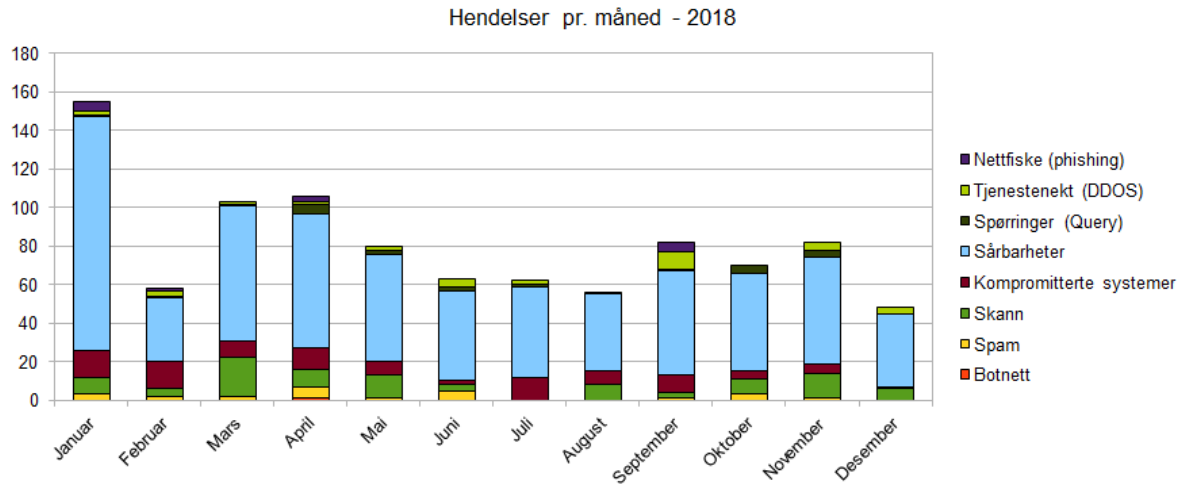
Uønsket aktivitet i forskningsnettet

Uninett CERT jobber med avdekking og varsling av IT-sikkerhetshendelser og dataangrep i det norske forskningsnettet. Uninett CERT lager månedlig statistikk om uønsket aktivitet i forskningsnettet. Statistikken for 2018 viser at det totalt gikk ut varsel om 965 sikkerhetshendelser, dataangrep eller sikkerhetsrelaterte utfordringer i forskningsnettet.[27]

[25] Det ble for eksempel rapportert om tilfeller hvor politiske aktivistgrupper hadde lagt ut propaganda på institusjonenes hjemmesider (de-facing).

[26] Epostmottakeren fikk melding om at avsenderen (pengeutpresseren) var i besittelse av kompromitterende bilder eller video hvor mottakeren figurerte. Mottakeren fikk deretter beskjed om at publisering ville skje dersom penger ikke ble overført til avsenderens bankkonto. Politianmeldelse ble vurdert ved minst én institusjon, men denne institusjonen valgte ikke å anmelde forholdet.

[27] Dette tallet inkluderer ikke hendelser som handlet om brudd på opphavsrett, for eksempel ulovlig nedlasting av filmer, musikk eller tv-serier.



FIGUR 1

Figuren viser oversikt over sikkerhetshendelser som Uninett CERT oppdaget og har varslet om i forskningsnettet pr. måned i 2018.

De hyppigst forekommende sikkerhetsutfordringene som ble varslet var, ifølge Uninett CERT sin 2018-statistikk:

1. Sårbare datamaskiner: 682 varslede saker i 2018.

2. Kompromitterte datamaskiner: 95 varslede saker i 2018.

3. Scan (skanning): 95 varslede saker i 2018.

Sårbare datamaskiner er datamaskiner (servere, PC-er, nettverkskomponenter, osv.) som har et sikkerhetshull (en sårbarhet) i seg som kan utnyttes av uvedkommende. Kompromitterte datamaskiner er maskiner som er blitt angrepet, enten som følge av at de har hatt en sårbarhet i seg eller at de er feilkonfigurert slik at uvedkommende har fått uautorisert tilgang til maskinene og bruker den til tvilsomme formål. Scan (skanning) er datamaskiner i forskningsnettet som leter etter sikkerhetssårbarheter eller åpne porter hos andre datamaskiner i eller utenfor forskningsnettet. Dette oppfattes som «fiendtlig» aktivitet i nettet og varsles.

Avvik fra lokale rutiner – personopplysninger

Ut over sikkerhetshendelser og dataangrep, ble det rapportert om avvik fra lokale rutiner for behandling av personopplysninger og brudd på personopplysningsregelverket (den norske personopplysningsloven og GDPR).

Nedenfor følger en kortfattet og punktvis oversikt over de viktigste rutineavvikene som institusjonene rapporterte om:

- Feil registrering og lagring av personopplysninger: Studenter og ansatte lagret sensitive eller sterkt personlige opplysninger på usikre lagringsområder eller på IT-utstyr (bærbare datamaskiner og minnepinner) hvor det ikke var tillatt å oppbevare slike opplysninger. Det handlet også om at studenter og forskere registrerte

personopplysninger på privat IT-utstyr (for eksempel mobiltelefoner) i strid med det lokale IT-reglementet.

- Manglende sletting av personopplysninger: Studenter og, i litt mindre grad, vitenskapelige ansatte glemte eller unnlot å slette personopplysninger ved avslutningen av studentoppgaver (bachelor og master), Ph.d.-arbeider eller andre typer forskningsprosjekter.

- Manglende vurdering av behandlingsgrunnlag: Studenter eller ansatte startet behandlingen av personopplysninger uten først å ha vurdert om de hadde lov til dette, og uten å ha avgjort hva den lovlige grunnen til behandlingen i så fall var.

- Feil bruk av nettressurser: Ansatte tok i bruk nettbaserte tjenester uten at det først var gjort en vurdering av informasjonssikkerheten i tjenestene. Det handlet blant annet om at nettbaserte tjenester ble tatt i bruk uten at det var inngått lovpålagte avtaler med leverandørene (databehandleravtaler).

- Feil publisering av personopplysninger: Ansatte som på grunn av hastverk eller ubetenksomhet ignorerte rutiner for publisering av personopplysninger på internettet. Det handlet også om feil bruk av lokale publiseringsløsninger (som gjorde opplysningene tilgjengelige fra internett).

- Mangelfull dokumentasjon: Informasjonssikkerhets- og personvernarbeid ble ikke skriftliggjort på tilfredsstillende måte. Det kunne medføre at dokumentasjonskrav, spesielt i personvernregelverket (GDPR), ikke ble godt nok ivaretatt.

Mange institusjoner rapporterte om avviksbekymringer (potensielle avvik), spesielt når det gjaldt ivaretakelsen av enkelte av personvernrettighetene i personopplysningsloven og forordningen (GDPR). Det gjaldt særlig retten til innsyn, retting og sletting av egne opplysninger.

Til slutt ble det rapportert om noen få tilfeller med uredelighet i forskning som også omfattet avvik fra lokale rutiner for sikker håndtering av personopplysninger (og brudd på lovverk som regulerer informasjonssikkerhet og personvern i forskning).

3. Risikoreduserende initiativ i sektoren

Innledning

I dette kapitlet diskuteres de viktigste risikoreduserende initiativene som institusjonene rapporterte at de hadde iverksatt. Initiativene hadde blitt iverksatt for å (i) unngå brudd på informasjonssikkerheten og (ii) styrke etterlevelsen av reglene om behandling av personopplysninger (GDPR).

Diskusjonene i kapitlet fokuserer på følgende risikoreduserende initiativ:

- Utarbeidelse av og vedtak om ledelsessystemer for informasjonssikkerhet (internkontroll), inkludert toppledelsens og styrenes rolle i arbeidet.
- Gjennomføring av GDPR-prosjekter eller -aktiviteter (inkludert utnevnelse av personvernombud, kartlegginger av IT-systemer/-tjenester og oversikter over behandlinger av personopplysninger).
- Behandling av personopplysninger i visse typer forskning.
- Iverksetting av informasjons-, bevisstgjørings- og opplæringstiltak.
- Økende bruk av risikovurderinger.
- IT-avdelingenes rolle, inkludert styrking av evnen til håndtering av IT-sikkerhetshendelser og dataangrep via internettet.

Nedenfor følger en gjennomgang av hver enkelt av disse risikoreduserende initiativene.

Ledelsessystemer for informasjonssikkerhet (internkontroll)

Alle institusjonene hadde utarbeidet eller var i ferd med å ferdigstille utarbeidelsen av ledelsessystemer for informasjonssikkerhet. Hos de institusjonene som var i ferd med å sluttføre utarbeidelsen ble det rapportert at den styrende delen[28] av ledelsessystemene var ferdigstilt, men at det fortsatt manglet viktige deler av eller enkelte elementer i de gjennomførende og kontrollerende[29] delene av systemet.

Institusjoner som hadde utarbeidet alle delene av sine ledelsessystemer rapporterte at det enten var iverksatt revisjoner av systemene eller at revisjoner var planlagt for å tilpasse systemene til det nye personvernregelverket.

Utarbeidelsen (helt eller delvis) av ledelsessystemer for informasjonssikkerhet innebar at alle institusjonene hadde utpekt en lokal leder eller koordinator/ressursperson for arbeidet med informasjonssikkerhet (informasjonssikkerhetsleder/-rådgiver). Samtidig innebar det at toppledelsen hadde blitt forelagt forslag til ledelsessystemer for behandling. I noen institusjoner var det derfor toppledelsen som hadde vedtatt innføringen av ledelsessystemer, men det var mer og mer vanlig at universitets- eller høgskolestyrene behandlet og vedtok systemene etter innstilling fra ledelsen.[30] Det var også en økende tendens til at universitets- eller høgskolestyrene ønsket rapportering på arbeidet med innføring av ledelsessystemer for informasjonssikkerhet.

Mange institusjoner rapporterte at de hadde et årshjul for arbeidet med informasjonssikkerhet, og at det ble gjennomført status- og planleggingsmøter med toppledelsen (ledelsens gjennomgang). Samtidig understreket flere av institusjonene at graden av involvering fra toppledelsen og styret kunne være personavhengig, for eksempel at det tidligere styret var mer opptatt av informasjonssikkerhet enn det nye (eller motsatt).

Hos noen institusjoner ble det rapportert at arbeidet med informasjonssikkerhet enten var integrert i den ordinære virksomhetsstyringen, eller at det forelå konkrete planer om dette. Tanken med dette var at informasjonssikkerhet ikke lenger skulle være en «satellitt» på siden av den øvrige virksomhetsstyringen, men at arbeidet måtte ses i sammenheng med annen internkontroll i virksomhetene, viktige digitaliseringstiltak og institusjonenes budsjettprosesser.

---

[28] Den styrende delen inneholder toppledelsens (direktør og/eller rektors) krav til og føringer for institusjonens arbeid med informasjonssikkerhet, for eksempel sikkerhetsmål/-strategi, beskrivelser av ansvars- og oppgavefordeling (sikkerhetsorganisering) og kriterier for vurdering av akseptabel risiko.

[29] De gjennomførende og kontrollerende delene inneholder beskrivelser av hvordan det praktiske informasjonssikkerhetsarbeidet skal utføres (for eksempel rutiner og verktøy for gjennomføring av risikovurderinger), og krav til gjennomføring av egnekontrollaktiviteter (revisjoner, avvikshåndtering, osv.).

[30] I enkelte institusjoner var hele ledelsessystemet (styrende, gjennomførende og kontrollerende deler) behandlet og vedtatt av enten toppledelsen eller styret. I andre institusjoner gjaldt dette bare den styrende delen.

GDPR-prosjekter og -aktiviteter

Alle 21 universiteter og høgskoler hadde etablert GDPR-prosjekter eller -aktiviteter (med aktiviteter menes tiltak for etterlevelse av GDPR, men som ikke formelt sett er organisert som et prosjekt). Disse prosjektene og aktivitetene inkluderte blant annet kartlegginger av IT-systemer/-tjenester og tekniske løsninger, og hvilke data/personopplysninger som systemene/tjenestene inneholdt (for eksempel administrative systemer, forskningsdatabaser, skytjenester eller nettbaserte undervisningsressurser).

Antallet systemer og tjenester som var kartlagt kunne være stort, og ble rapportert å variere fra omkring 650 til i overkant av 40. Mange av institusjonene rapporterte at system- og tjenestekartleggingene ikke var fullstendige, og at det derfor gjensto noe kartleggingsarbeid.

I tillegg hadde det blitt utarbeidet oversikter (protokoller) som inneholdt nøkkelopplysninger om behandlinger av personopplysninger, for eksempel hvilke typer opplysninger som ble behandlet i ulike systemer/tjenester, hvem opplysningene dreide seg om, osv. Det var dessuten utarbeidet nye eller foretatt revidering av eksisterende rutiner og retningslinjer for håndtering av personopplysningene, inkludert hvordan personvernrettighetene til blant annet studenter, ansatte og deltakere i forskningsprosjekter skulle ivaretas.

FIGUR 2

Figuren viser i hvilken grad de 21 institusjonene rapporterte at de hadde oversikt over sine informasjonsverdier, inkludert personopplysninger, i alle deler av organisasjonen.

Til slutt hadde enkelte institusjoner utarbeidet eller revidert sine ledelsessystemer for informasjonssikkerhet innenfor rammen av sine GDPR-prosjekter/aktiviteter.

Alle institusjonene hadde ansatt, leid inn eller utpekt personvernombud.

Personopplysninger i visse typer forskning

Riksrevisjonens funn fra revisjoner av forskningssystemer gjennomført hos tre universiteter og høgskoler i 2017, reiste spørsmål om hvor god kontrollen med bruken av personopplysninger i forskning er.[31] Her ble det særlig pekt på at disse institusjonene ikke kunne dokumentere at de hadde den oversikten over og kontrollen med personopplysninger som kreves etter personvernregelverket.

Et gjennomgående trekk i rapporteringen fra institusjoner hvor det foregikk medisinsk og helsefaglig forskning, var at oversikten over og kontrollen med behandlinger av helsedata i disse prosjektene ble rapportert å være relativt god eller tilfredsstillende. Årsakene til dette ble dels rapportert å være at denne typen forskning er underlagt særskilt rettslig regulering.[32] Dels handlet det om at mange institusjoner hadde medarbeidere i forskningsadministrasjonen (sentralt eller på fakultetsnivå) med særskilt kompetanse på forskningsetikk, inkludert informasjonssikkerhet og personvern i medisinsk og helsefaglig forskning.

Institusjonene rapporterte at de støttet seg på tjenestene fra Norsk senter for forskningsdata (NSD) for å holde oversikt over prosjektporteføljen i andre typer forskningsprosjekter (enn

[31] Riksrevisjonen (2017): Revisjonsrapport for 2017 om informasjonssikkerhet i forskningssystemer. Tilgjengelig på https://www.riksrevisjonen.no/globalassets/rapporter/no-2018-2019/revisjonsrapport2017informasjonssikkerhetforskningssystemer.pdf.

[32] Se lov om medisinsk og helsefaglig forskning. Loven krever blant annet at medisinske og helsefaglige student- eller forskningsprosjekter må godkjennes av regionale forskningsetiske komiteer før oppstart av prosjektene. I forskrift om organisering av medisinsk og helsefaglig forskning stilles det krav til institusjonene (forskningsansvarlig) om internkontroll og forskningsprotokoll.

medisinske og helsefaglige) hvor personopplysninger ble behandlet. Disse prosjektoversiktene var viktige for institusjonenes kontroll med informasjonssikkerhet og personvern.

Institusjonene rapporterte imidlertid at de ikke kunne vite om alle student- og forskningsprosjekter som skulle meldes til NSD faktisk ble meldt. Ved flere institusjoner ble det uttrykt mistanke om at underrapporteringen (til NSD) kunne ha et ikke helt ubetydelig omfang.

Mange institusjoner rapporterte at «Tjenester for sensitive data» (TSD), som tilbys og driftes av IT-avdelingen ved Universitetet i Oslo (USIT),[33] hadde vært viktig for informasjonssikkerheten i forskningsprosjekter hvor det ble behandlet sensitive personopplysninger, spesielt helsedata. Oppfatningen var at TSD hadde gitt et viktig bidrag til institusjonenes kontroll med hensyn til sikkerhet og personvern i forskning hvor særlig beskyttelsesverdige personopplysninger håndteres.

Samtidig mente flere av institusjoner at TSD ble for kostbart for små forskningsprosjekter, inkludert studentforskning. Disse institusjonene uttrykte forventninger til at neste-generasjons TSD («TSD light») ville kunne anvendes i slike prosjekter.[34]

Informasjons-, bevisstgjørings- og opplæringstiltak

Alle institusjoner hadde iverksatt ulike typer tiltak for å informere og bevisstgjøre studenter og medarbeidere om (i) viktigheten av informasjonssikkerhet og personvern og (ii) hvilke krav som gjaldt for behandling av personopplysninger. Mange av disse tiltakene var iverksatt i forbindelse med GDPR-prosjekter/-aktiviteter, men informasjons- og bevisstgjøringstiltak som spesielt omhandlet informasjonssikkerhet var ikke direkte koblet til GDPR. Det vanligste tiltaket på informasjonssikkerhetsområdet var deltakelse i Norsk senter for informasjonssikring sin årlige sikkerhetskampanje i oktober («Sikkerhetsmåneden»).[35]

Institusjonene rapportert at det var gjennomført interne kurs og informasjonsmøter om informasjonssikkerhet og personvern, særlig i tilknytning til GDPR-arbeidet. Kursene og informasjonsaktiviteten var primært rettet mot institusjonenes medarbeidere, både administrativt og vitenskapelige ansatte, men det ble også rapportert om aktivitet rettet mot studentmassen. Spesielt enkelte av høgskolene rapporterte at det var (eller var i ferd med å bli) gjennomført kurs for ansatte i praktisk informasjonssikkerhets- og personvernarbeid.

Mange institusjoner hadde gjort tilgjengelig informasjon om sikkerhet og personvern på hjemmesider eller via intranettet. Her kunne det blant annet bli gitt informasjon om GDPR og lokale rutiner eller retningslinjer for sikker og lovlig behandling av personopplysninger. Det ble videre informert om institusjonenes ledelsessystem for informasjonssikkerhet, og det var

[33] Denne tjenesten tilbyr sikker innsamling, analyse/beregning og lagring av sensitive forskningsdata, se https://www.uio.no/tjenester/it/forskning/sensitiv/mer-om/.

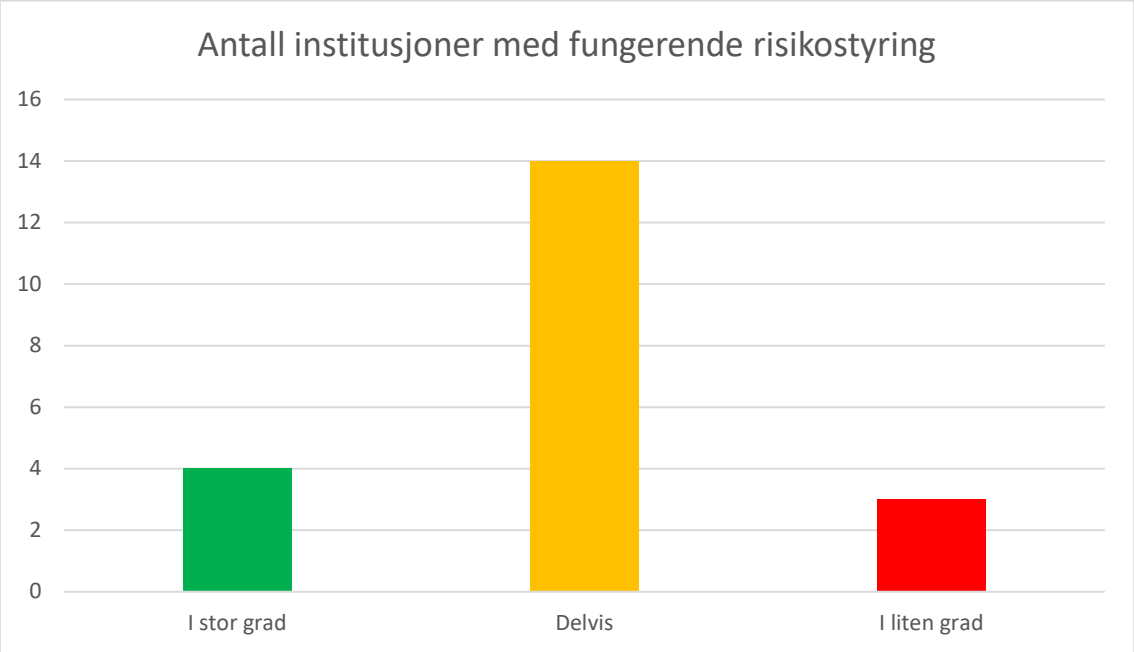
[34] Beskrivelse av og planer for «TSD light» er tilgjengelig på https://www.usit.uio.no/om/it-dir/planer/2019/dokumenter/tsd-light-oppstart.html.

[35] «Sikkerhetsmåneden» tilbyr en informasjons- og opplæringspakke til deltakende virksomheter. Pakken inkluderer blant annet nano-læringskurs. Institusjonene rapporterte om til dels stor deltakelse blant studenter og ansatte i «Sikkerhetsmåneden». Det var ikke uvanlig at det ble arrangert egne foredrag om informasjonssikkerhet for studenter og ansatte hvor eksterne foredragsholdere var invitert.

publisert personvernerklæringer (generell informasjon om hvordan institusjonene håndterte personopplysninger rettet til «alle og enhver»). Det kunne også bli gitt informasjon om institusjonenes personvernombud.

Risikovurderinger

Alle institusjonene rapporterte at det hadde vært gjennomført risikovurderinger av informasjonssikkerheten i ett eller flere IT-systemer og -tjenester. Risikovurderingene virket primært å omfatte IT-systemer eller -tjenester hvor det ble behandlet personopplysninger. Antallet risikovurderinger som hadde blitt gjennomført varierte en god del mellom de ulike institusjonene.



FIGUR 3

Figuren viser hvor mange av de 21 institusjonene som rapporterte at de helt, delvis eller i liten grad gjennomførte risikovurderinger og fulgte opp vurderingene med nødvendige sikringstiltak.

Inntrykket var at risikovurderinger blir gjennomført med større hyppighet i dag enn for få år tilbake. Dette gjaldt spesielt ved anskaffelser av nye IT-systemer eller -tjenester. Enkelte institusjoner beskrev risikovurderinger av nye systemer og tjenester som en innarbeidet rutine.

Det ble også vist til at risikovurderinger gjennomført i regi av Uninett i forbindelse felles-anskaffelser i sektoren, for eksempel digital eksamen eller ny læringsplattform (Canvas), hadde bidratt til at det ble gjort vurderinger av informasjonssikkerheten i lokale anskaffelsesprosesser.

IT-avdelingene og hendelseshåndteringskapasitet

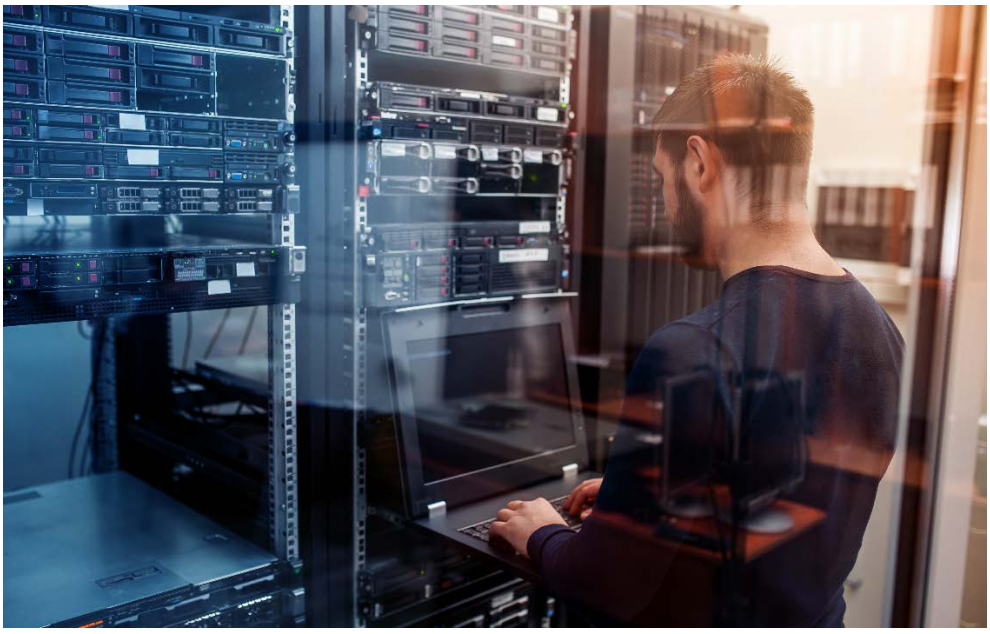
Mange av personalressursene som institusjonene rapporterte om, det vil si stillinger som helt eller delvis var dedikert til arbeidet med informasjonssikkerhet og personvern, var knyttet til IT-avdelingene. IT-avdelingene utgjorde derfor ryggraden i det lokale arbeidet med informasjonssikkerhet og (til dels) personvern/GDPR.

IT-avdelingenes sentralitet kan forstås som en sårbarhet etter som informasjonssikkerhet og personvern handler om langt mer enn teknisk sikring av IT-løsninger.[36] På den annen side: dersom vi ser bort fra de personalressursene som IT-avdelingene bidro med, blir det relativt lite annet igjen. IT-avdelingenes ressursinnsats må derfor forstås som en av styrkene i institusjonenes arbeid med informasjonssikkerhet og personvern/GDPR.

20 av 21 institusjoner rapporterte at de hadde (etter initiativ fra Uninett CERT) opprettet lokale hendelseshåndteringsteam (IRT-er). Team-medlemmene var vanligvis ansatt i IT-avdelingene, og deres hovedoppgaver var todelt: (i) mottok meldinger om IT-sikkerhetshendelser og dataangrep fra Uninett CERT og (ii) iverksette lokale tiltak for å hindre eller redusere skadevirkningene av eventuelle hendelser og angrep. Denne sektoromspennende «brannslukkingsstyrken» representerer en ny infrastruktur for beskyttelse av data, opplysninger, applikasjoner, nettverk og andre digitale ressurser mot trussel-aktører som angriper via internett og forskningsnettet.

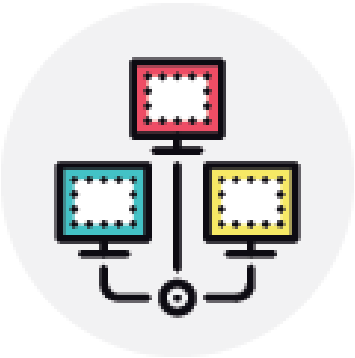
I tillegg rapporterte institusjonene at de benyttet seg av tjenester for overvåking og analyse av datatrafikk for å avdekke og forhindre dataangrep. Dette handlet om tjenester fra Uninett CERT, men også fra kommersielle leverandører. Også tjenester fra Universitetet i Oslo ble benyttet for å forebygge/håndtere dataangrep.

Til slutt var det enkelte store institusjoner som hadde bygd opp sentrale spesialistmiljøer for forebygging, avdekking og håndtering av IT-sikkerhetshendelser og dataangrep (CERT-/SOC-enheter). Disse spesialistmiljøene samarbeidet blant annet med Uninett CERT.



[36] Å hevde at IT-teknisk sikring er alt som trengs for å ivareta informasjonssikkerheten og personvernet blir som å hevde at trafikksikkerheten kun avhenger av bilens tekniske stand. Men det finnes andre viktige forhold, for eksempel om sjåføren har fått tilstrekkelig kjøreopplæring eller kvaliteten på veivedlikeholdet, som ikke er helt uten betydning når trafikksikkerheten skal vurderes.

4. Sårbarhetene i det lokale arbeidet



Initiativene diskutert i forrige kapittel har bidratt til å redusere risikoen for brudd på informasjonssikkerheten og for manglende etterlevelse av regler om behandling av personopplysninger (GDPR).

Men kartleggingen avdekket også at arbeidet med informasjonssikkerhet og personvern i sektoren preges av viktige sårbarheter. Med sårbarheter menes områder hvor institusjonene selv rapporterte at arbeidet med informasjonssikkerhet og personvern ikke fungerte godt nok, og hvor det ble rapportert om tydelig forbedringspotensial.

I dette kapitlet diskuteres de viktigste sårbarhetene som institusjonene rapporterte om. Diskusjonene fokuserer på følgende sårbarheter:

- Begrensede personalressurser og kapasitet.
- Mangelfull kompetanse om informasjonssikkerhet og personvern.
- Mangelfull iverksetting av ledelsessystemer for informasjonssikkerhet.
- Mangelfull oversikt over informasjonsverdier i visse typer forskning.
- Betydelig teknisk og organisatorisk kompleksitet.
- Manglende planer for håndtering av større informasjonssikkerhetshendelser (kontinuitet).

Nedenfor følger en gjennomgang av hver enkelt av de nevnte sårbarhetene.

Begrensede personalressurser og kapasitet

Et vesentlig element i ledelsessystem for informasjonssikkerhet er at ledelsen setter av tilstrekkelige ressurser til å gjennomføre det praktiske sikkerhetsarbeidet. Når dette ikke er tilfelle representerer det en sårbarhet som kan bidra til økt risiko for hendelser.

19 av 21 institusjoner ga uttrykk for at personalressursene som var avsatt til arbeidet med informasjonssikkerhet og personvern ikke var tilstrekkelig for å dekke behovet. Dette til tross for at ressurssituasjonen hadde forbedret seg noe de siste årene, for eksempel ved at personvernombud hadde blitt ansatt, innleid eller utnevnt. Det var også enkelte institusjoner som rapporterte at IT-avdelingene ville ansette medarbeidere med IT-sikkerhetskompetanse.

Selv om mange institusjoner ønsket flere dedikerte årsverk eller større stillingsprosenter på sentralt nivå i virksomhetene, var det et minst like tydelig budskap at det var behov for «flere hender i arbeid» i hele organisasjonslandskapet, for eksempel på fakulteter eller i fagavdelinger. Konsekvensen av manglende personalressurser var, ifølge institusjonene, at mange oppgaver ikke ble utført, ble utført for sjelden, eller ble utført med mangelfull kvalitet.

I det følgende gis en oversikt over hvilke andre sårbarheter som begrensede personalressurser og kapasitet ble rapportert å føre til.

Sentralisert versus desentralisert

Universiteter og høgskoler er relativt desentraliserte organisasjoner hvor lokale enheter kan ha forholdsvis stor grad av autonomi, spesielt på forsknings- og undervisningssiden. Samtidig er det meningen at arbeidet med informasjonssikkerhet og personvern skal strekke seg fra toppledelsen og ut til det enkelte fakultet, institutt, fagavdeling – og nå frem til hver enkelt medarbeider og student. Det er derfor av betydning hvordan den rapporterte personalinnsatsen er organisert og fordelt i organisasjonslandskapet.

Som allerede indikert, var det overordnede bildet at personalinnsatsen var konsentrert på sentralt nivå. Ovenfor har vi sett at IT-avdelingene var tunge aktører – det var i disse avdelingene at mye av personalinnsatsen foregikk. Når det gjaldt personvern kom også enkelte andre avdelinger i sentraladministrasjonen i spill, for eksempel arkiv, lønn/personal og forskningsavdelingene.

Personalinnsatsen på enhetsnivå (fakulteter, institutter, fagavdelinger, osv.), både med hensyn til informasjonssikkerhet og personvern, ble enten beskrevet som variabel eller beskjeden – eller at man manglet oversikt over hva som foregikk. Det ble med noen få unntak ikke rapportert om at det på enhetsnivå fantes helt eller delvis dedikerte personalressurser som jobbet med personvern eller informasjonssikkerhet.[37]

Enkelte større institusjoner hadde opprettet personvernkontakter/-rådgivere på enhetsnivå.[38] Personvernkontaktene skulle bistå lokalt ansatte med spørsmål knyttet til personvern og, til dels, informasjonssikkerhet. Omfanget av innsatsen til personvernkontaktene ble rapportert å være variabel. Det ble videre rapportert fra enkelte institusjoner at arbeidet med personvernkontakter/-rådgivere kunne vært organisert på en mer systematisk måte.

Enkelte andre institusjoner hadde opprettet egne informasjonssikkerhetsforum.[39] Forumenes hovedoppgave var å planlegge, koordinere og å bidra til å løfte arbeidet med informasjonssikkerhet og personvern i alle delene av organisasjonen, inkludert på enhetsnivå. Hos institusjoner med denne typen forum ble det likevel rapportert at omfanget av ressursinnsatsen på enhetsnivå var noe uklar/variabel, eller ikke av samme omfang som på sentralt nivå.

---

[37] Unntakene gjaldt de største institusjonene. Her ble det rapportert om ansatte i forskningsadministrasjonen på enhetsnivå, primært på medisinske eller helsefaglige fakultet, som jobbet dedikert med personvern og GDPR.

[38] Personvernkontaktene/-rådgiverne var administrativt ansatte med særskilt kompetanse om rettslige regler for elektronisk behandling av personopplysninger (GDPR). Personvernkontakt/-rådgiver var vanligvis, men ikke alltid, en rolle som det ikke var knyttet stillingsprosenter til.

[39] Informasjonssikkerhetsforum var typisk en del av virksomhetenes ledelsessystemer for informasjonssikkerhet. Funksjonen til forumene kunne variere noe, men var vanligvis å koordinere arbeidet med informasjonssikkerhet, og å gi råd til toppledelsen om sikkerhetsprioriteringer og større initiativ/tiltak.

I de minste institusjonene ble det rapportert at forholdene var relativt oversiktlige, det vil si at personalressurser på sentralt nivå (informasjonssikkerhetsleder/-rådgiver og/eller personvernombudet) relativt enkelt kunne skaffe seg kunnskap om omfanget av og statusen på enhetenes arbeid med informasjonssikkerhet og personvern. Sentralt plasserte personalressurser hadde dermed forutsetninger for å gi støtte til arbeidet på enhetsnivå. Men også her ble det rapportert at arbeidet på enhetsnivå ikke sto stødig på egen kjøl: initiativ og tilrettelegging fra sentralt hold var vanligvis avgjørende for at informasjonssikkerhets- og personvernaktiviteter skulle bli gjennomført.

Samordnet versus fragmentert

Ledelses- og internkontrollsystemer for informasjonssikkerhet og personvern skal, i teorien, strukturere og samordne ressursinnsatsen slik at helheten i arbeidet blir noe mer enn summen av enkeltinnsatser og -tiltak. Poenget er at enkeltinnsatser og -tiltak skal henge sammen og supplere hverandre. Men det som er sagt ovenfor indikerer at det er usikkert om tiltakene har hatt den tiltenkte effekten, så langt.

Også på sentralt nivå virket deler av personalinnsatsen å være noe fragmentert. Mye av innsatsen var, som tidligere nevnt, knyttet til IT-avdelingene. Denne innsatsen fremsto som best organisert og mest samordnet. Innsatsen i de øvrige delene av sentraladministrasjonen (utenfor IT-avdelingene) virket å være noe mer tilfeldig. Her dreide det seg ofte om enkelt-ansatte i forskningsadministrasjon, studieadministrasjon eller på lønns- og personalsiden som hver på sin kant jobbet noe med informasjonssikkerhet og personvern.

Samtlige institusjoner hadde ansatt, leid inn eller utnevnt personvernombud. Ombudene er ment å spille en rådgivende og kontrollerende rolle i arbeidet med personvern og GDPR. Det ble likevel rapportert at mange av ombudene hadde gjort en større innsats enn det som kreves av dem etter loven. Enkelte ombud hadde for eksempel stått i spissen for det lokale GDPR-arbeidet.

Dette kan tyde på at enkelte av ombudene var i ferd med å få en samordningsrolle for deler av innsatsen på personvernområdet. I noen institusjoner ble det derfor rapportert at samordningsrollen strakk seg ut over – og kunne komme i konflikt med – de rådgivings- og kontrolloppgavene som ombudene etter loven er ment å ivareta.

Administrativt versus vitenskapelig ansatte

De fleste av personalressursene som ble benyttet i arbeidet med informasjonssikkerhet og personvern var altså knyttet til sentraladministrasjonen. Denne ressursfordelingen innebar at personalressursene i det alt vesentlige var rekruttert blant de administrativt ansatte: det var disse medarbeiderne som gjorde hovedjobben. Det ble i liten grad rapportert om tilsvarende innsats blant de vitenskapelig ansatte, men med et visst unntak for medisinsk og helsefaglig forskning.

Det ble likevel opplyst at vitenskapelig ansatte, og studenter, var ment å utføre viktige arbeidsoppgaver knyttet til informasjonssikkerhet og personvern. Utfordringen, slik den ble rapportert av institusjonene, var enten at dette i liten grad var tilfelle, eller at man ikke kjente godt nok til hvordan spørsmål om informasjonssikkerhet og personvern ble håndtert av de vitenskapelig ansatte (igjen med et visst unntak for medisinsk og helsefaglig forskning).

Mangelfull kompetanse

Mangelfull kompetanse i praktisk informasjonssikkerhets- og personvernarbeid var et annet gjennomgående trekk i rapporteringen fra institusjonene. Mangelen på praktisk kompetanse ble

rapportert å gjelde alle grupper, det vil si administrativt og vitenskapelig ansatte, studenter og eksterne veiledere eller sensorer. Bekymringene var imidlertid størst når det gjaldt vitenskapelig ansatte og studenter. Dette kom spesielt til uttrykk ved at risikoen for brudd på informasjonssikkerheten eller for manglende etterlevelse av personvernregelverket ble vurdert å være størst i forskning, studentforskning og undervisning.

Det ble videre rapportert at ledere i forskningsprosjekter og veiledere i student- og ph.d.-prosjekter var ment å sørge for eller bidra til at behandling av forskningsdata i disse prosjektene skjedde på en sikker, etisk forsvarlig og lovlig måte. Det ble understreket at dette i noen grad også var tilfelle. Her ble det særlig fremhevet at mange forskere innenfor fagområder som medisin og livsvitenskap, helse- og sosialfag hadde til dels høy bevissthet om informasjonssikkerhet og personvern.

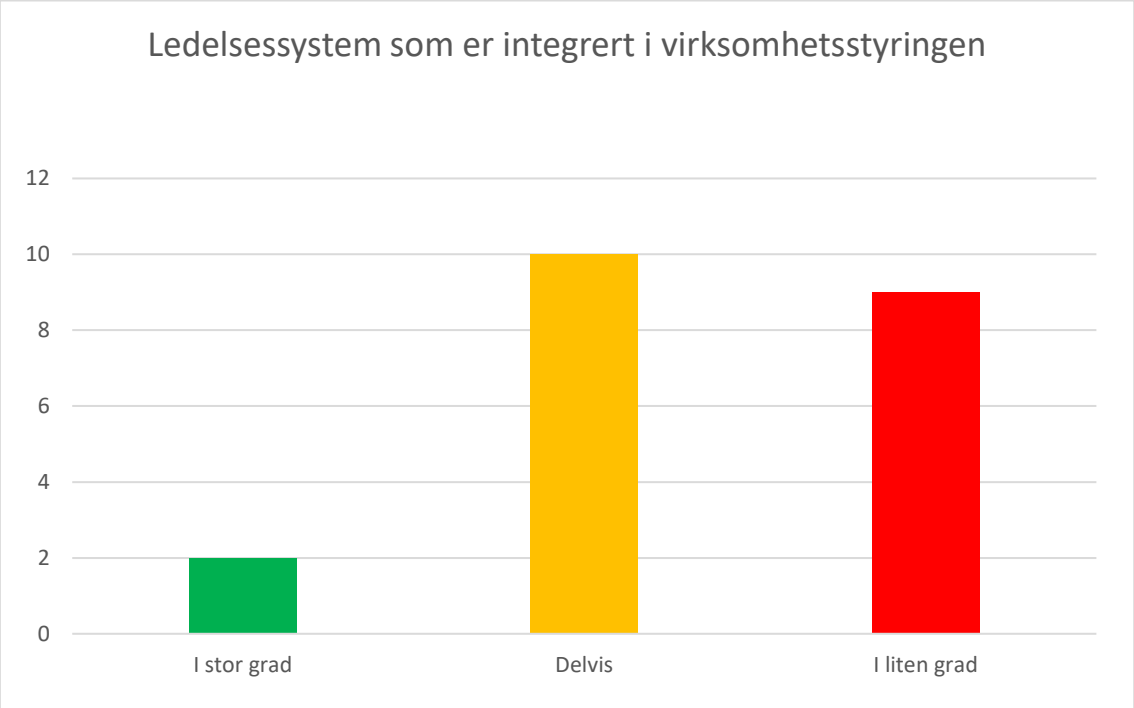
Samtidig ble det rapportert at vitenskapelig ansatte og studenter manglet kompetanse om hvilke retningslinjer som gjaldt, særlig når det kom til sikring av forskningsdata. Dette handlet for eksempel om bruk av elektronisk opptaksutstyr for registrering av intervjudata (video- eller audioopptak), sikker lagring av data underveis i forsknings- eller studentprosjekter og forsvarlig sletting, eller anonymisering og arkivering, av forskningsdata ved prosjektslutt. Selv om enkelte høgskoler rapporterte om at det var iverksatt, eller planlagt iverksatt, kurs i informasjonssikkerhet og personvern som også var rettet mot vitenskapelig ansatte, mente flertallet av institusjonene at det var vanskelig å nå ut til fakulteter, institutter eller fagavdelinger med effektive opplæringstiltak.

Det typiske bilde i de 21 institusjonene var derfor at de vitenskapelig ansatte kunne ha til dels høy personvern- og sikkerhetsbevissthet, i alle fall innenfor enkelte fagområder. Det ble likevel rapportert at innenfor de fleste fagområdene var det en mindre krets av administrativt ansatte, det vil si forskningsrådgiverne sentralt eller på fakultetsnivå, som tilrettela for at informasjonssikkerheten og rettslige krav til personvern ble ivaretatt.

I denne sammenheng er det verdt å notere at risikovurderinger av forskningsprosesser, som det tidligere sekretariatet for informasjonssikkerhet gjennomførte i sektoren, indikerte at forskerne ivaretok informasjonssikkerheten og personvernet uten at administrasjonen var kjent med det. Det kunne for eksempel handle om at forskerne på eget initiativ tok i bruk krypteringsløsninger for å sikre viktige data fordi det ikke fantes tekniske løsninger for dette på institusjonsnivå. Det kan derfor tenkes at informasjonssikkerhets- og personvernkompetansen på forskersiden er noe større enn hva som gjennomgående ble rapportert i denne kartleggingen.

Mangelfull iverksetting av ledelsessystemer

Ovenfor har vi sett at institusjonene hadde etablert og vedtatt ledelsessystemer for informasjonssikkerhet, eller var i ferd med å gjøre det. Ledelsessystemene var enten vedtatt av toppledelsen eller av styrene. Det ble likevel rapportert at innføringen av systemene – sørge for at sikkerhetsoppgaver faktisk ble utført og at informasjonssikkerheten eller personvernet ble forbedret – var en utfordring hos mange institusjoner. Det innebar at ledelsessystemene i varierende grad var integrert i den øvrige virksomhetsstyringen. Hos et fåtall institusjoner var dette tilfelle, men det var også institusjoner som rapporterte om at de hadde iverksatt tiltak med tanke på å integrere systemene i virksomhetsstyringen.



FIGUR 4

Figuren viser hvor mange av de 21 institusjonene som rapporterte at de hadde et velfungerende ledelsessystem for informasjonssikkerhet som er integrert i virksomhetsstyringen.

Det ble videre rapportert at hovedårsakene til mangelfull iverksetting av ledelsessystemene var kombinasjonen av begrensede personalressurser og lite kompetanse om praktisk informasjonssikkerhets- og personvernarbeid. Det ble også nevnt at manglende iverksetting kunne skyldes liten bevissthet om utfordringer knyttet til informasjonssikkerhet og personvern. Noen institusjoner omtalte sine ledelsessystemer som «godt bevarte hemmeligheter».

Mangelfull iverksetting av ledelsessystemer for informasjonssikkerhet ble rapportert å medføre følgende sårbarheter i institusjonenes arbeid:

Gjennomføring av risikovurderinger

I forrige kapittel så vi at institusjonene rapportert at risikovurderinger av informasjonssikkerheten i IT-systemer og -tjenester ble gjennomført i større grad nå enn tidligere, spesielt i anskaffelsesprosesser. Det ble likevel opplyst at arbeidet med risikovurderinger fortsatt var noe mangelfullt eller at slike vurderinger trolig ikke ble gjennomført slik som forutsatt.

Mangelfull gjennomføring av risikovurderinger handlet dels om at det ble gjort for få vurderinger sammenliknet med behovet. Dette hang i noen grad sammen med at mange institusjoner manglet fullstendig oversikt over hvilke IT-systemer og -tjenester som var i bruk. Dermed ble det vanskelig å vite om alle systemer eller tjenester ble risikovurdert. Dels handlet det om at kvaliteten på gjennomførte vurderinger ble rapportert å være usikker eller svak (jf. det som er sagt om mangelfull kompetanse ovenfor). Hos disse institusjonene ble det derfor pekt på behovet for å kvalitetssikre den jobben som var gjort.

Flere institusjoner opplyste at dokumentasjonen av vurderingene burde vært bedre.

Oppfølging av risikovurderinger (innføring av sikringstiltak)

Enkelte institusjoner rapporterte at det vanligvis ble iverksatt nye sikringstiltak dersom risikovurderingene viste at det var behov for det. Flertallet av institusjonene opplyste imidlertid at de ikke hadde oversikt over om risikovurderinger ble fulgt opp med nødvendige tiltak. Det ble derfor rapportert at det var uklart om sikringstiltak faktisk ble iverksatt.

Usikkerheten knyttet til statusen på arbeidet med oppfølging av risikovurderinger, berodde i stor grad på at de som hadde ansvaret for å iverksette sikringstiltak (vanligvis system- eller tjenesteeiere) ikke rapporterte om dette til informasjonssikkerhetsleder/-rådgiver. Bortsett fra hos enkelte av de mindre institusjonene, fantes det derfor lite tilfredsstillende oversikt over statusen for tiltaksarbeidet.

Mangelfull melding og håndtering av sikkerhetshendelser og avvik

Alle institusjoner hadde opprettet kanaler og laget rutiner for melding av sikkerhetshendelser og avvik fra rutiner for behandling av personopplysninger. Det ble likevel rapportert at relativt få eller ingen hendelser og avvik ble meldt gjennom de offisielle meldingskanalene. Samtidig ble det opplyst at det var gjort lite for å gjøre kanalene kjent blant studenter og ansatte. Det innebar ikke nødvendigvis at hendelser og avvik ikke ble meldt, men at formidlingen skjedde på andre måter: via epost og telefon eller ved fysisk oppmøte hos IT-support.[40]

Konsekvensen var at institusjonene manglet en samlet oversikt over meldte sikkerhetshendelser og rutineavvik.

Manglende oversikt over viktige forskningsdata

Oversikter over informasjonsverdier som trenger sikkerhet og hvor de befinner seg ble rapportert å eksistere når det gjaldt administrative behandlinger av opplysninger om studenter og ansatte (personopplysninger). I forbindelse med GDPR-prosjektene eller -aktivitetene var det også gjort en innsats for å få oversikt over hvor personopplysninger ble behandlet for forskning.

Et gjennomgående trekk var at institusjonene manglet en samlet oversikt over beskyttelsesverdige forskningsdata som ikke var personopplysninger. Dette gjaldt forskningsdata innenfor områder som robotikk, maritim forskning, energieffektive materialer, klimaforskning, oljeteknologi, molekylærbiologi, data science, droneforskning, kryptologi, nordområdene-forskning, deler av livsvitenskapen og geologiske undersøkelser. Det samme gjaldt for forskningsdata innenfor en rekke andre forskningsområder hvor personopplysninger ikke er sentrale informasjonsverdier.

Samtidig ble det rapportert at forskningsdata innenfor disse fagområdene representerte noen av de aller viktigste informasjonsverdiene som institusjonene forvaltet. Det innebar ikke nødvendigvis at alle disse forskningsdataene var mangelfullt sikret. Det fremsto likevel som uklart om eller i hvilken grad det var iverksatt nødvendige tiltak for å beskytte forskningsdata som ikke var personopplysninger.

[40] Slike henvendelser ble i noen grad registrert i ticket-systemer.

Teknisk og organisatorisk kompleksitet

Flere institusjoner, både universiteter og høgskoler, pekte på økende teknisk kompleksitet som en viktig utfordring i arbeidet med informasjonssikkerhet og personvern. Poenget her var at økende teknisk kompleksitet førte til flere potensielle svakheter og sikkerhetshull i digitale løsninger. Dette økte sannsynligheten for at ting gikk feil, og at feil ett sted spredte seg til andre systemer eller tjenester.[41]

Viktige årsaker til økt teknisk kompleksitet ble blant annet oppgitt å være duplisering av digitale løsninger, for eksempel ved at ulike lagringsløsninger ble benyttet parallelt (lokal lagring og skylagring). Tusenvis av brukere og datamaskiner, hundrevis av IT-systemer og nettjenester og store og åpne datanettverk bidro også til at det digitale landskapet ble beskrevet som komplisert. Det ble videre pekt på at lange og uoversiktlige tjenestekjeder, spesielt knyttet til nettbaserte tjenester, gjorde det utfordrende å vite hvor sikre løsningene var. Samtidig ble det vanskeligere å vite hvilke aktører som deltok i databehandlingen (leverandører, underleverandører, osv.), hvilke opplysninger aktørene hadde tilgang til, hva de brukte opplysningene til, hvordan opplysningene ble sikret og om opplysningene ble slettet ved avslutning av kundeforholdet.[42]

Hos flere av institusjonene ble utfordringer knyttet til teknisk kompleksitet forstått i lys av manglende kompetanse og kapasitet. Det ble særlig rapportert at komplekse tekniske løsninger gjorde det vanskelig for IT-medarbeiderne å drifte løsningene på en sikker og profesjonell måte. Det ble også opplyst at institusjonene savnet kapasitet til å lage retningslinjer for å gi veiledning om sikker og lovlig bruk av komplekse systemer.

Når det gjaldt organisatorisk kompleksitet handlet dette om at institusjonene ble beskrevet som sammensatte og desentraliserte: mange titalls organisatoriske enheter av varierende størrelse og med ulik faglig innretning, som var preget av forskjellige kulturer og tradisjoner og som kunne ha, til dels, betydelig autonomi. Det ble rapportert at det kunne være problematisk å innføre helhetlige systemer for styring av informasjonssikkerhet og etterlevelse av GDPR i et slikt organisasjonslandskap. Dette ble blant annet forklart med at organisatorisk kompleksitet gjorde det utfordrende å nå ut til alle sentrale og lokale enheter med riktig og tilpasset informasjon, for eksempel om hvilke rutiner som gjaldt for innhenting, lagring eller sletting av personopplysninger. Det kunne også gjøre det vanskelig og ressurskrevende å iverksette kompetansehevende tiltak.

Til slutt ble det rapportert at organisatorisk kompleksitet kunne føre til at det ble problematisk å få oversikt over risikobildet, det vil si å vite hvilke typer sikkerhets- og personvernproblemer som ulike deler av institusjonene faktisk sto overfor.

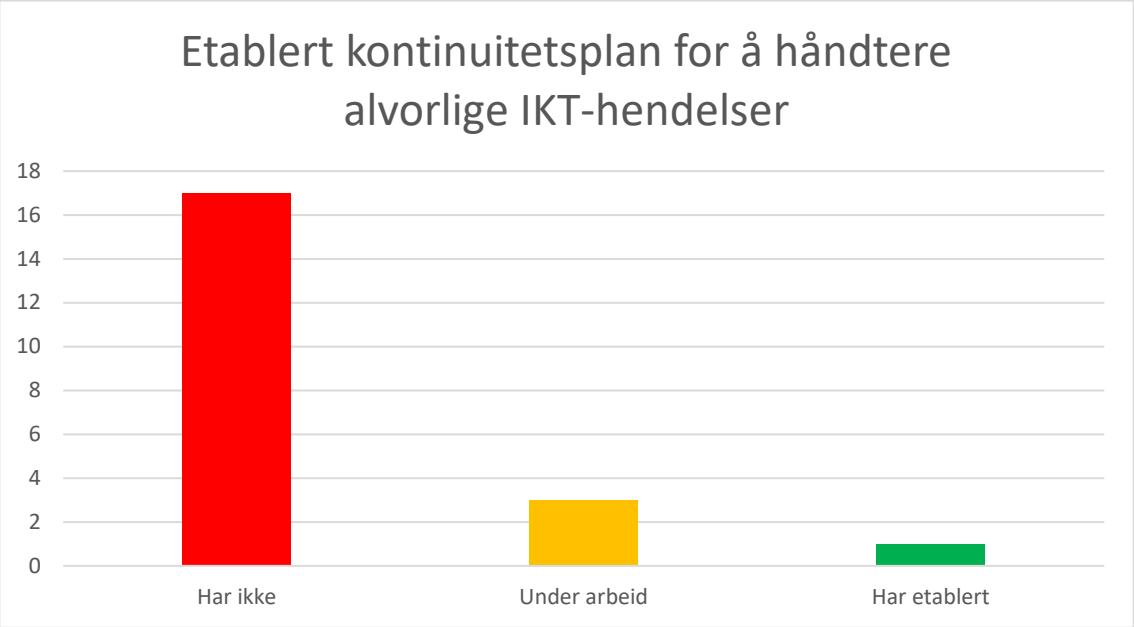
---

[41] Forholdet mellom teknisk kompleksitet og informasjonssikkerhet beskrives vanligvis som problematisk: «We do not know how to build secure systems of substantial complexity. But we can build very secure systems of limited functionality». Andrew Odlyzko (2019): Cybersecurity is Not Very Important. Side 17. Tilgjengelig på http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf.

[42] Lange leverandørkjeder, det vil si med mange underleverandører lokalisert i ulike land og verdensdeler, er vanlig i store skytjenester, for eksempel tjenestene til Google, Amazon og Microsoft.

Manglende beredskap for håndtering av større informasjonssikkerhetshendelser (kontinuitet)

Få institusjoner rapporterte at de hadde planer for gjenoppretting av driften dersom systemer, tjenester eller IT-infrastruktur ble rammet av et alvorlig dataangrep eller andre større sikkerhetshendelser. Det ble derfor heller ikke rapportert om at det var stilt krav til hvor raskt det var forventet at kritiske systemer eller tjenester skulle være tilgjengelige for bruk igjen etter at slike hendelser/angrep hadde inntruffet (kontinuitetsplaner). Enkelte institusjoner rapporterte imidlertid at de var i ferd med å utarbeide slike planer.



FIGUR 5

Figuren viser de 21 institusjonenes rapporterte status for arbeidet med etablering av kontinuitetsplaner.

En del institusjoner rapporterte at det var laget rollekort for håndtering av brudd på IT-sikkerheten. Rollekortene inngikk i det generelle beredskapsplanverket ved disse institusjonene. Det ble også rapportert fra flere institusjoner at det var iverksatt tiltak for å redusere skadevirkninger som følge av alvorlige dataangrep eller sikkerhetshendelser. Eksempler på dette var lagring av sikkerhetskopier på geografisk separate lokasjoner.

Det ble videre rapportert at det i liten grad ble gjennomført øvelser på håndtering av alvorlige sikkerhetsbrudd. Ved noen institusjoner ble det opplyst at beredskapsøvelser hadde inneholdt IT-spesifikke enkelt-elementer, for eksempel sjekking av logger i adgangskontrollsystemer. Flere institusjoner rapporterte at det var planlagt øvelser på håndtering av alvorlige informasjonssikkerhetshendelser i løpet av 2019.

Andre sårbarhetskilder

Institusjonene nevnte enkelte andre sårbarheter i arbeidet med informasjonssikkerhet og personvern. Dette var sårbarheter knyttet til fellessystemer og fellesinitiativ i sektoren, eller sårbarheter som institusjonene mente oppsto på grunn av manglende fellesinitiativ.

Fellessystemer

Flere institusjoner mente at det var behov for sterkere vektlegging av informasjonssikkerhet og personvern ved utvikling eller anskaffelser av fellessystemer i sektoren. Mer konkret handlet problematikken om at fellessystemer i sterkere grad burde tilrettelegges slik at det ble enklere for institusjonene å ivareta rettighetene i GDPR, spesielt retten til innsyn i egne opplysninger og retten til retting eller sletting av opplysninger.

Situasjonen, slik den ble rapportert av disse institusjonene, var at dersom dette ikke skjedde måtte jobben gjøres manuelt. Dette ble beskrevet som ineffektiv bruk av knappe ressurser. I enkelte tilfeller var det heller ikke mulig å få jobben gjort på grunn av manglende funksjonalitet.

Tjenesteyting på sektornivå

Flertallet av institusjonene, spesielt høgskolene, ga uttrykk for at det var problematisk at det ikke lenger finnes en enhet i sektoren som kan gi konsulent- og rådgivingsbistand til institusjonene på informasjonssikkerhet og personvern. Det ble understreket fra disse institusjonene at det er viktig at et slikt tjenestetilbud blir etablert, spesielt sett i lys av mangelfull kapasitet på institusjonsnivået.

Arbeidsverktøy

Til slutt ble det rapportert at institusjonene manglet egnede verktøy for å administrere arbeidet med informasjonssikkerhet og personvern. Dette ble oppfattet som en sårbarhet etter som manglende verktøystøtte gjorde det utfordrende å holde oversikt over viktige arbeidsoppgaver og statusen på disse. Det ble særlig etterspurt verktøy som gjorde det enklere å gjennomføre og følge opp risikovurderinger av informasjonssikkerheten i systemer og tjenester. Tilsvarende verktøy for vedlikehold av nøkkelinformasjon om institusjonenes behandling av personopplysninger (protokoller) ble også etterlyst.

Institusjonene ga uttrykk for at denne sårbarheten burde håndteres gjennom felles-anskaffelser på sektornivå.

5. Vurdering av risiko og anbefalinger

Innledning

I dette kapitlet gis en samlet og kortfattet vurdering av risiko opp mot sektormålene for arbeidet med informasjonssikkerhet og personvern (jf. drøftelsen av målene i innledningen til denne rapporten).

Avslutningsvis gis enkelte anbefalinger om hvilke tiltak som kan iverksettes for å håndtere risikoen, både av institusjonene selv, Unit og Kunnskapsdepartementet.

Informasjonsverdier

Statlige universiteter og høgskoler forvalter betydelige informasjonsverdier på vegne av fellesskapet. Verdiene foreligger i form av data og opplysninger i administrasjon og undervisning, og som forskningsdata innenfor en lang rekke viktige forskningsområder. Data og opplysninger som behandles innenfor de ulike virksomhetsområdene (forskning, undervisning, administrasjon og formidling) spenner fra det trivielle til det svært sensitive.

I tillegg forvalter institusjonene store verdier når det gjelder tekniske løsninger (applikasjoner, systemer, datanettverk, osv.). Noen av disse løsningene eies og driftes av institusjonene selv, men stadig flere leveres av eksterne aktører i og utenfor sektoren.

Variasjonsbredden og omfanget av informasjonsverdier er, naturlig nok, fortsatt størst hos de tradisjonelle breddeuniversitetene. Men strukturendringene i sektoren har ført til at også mange høgskoler forvaltet store, sammensatte og uoversiktlige informasjonsverdier, spesielt innenfor forskningsområdet, inkludert studentforskning.

Trusler

Informasjonsverdienes omfang, kvalitet og betydning for sektoren selv og resten av samfunnet, gjør at universiteter og høgskoler kan være attraktive mål for trussel-aktører (enkeltpersoner, kriminelle grupper, nasjonalstater, osv.). Slike aktører kan påføre informasjonsverdiene betydelig skade. Samtidig kan feil håndtering av data, opplysninger og tekniske løsninger eller rene uhell medføre skade.

Denne rapporten gir likevel ikke grunnlag for å hevde at sektoren er mer utsatt for skadehendelser (forårsaket av trussel-aktører eller egne feil/uhell) enn hva som synes å være vanlig ellers i samfunnet. Bildet som avtegnet seg likner derfor i stor grad på det som virker å gjelde i resten av samfunnet[43]: Mange sikkerhetshendelser eller avvik (og trolig mange flere enn hva institusjonene selv hadde oversikt over), men relativt få av dem kan betegnes som alvorlige. Dette er i tråd med hva som virker å være situasjonen også internasjonalt (se kapittel 2).

[43] Slik som rapportert av blant annet Nasjonal sikkerhetsmyndighet og Politiets sikkerhetstjeneste. Se også Datatilsynets årsmelding for 2018 (https://www.datatilsynet.no/globalassets/global/om-oss/aarsmelding/arsmeldingen2018.pdf, «Mørketallsundersøkelsen» gjennomført av Næringslivets sikkerhetsråd (https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf) og undersøkelse gjennomført av Direktoratet for forvaltning og IKT om arbeidet med informasjonssikkerhet i statsforvaltningen (rapport 2018: 4, https://www.difi.no/rapport/2018/06/arbeidet-med-informasjonssikkerhet-i-statsforvaltningen).

Sårbarheter

Statlige universiteter og høgskoler rapporterte at de i noen grad hadde styrket arbeidet med informasjonssikkerhet og personvern de siste par årene. Dette kom blant annet til uttrykk gjennom at det var utarbeidet ledelsessystemer for informasjonssikkerhet, toppledelsen og styrene var mer involvert i arbeidet enn tidligere, GDPR-prosjekter var iverksatt, personvernombud var ansatt, innleid eller utpekt, og IT-avdelingene gjorde en viktig jobb (særlig med hensyn til informasjonssikkerhet).

Dette indikerer at det var gjort mye godt arbeid av relativt få personer, men ressursrammene var likevel noe knappe sett i forhold til arbeidets omfang og kompleksitet. Få institusjoner rapporterte at de hadde konkrete planer om, eller var i ferd med, å utvide ressursrammene (nyansettelser eller interne omdisponeringer). Hos enkelte institusjoner ble det rapportert at ressursinnsatsen kunne bli redusert når GDPR-prosjektene ble avsluttet, men at det da var meningen at mer arbeid skulle utføres i linjen.

Ressursinnsatsen fremsto som noe fragmentert. Samtidig var den konsentrert om administrasjonen på sentralt nivå i organisasjonene. På fakultetsnivå eller i fagavdelinger ble arbeidet beskrevet som variabelt eller at statusen var ukjent. Det samme gjaldt innenfor viktige deler av forsknings- og undervisningsvirksomheten.

Flertallet av institusjonene rapporterte at vedtatte ledelsessystemer for informasjonssikkerhet ikke var tilfredsstillende innført og praktisert i organisasjonene. I tillegg ble det reist spørsmål ved kompetansen til medarbeidere som skulle utføre viktige oppgaver innenfor rammen av ledelsessystemene (typisk system- eller tjenesteeiere): Ville de i mangel av tilstrekkelig opplæring være i stand til å gjennomføre oppgavene godt nok?

Risiko for manglende måloppnåelse

Dette innebærer, slik Unit vurderer det, en relativt høy risiko for at dagens sektormål på informasjonssikkerhets- og personvernområdet, slik de er definert i «Digitaliseringsstrategi for universitets- og høyskolesektoren, 2017-2021», ikke vil nås, eller vil nås bare delvis.

Av digitaliseringsstrategien fremgår følgende hovedmålsettinger for sektorens arbeid med informasjonssikkerhet og personvern:

1. Helhetlig styring og ledelse av arbeidet med informasjonssikkerhet og personvern som fundament for digitalisering og strategiske satsninger.
2. Systematisk arbeid for styrket informasjonssikkerhet og personvern basert på nasjonale føringer, for eksempel rettslige krav og krav i tildelingsbrev til institusjonene.
3. Bevisstgjøring av studenter og forskere med hensyn til datasikkerhet og riktig håndtering av data.
4. Et nivå på oppnådd informasjonssikkerhet og personvern som ligger høyere enn de nasjonale minstekravene.

Det fremstår som mest realistisk at målsetting 3 – bevisstgjøring av studenter og forskere – kan nås. Dette skyldes at mange institusjoner har jobbet med bevisstgjøringstiltak i flere år allerede (særlig med basis i informasjons- og kampanjemateriell fra Norsk senter for informasjonssikring).

Når det gjelder sektormål 1, 2 og 4, vurderes risikoen for mangelfull måloppnåelse (i løpet av strategiperioden) å være større enn hva gjelder målsetting 3. Med hensyn til sektormål 4 – informasjonssikkerheten og personvernet i sektoren skal være bedre ivaretatt enn hva som følger av de nasjonale minstekravene – er det, etter Unit sin vurdering, størst risiko for mangelfull måloppnåelse.

Begrunnelsen for disse konklusjonene er kombinasjonen av følgende forhold:

- Sektoren forvalter store, sammensatte og uoversiktlige informasjonsverdier. Informasjonsverdiene er av vesentlig betydning for samfunnet, institusjonene selv og den som opplysningene gjelder (studenter, ansatte, forskningsdeltakere, osv.). Mange av verdiene er av sensitiv og til dels svært sensitiv karakter.

- Forskning og høyere utdanning er ikke, så langt Unit kan vurdere, mindre utsatt for sikkerhetshendelser og avvik enn hva som synes å være tilfelle i samfunnet ellers.

- Det er en ubalanse i forholdet mellom risikoreduserende initiativ og sårbarhetene i sektorens arbeid med informasjonssikkerhet og personvern: viktige initiativ er gjennomført, men de har ikke fullt ut kompensert for sårbarhetene.

Enkelte anbefalinger

Nedenfor følger enkelte anbefalinger til tiltak på institusjonsnivå og på nasjonalt nivå. Anbefalingene har som siktemål å redusere risikoen i sektoren for manglende måloppnåelse.

Institusjonsnivået

Statlige universiteter og høgskoler anbefales å iverksette følgende tiltak:

- Arbeidet med informasjonssikkerhet og personvern bør prioriteres høyere enn i dag. Dette innebærer styrket personalinnsats, bedre samordning av ressursinnsatsen og økt fokus på kompetanseheving. Det er behov for kompetanseheving innenfor alle virksomhetsområder, men med særlig fokus på forskning og undervisning, inkludert studentforskning. Den øverste ledelsen skal vise lederskap og forpliktelse i arbeidet med informasjonssikkerhet og personvern ved å sørge for at det tilgjengeliggjøres tilstrekkelig med ressurser og kompetanse.

- Det iverksettes tiltak for innføring og praktisering av institusjonenes ledelsessystemer for informasjonssikkerhet. Det legges særlig vekt på at system- eller tjenesteeiere tilbys opplæring og arbeidsverktøy som gjør det mulig for dem å utføre pålagte oppgaver.

- Oversikter over institusjonenes informasjonsverdier, inkludert digitale systemer og tjenester, ferdigstilles og vedlikeholdes.

- Det utarbeides planer for rask gjenoppretting av kritiske systemer og tjenester i etterkant av alvorlige sikkerhetshendelser. Institusjonene øver regelmessig på gjenoppretting av normal drift.

Det nasjonale nivået

På nasjonalt nivå anbefales det at følgende tiltak iverksettes:

- Det bør utarbeides tydelige og målbare sektormål for informasjonssikkerhet og personvern. Målene innarbeides i Units «Handlingsplan for digitalisering i høyere utdanning og forskning». I handlingsplanen bør det legges særlig vekt på de tiltakspunktene som er nevnt ovenfor (institusjonsnivået).

- Det bør etableres en konsulent- og rådgivingstjeneste i sektoren innenfor rammen av «Program for styrket informasjonssikkerhet i UH-sektoren».[44] Tjenesten må ha kapasitet til å bistå med innføring av ledelsessystemer, opplæring i praktisk informasjonssikkerhets- og personvernarbeid, risikovurderinger og sikkerhetsrevisjoner, og utredning av juridiske problemstillinger.

- Ved utvikling eller anskaffelser av fellestjenester bør det legges det vekt på at krav til informasjonssikkerhet og personvern blir tilfredsstillende ivaretatt på system- eller tjenestenivå (innebygd informasjonssikkerhet og personvern). Alternativet er at disse kostnadene overføres til og må bæres av hver enkelt institusjon.

[44] Se tildelingsbrevet til Unit, kapittel 3.2 (https://www.unit.no/sites/default/files/media/filer/2019/01/Tildelingsbrev%202019%20Unit.pdf).

- I den nasjonale styringen bør det fokuseres på å følge opp sektorens ressursinnsats og på institusjonenes arbeid med informasjonssikkerhet og personvern i forskning og undervisning, inkludert studentforskning.

Sertifiseringer og atferdsnormer

Institusjoner i forskning og høyere utdanning har i liten grad sertifisert seg på informasjonssikkerhet eller personvern. Unit kjenner bare til at Helseundersøkelsen i Nord-Trøndelag og IT-avdelingen ved Universitetet i Stavanger har sertifisert seg på informasjonssikkerhet (ISO/IEC 27001). Spørsmål om sertifisering bør fortsatt vurderes og besvares lokalt. Unit ser ikke at det per i dag er behov for nasjonale anbefalinger eller andre tiltak med hensyn til sertifisering.[45]

Personvernlovgivningen (GDPR) åpner for bruk av atferdsnormer for behandling av personopplysninger på bransje- eller sektornivå. Datatilsynet skal godkjenne slike normer.[46] Det anbefales ikke at det utarbeides en atferdsnorm for informasjonssikkerhet og personvern i forskning og høyere utdanning. Dette vil imidlertid kreve et organisatorisk apparat (sekretariat) som det per i dag ikke finnes ressurser til. Det vil også kreve mye av institusjonene i sektoren i form av involvering og ressursbruk.

[45] Effekten av sertifiseringer på informasjonssikkerhetsområdet (om de bidrar til substansielt bedre sikkerhet eller ikke) har lenge vært et omdiskutert spørsmål. Se for eksempel Steven J. Murdoch, Mike Bond og Ross Anderson (2012): How Certification Systems Fail: Lessons from the Ware Report. Computer Laboratory, University of Cambridge.

[46] Unit er kjent med at «Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten», hvor sekretariatet ligger til Direktoratet for e-helse, har søkt Datatilsynet om å bli godkjent som atferdsnorm. Se https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet.

Vedlegg: 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. Kartleggingsmøtene ble gjennomført i perioden 29. januar til 3. april 2019.

Forberedelse og kontakt

Institusjonene mottok et brev fra Unit, datert 17. januar 2019. I brevet ble det opplyst om at Unit ville gjennomføre besøk hos hver enkelt institusjon for å kartlegge statusen i arbeidet med informasjonssikkerhet og personvern (GDPR).

Et kartleggingsskjema med 24 spørsmål var vedlagt brevet fra Unit.[47]

Deltakelse og deltakere

Institusjonenes deltakelse på kartleggingsmøtene varierte noe – fra tre til åtte ledere og medarbeidere. Deltakerne var primært sikkerhets- og beredskapsledere, informasjonssikkerhetsledere eller -rådgivere, rådgivere i forskningsadministrasjonen og personvernombud.

Unit stilte vanligvis med tre deltakere, men på enkelte møter med to.

Gjennomføring og datainnsamling

Det var satt av to timer til besvarelse av spørsmålene i kartleggingsskjemaet. Ved enkelte institusjoner tok gjennomgangen noe lengre tid enn berammet.

Det ble dels avholdt fysiske møter hos institusjonene. 10 av møtene ble avholdt som videokonferanser.

Fra to institusjoner mottok Unit skriftlige besvarelser i forkant av møtene. De skriftlige besvarelsene fra disse institusjonene ble gjennomgått under møtene. Ved de øvrige 19 universitetene og høgskolene ble svarene på spørsmålene i kartleggingsskjemaet gitt muntlig i møtet. Svarene ble notert av deltakerne fra Unit.

Etterarbeid og tilbakemeldinger

I etterkant av møtene utarbeidet Unit et kartleggingsreferat som oppsummerte institusjonenes svar på spørsmålene i skjemaet. Referatene ble sendt til institusjonene for kommentarer og kvalitetssikring.[48]

Etter at Unit hadde mottatt kommentarer og innspill fra institusjonene, ble svarene fra institusjonene vurdert i Units enhet for styring av informasjonssikkerhet og personvern. Deretter utformet Unit en kortfattet tilbakemelding til den enkelte institusjon. Her ble det gitt

[47] Spørsmålene i skjemaet dreier seg om følgende forhold: ressursinnsats/-prioritering, informasjonsverdier, systematikken i arbeidet, sikkerhetshendelser og avvik, sårbarheter og utfordringer, trusler mot informasjonsverdiene, kontinuitets- og beredskapsplaner, øvelser, oversikt over personopplysninger, melding og håndtering av hendelser/avvik, informasjons- og bevisstgjøringsarbeid, regelkompetanse og statusen på etterlevelse av GDPR.

[48] Dette ble ikke gjort for de to institusjonene som leverte skriftlige besvarelser.

anbefalinger om hva institusjonene bør legge vekt på i det videre arbeidet med informasjonssikkerhet og personvern.

Andre datakilder

Informasjon fra andre kilder enn kartleggingsmøtene inngår i datagrunnlaget for rapporten. Dette gjelder statistikk om IT-sikkerhetshendelser i forskningsnettet fra Uninett CERT; risiko- eller trusselvurderinger eller sikkerhetskartlegginger fra nasjonale myndigheter; risiko- eller trusselvurderinger fra internasjonale aktører og forskningslitteratur innenfor relevante fagområder.

Enkelte begrensninger

Rapporten bygger primært på hva Unit ble fortalt i løpet av kartleggingsmøtene. Utsagn og påstander fra institusjonenes side ble ikke forsøkt verifisert, for eksempel ved å be om tilgang til skriftlig dokumentasjon.

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

Sikkerhets- og personverntiltak som institusjonene hadde iverksatt ble ikke kontrollert. Rapporten gir derfor ikke innsikt i om iverksatte tiltak er hensiktsmessige og om de virker som forutsatt. Tekniske sårbarheter ble heller ikke kartlagt. Fokuset var isteden helheten og systematikken i institusjonenes arbeid med informasjonssikkerhet og personvern.

www.unit.no
Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning