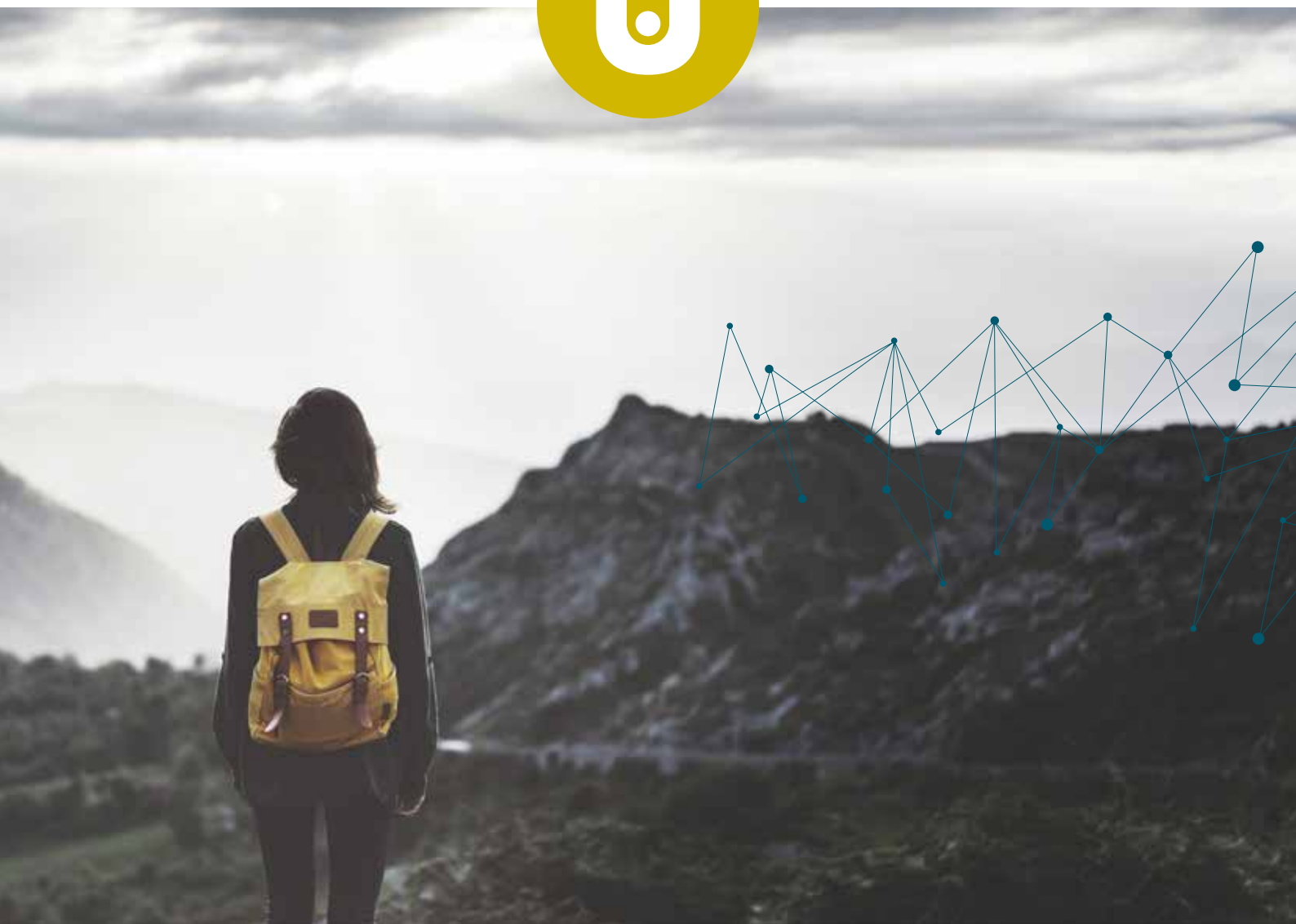
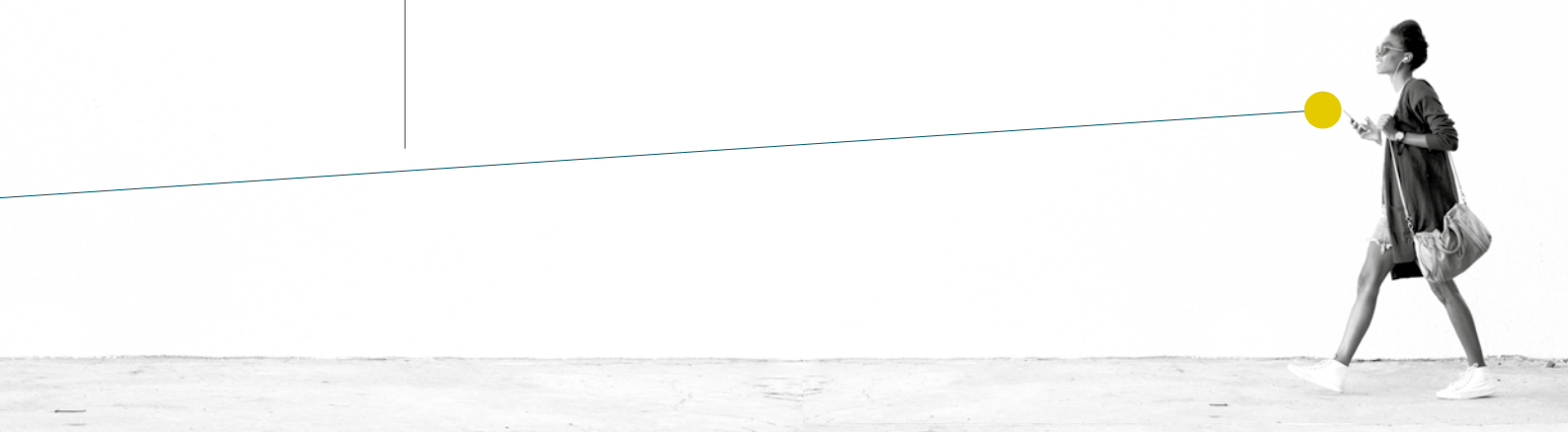
INFORMASJONSSIKKERHET OG PERSONVERN I HØYERE UTDANNING OG FORSKNING

Risiko- og tilstandsvurdering 2021



INNHOLD



SAMMENDRAG

Årets risiko- og tilstandsrapport presenterer trusselbildet i UH-sektoren og status for arbeidet med informasjonssikkerhet og personvern hos de 30 universitetene, høgskolene, direktoratene og selskapene som er direkte underlagt Kunnskapsdepartementet.

Kravene til arbeidet med informasjonssikkerhet og personvern fremgår av «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». Policyen oppsummerer rettslige krav til informasjonssikkerhet og personvern. Formålet med den er tilfredsstillende sikring av digitale verdier og forsvarlig håndtering av personopplysninger i innovative og åpne lærings- og forskningsmiljøer hvor internasjonalt samarbeid er viktig.

Policyen er fastsatt av Kunnskapsdepartementet i rundskriv F-04-20 og gjelder fra 1. oktober 2020.

Etterlevelse av kravene i policyen er avgjørende for at sektormålene på informasjonssikkerhets- og personvernområdet skal kunne oppnås. Disse målene er definert i «Digitaliseringsstrategi for universitets- og høgskolesektoren, 2017-2021».

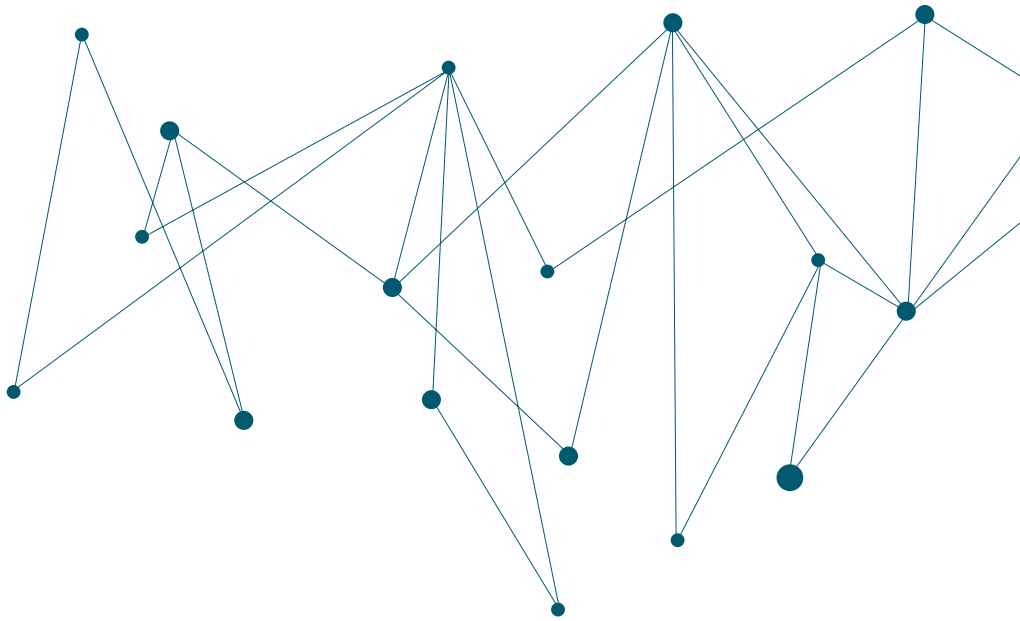
UTFORDRENDE TRUSSELBILDE

Årets risiko- og tilstandsrapport indikerer at risikoen for informasjonssikkerhetsbrudd og personvernkrenkelser er noe større enn i 2019. Det skyldes at trusselbildet i sektoren er mer utfordrende enn tidligere:

- Det generelle trusselbildet er skjerpet. Flere norske virksomheter i ulike sektorer og bransjer har vært utsatt for alvorlige digitale sikkerhetshendelser i 2020.
- Dobling i det totale antallet rapporterte hendelser og avvik hos direktoratene og selskapene sammenliknet med 2018-19. Hos universitetene og høgskolene har antallet hendelser og avvik hold seg forholdsvis stabilt.
- Noen flere virksomheter i UH-sektoren har vært utsatt for alvorlige eller potensielt alvorlige digitale sikkerhetshendelser i 2020.
- Noen flere tilfeller av datainntrengning hvor det mistenkes at statlige eller statsstøttede hackergrupper står bak.
- Oppdagelsestiden – antall dager fra første indikasjon på kompromittering til hendelsen oppdages og håndteres – er i enkelte tilfeller noe lengre enn hva vi har sett tidligere.
- Reparasjonstiden – antall dager fra hendelsen oppdages til problemet er løst – er i enkelte tilfeller noe lengre enn hva vi har sett tidligere.
- Noen flere tilfeller av at sårbarheter i digitale løsninger utnyttes av trusselaktører, eller hvor slike sårbarheter medfører økt risiko for hendelser.
- Dobling i antallet hendelser og avvik som universitetene og høgskolene meldte til Datatilsynet sammenliknet med 2019.
- Nasjonale sikkerhetsmyndigheter understreker at norsk forskning fortsatt er mål for ulike typer etterretningsvirksomhet.

Virksomhetene opplyste om at digitale verdier (data, maskin- og programvare, datanettverk, osv.) er blitt viktigere for deres evne til å utføre sine kjerneoppgaver. Det indikerer at konsekvensene av hendelser og avvik som påvirker disse verdiene på en negativ måte kan bli større enn tidligere.

Det ser ikke ut til at korona-situasjonen, med mer digital undervisning og fjernarbeid, har ført til en vesentlig økning i antallet uønskede informasjonssikkerhets- og personvernhendelser.



STYRKET ETTERLEVELSE

Skjerpingen av trusselbildet skjer samtidig med at sektorens evne til å etterleve kravene i departementets policy for informasjonssikkerhet og personvern er styrket. Styrkingen er ikke like stor som i 2019. Det kan skyldes at arbeidet med etterlevelse har blitt noe nedprioritert til fordel for gjennomføring av korona-tiltak, primært hos de mindre virksomhetene. Men systematikken og helheten i arbeidet har også i 2020 blitt bedre i deler av sektoren.

Virksomhetene har i 2020 gjennomført en rekke tekniske, organisatoriske og pedagogiske tiltak som bidrar til at sårbarheter og mangler gradvis utbedres.

Vår vurdering er likevel at det er svært lite sannsynlig at samtlige 30 virksomheter vil kunne overholde kravene i departementets policy for informasjonssikkerhet og personvern i løpet av 2021. Denne konklusjonen må imidlertid nyanseres noe:

- Vi mener at 12 av 30 virksomheter allerede ivaretar policyens krav eller er i posisjon til å gjøre det ved utgangen av 2021. Vi forventer ikke at alle som er i posisjon til det, vil lykkes med å overholde kravene på en tilfredsstillende måte i 2021.

- For 18 av 30 virksomheter mener vi at tilfredsstillende overholdelse av kravene i policyen i løpet av 2021 er lite eller svært lite sannsynlig. Flere av disse virksomhetene har likevel vist god fremgang i 2020.

MÅLOPPNÅELSE

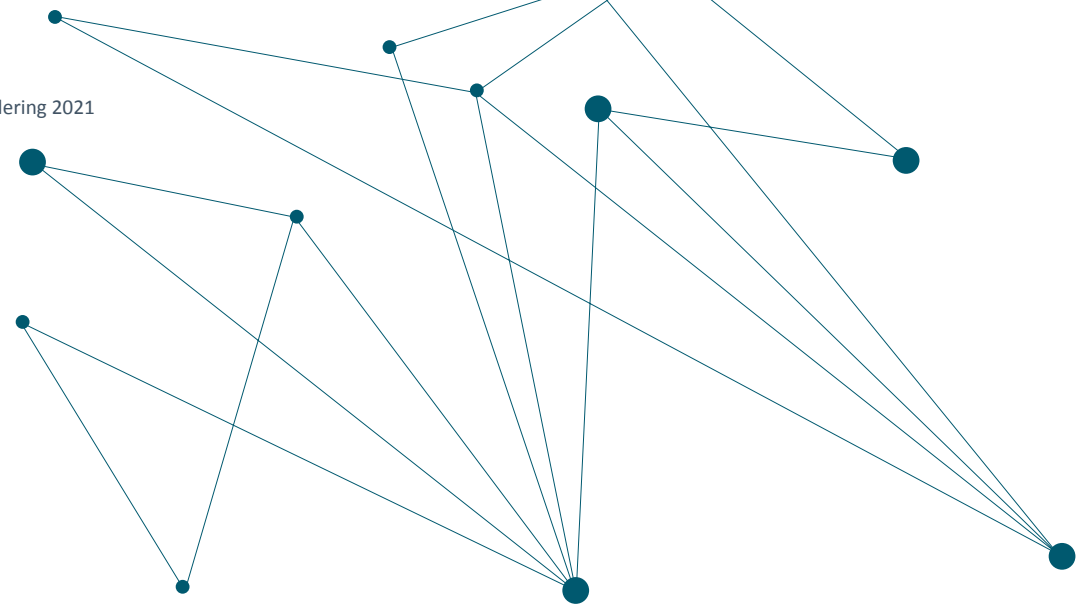
På tross av styrket evne til etterlevelse av kravene i departementets policy, mener vi at sektoren som helhet ikke vil oppnå tre av de fire hovedmålsettingene for arbeidet med informasjonssikkerhet og personvern i sektorens digitaliseringsstrategi. Sektoren nærmer seg og arbeidet er styrket, hensiktsmessige sikringstiltak er iverksatt og bevisstheten om personvern er forbedret, men tiden frem til strategiperiodens slutt blir for knapp.

Slik vi ser det, vil følgende målsettinger ikke bli realisert: (i) virksomhetene skal etablere helhetlig styring og ledelse av arbeidet med informasjonssikkerhet og personvern, (ii) virksomhetenes arbeid med styrking av informasjons-sikkerheten og personvernet skal være systematisk, (iii) nivået på arbeidet med informasjonssikkerhet og personvern skal ligge høyere enn de nasjonale minstekravene (blant annet rettslige krav).

Den fjerde målsettingen – studenter og ansatte skal bevisstgjøres problemstillinger knyttet til informasjons-sikkerhet og personvern – vil kunne realiseres.

RISIKO OG TRUSSELAKTØRER

Et mer utfordrende trusselbilde og fortsatt mangler med hensyn til etterlevelse og måloppnåelse, gjør at risikoen for uønskede hendelser og avvik trolig er noe større i 2021 enn i 2020.



Vi mener at dette særlig gjelder følgende forhold:

- Høy risiko for hendelser som skyldes skadevare, spesielt løsepengevirus.
- Høy risiko for hendelser som skyldes kompromitterte administrator- eller brukerkontoer.
- Middels risiko for hendelser som følge av direktør- eller fakturasvindel.
- Middels risiko for hendelser som følge av feil håndtering av digitale tjenester, dokumenter eller opplysninger.
- Lav risiko for større tjenestenektangrep.

Vi mener at trusselen som statlige eller statsstøttede grupper utgjør er ujevnt fordelt i sektoren (APT-hendelser). For enkelte virksomheter, for eksempel der det utføres forskning innen høyteknologi eller sensitive politikkområder, kan risikoen for APT-hendelser være høy. Enkelte hendelser i sektoren i 2020 indikerer dette. For øvrige deler av sektoren vurderes risikoen som lav.

Nettfiske i kombinasjon med manglende brukerkompetanse er fortsatt den viktigste årsaken til hendelser som medfører brudd på informasjonssikkerheten og krenkelser av personvernet.

OPPFØLGING OG ANBEFALINGER

«Cybersikkerhetssenteret for forskning og utdanning» ble lansert 25. mars i år, og er et samarbeid mellom Uninett, NTNU, UiO og NSD. Senteret vil, slik det er planlagt, være et viktig virkemiddel for å styrke arbeidet med informasjons-sikkerhet og personvern i UH-sektoren.

Resultatene fra årets kartlegging innebærer, slik vi ser det, at senteret i første omgang bør utvikle/videreutvikle følgende tilbud til sektoren:

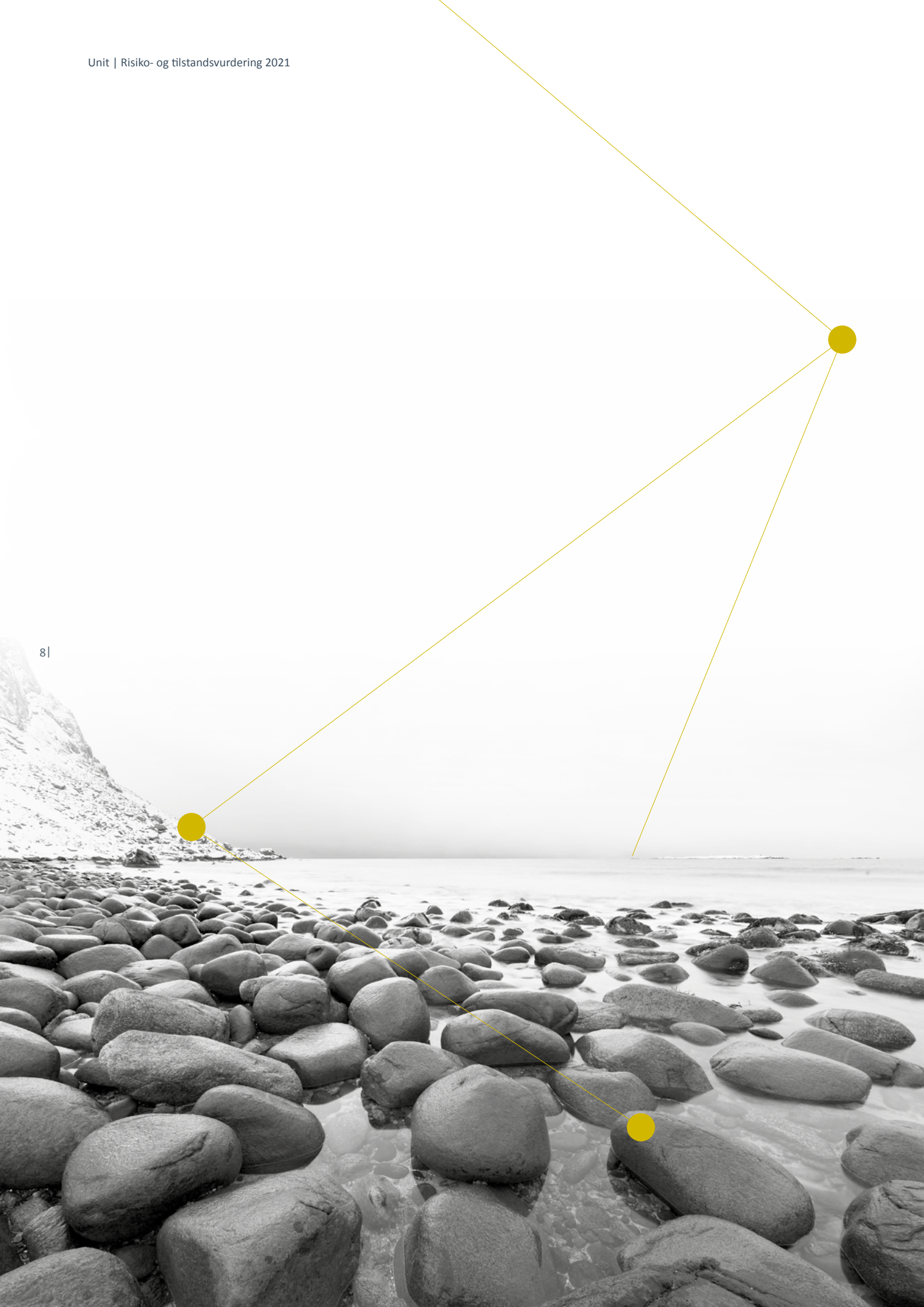
- Etablere et tilbud om sikkerhetsrevisjoner. Et slikt tilbud er avgjørende for å kvalitetssikre arbeidet med informasjonssikkerhet. Tilbudet bør på sikt inkludere testing av sikringstiltak.
- Styrke tilbudet om kompetanseheving for lokale hendelseshåndteringsteam (IRT). Det er viktig at lokale team tilføres nødvendig og oppdatert kompetanse innenfor et fagområde i rask utvikling og hvor truslene er komplekse.
- Bistå virksomhetene med etablering og revisjon av beredskaps- og kontinuitetsplaner. Dette er og har vært en gjennomgående mangel i deler av sektoren. Tilstanden har i begrenset grad forbedret seg siden 2018.

Videre mener vi at senteret bør ha fokus på opplæring og kompetanseheving, spesielt rettet mot ledere og medarbeidere som er ment å ivareta viktige oppgaver i det lokale arbeidet med informasjonssikkerhet og personvern.

Vi ser det også som viktig at cybersikkerhetssenteret bidrar til at hele sektoren får ta del i erfaringer fra håndtering av alvorlige sikkerhetshendelser. Det kan skje på ulike arenaer og møteplasser, for eksempel i sektorens CISO-forum og Forum for personvernombud. Erfaringene bør også benyttes til revisjon av sektorens rammeverk for håndtering av alvorlige IKT-sikkerhetshendelser.

Unit vil også i år utarbeide brev til den enkelte virksomhet med anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern.

Departementet vil i tillegg følge opp funnene denne rapporten i styringsdialogen med virksomhetene.



INNLEDNING

Denne rapporten oppsummerer hovedfunnene i Unit sin kartlegging av arbeidet med informasjonssikkerhet og personvern i høyere utdanning og forskning.

Kartleggingen omhandler sektorens arbeid innenfor disse områdene i 2020.[1] Rapporten inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i UH-sektoren.[2]

Formålet med rapporten er tredelt.

For det første å gi en oversikt over 2020-tilstanden på informasjonssikkerhets- og personvernområdet hos de 30 universiteter, høgskoler, direktorater og selskaper som omfattes av departementets styringsmodell.

For det andre å vurdere

- sannsynligheten for at sektoren vil etterleve kravene i departementets policy for informasjonssikkerhet og personvern i løpet av 2021,[3]
- om sektormålene for informasjonssikkerhet og personvern i gjeldende digitaliseringsstrategi kan oppnås, og
- overordnet vurdering av risiko i sektoren og risiko for konkrete informasjonssikkerhetshetshendelser og personvernkrenkelser.

For det tredje å gi anbefalinger om tiltak som bør iverksettes for å

- styrke virksomhetenes evne til å etterleve kravene i «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning» i 2021,
- forbedre virksomhetenes kapasitet til å forebygge, oppdage og håndtere informasjonssikkerhetshendelser eller personvernkrenkelser som vurderes å ha høy eller middels risiko, og
- styrke virksomhetenes evne til å gjenopprette normal driftstilstand etter alvorlige informasjonssikkerhets-hendelser eller personvernkrenkelser.

[1] Tilsvarende kartlegginger er gjennomført for 2018 og 2019.

[2] Styringsmodellen ble presentert for Kunnskapsdepartementets underliggende virksomheter i brev fra statsråden av 7. januar 2019. Beskrivelse av styringsmodellen finnes på https://www.unit.no/styringsmodell-informasjonssikkerhet-i-hoyere-utdanning-og-forskning.

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

KORT OM INFORMASJONSSIKKERHET OG PERSONVERN

Med informasjonssikkerhet menes evnen til å beskytte systemer, tjenester og digital infrastruktur slik at data eller opplysninger ikke eksponeres for uvedkommende, skades eller ødelegges, endres eller slettes på uautoriserte måter eller er utilgjengelige for rettmessige brukere.[4]

Med personvern menes i denne sammenheng regler for behandling av opplysninger om enkeltpersoner, for eksempel studenter, ansatte eller forskningsdeltakere. Reglene har til hensikt å unngå urettmessige inngrep i privat- og familieliv, hjem og korrespondanse, og krenkelser av anseelse og den personlige integriteten. Dette ivaretas ved at den som opplysningene gjelder sikres medinnflytelse over og en viss kontroll med bruken (behandlingen) av opplysningene.[5]

RISIKOVURDERING – DIGITALE VERDIER, TRUSLER OG SÅRBARHETER

Vurderingene av risiko i denne rapporten baserer seg på tradisjonell metodikk.[6] Rammeverket som ble benyttet beskrives i vedlegg 4.

Risikovurderinger handler ikke primært om å finne årsaker til det som har skjedd, men å bedre oddsen for å oppnå det man ønsker.[7] Mer konkret innebærer dette at risiko avgjøres av forholdet mellom tre faktorer – digitale verdier, trusselkilder og sårbarheter:

- **Digitale verdier:** Det som sektoren skal beskytte mot fare eller skade. Dette dreier seg om tre hovedtyper digitale verdier: (i) informasjon eller data som anvendes i forskning, undervisning, administrasjon og formidling, (ii) dataressurser (datamaskiner, programvare, tjenester, nettverksutstyr, osv.) som virksomhetene benytter til å utføre disse oppgavene, og (iii) økonomiske midler som virksomhetene forvalter.
- **Trusselkilder:** Det som kan utsette digitale verdier for fare eller skade. Dette kan for eksempel være trusselaktører (nettkriminelle grupper, statlige aktører, script kiddies, osv.) som opererer på internettet. Det kan også være studenter eller medarbeidere som ikke håndterer digitale verdier på en sikker, forsvarlig eller lovlig måte.
- **Sårbarheter:** Svakheter eller mangler som kan føre til fare eller skade. Dette kan for eksempel inkludere manglende kompetanse blant studenter eller medarbeidere i forsvarlig og lovlig håndtering av personopplysninger, mangelfull eller uklar organisering av arbeidet med informasjonssikkerhet og personvern, eller sårbarheter i maskin- eller programvare.

Det betyr for eksempel at risikoen for uønskede informasjonssikkerhetshendelser og personvernkrenkelser kan sies å være høy dersom sektorens digitale verdier utsettes for betydelige trusler, samtidig som arbeidet med informasjonssikkerhet og personvern preges av få effektive tiltak og vesentlige sårbarheter.

---

[4] ISO/IEC 27001: Information Technology Security Techniques. Information Security Management Systems – Requirements. Se også Håkon Bergsjø og Ronny Windvik (2018): Datasikkerhet for ledere. Hvordan beskytte din virksomhet. Oslo: Universitetsforlaget, eller Torgeir Daler et al. (2010): Håndbok i datasikkerhet – informasjonsteknologi og risikostyring. Trondheim: Tapir akademiske forlag.

[5] Se for eksempel Dag Wiese Schartum (2020): Personvernforordningen. En lærebok. Bergen: Fagbokforlaget; Jon Wessel-Aas og Magnus Ødegaard (2018): Personvern. Publisering og behandling av personopplysninger. Oslo: Gyldendal.

[6] ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management. Janita A. Bruvoll et al. (2020): «Funksjonsbasert risikovurdering». I Håkon Bergsjø et al. (red.): Digital sikkerhet. En innføring. Oslo: Universitetsforlaget.

[7] Sagt på en annen måte: "Risk management means taking deliberate action to shift the odds in your favor – increasing the odds of good outcomes and reducing the odds of bad outcomes" (Daniel Geer: "Measuring Security". http://geer.tinho.net/measuringsecurity.tutorial.pdf).

OM KARTLEGGINGENS BEGRENSNINGER

Vurderingene og konklusjonene i denne rapporten bygger primært på informasjon innhentet av Unit i møter med den enkelte virksomhet, se vedlegg 1. Det ble ikke bedt om tilgang til interne dokumenter som beskriver arbeidet med informasjonssikkerhet og personvern. Det er heller ikke gjennomført kontroller eller tester av tekniske, organisatoriske, pedagogiske eller fysiske tiltak for å vurdere effekten av tiltakene. Nærmere kvalitetssikring av det lokale arbeidet og iverksatte tiltak må skje gjennom sikkerhets- og etterlevelsesrevisjoner.

Hensikten med undersøkelsen har isteden vært å kartlegge (i) systematikken og helheten i arbeidet med informasjonssikkerhet og personvern, (ii) viktige oppgaver og tiltak som ble gjennomført i 2020, og (iii) viktige sårbarheter og trusler i sektoren.

Vurderinger av etterlevelse av kravene i departementets policy baserer seg på sannsynlighetsverdiene som PST anvender i sine årlige trusselvurderinger. Disse varierer mellom ytterverdiene «meget sannsynlig» (meget god grunn til å forvente tilfredsstillende etterlevelse i 2021) og «svært lite sannsynlig» (svært liten grunn til å forvente tilfredsstillende etterlevelse i 2021).[8]

METODE OG DATAGRUNNLAG

Arbeidet med rapporten (metodikk og datagrunnlag) gjøres rede for i vedlegg 1-3.

KAPITTELOVERSIKT

I kapittel 1 gis et tentativt omriss av hvilke hovedtyper digitale verdier som forvaltes i sektoren og virksomhetenes avhengighet av disse verdiene.

I kapittel 2 drøftes hvilke informasjonssikkerhets- og personvern-tiltak som de statlige universitetene og høgskolene har iverksatt i 2020. Det gis også en oversikt over sårbarheter som disse virksomhetene mente preger arbeidet med informasjonssikkerhet og personvern.

I kapittel 3 gis en oversikt over trusselkilder og uønskede hendelser som de statlige universitetene og høgskolene opplyste om i 2020.

I kapittel 4 presenteres funnene fra arbeidet med informasjonssikkerhet og personvern hos de ni direktoratene og selskapene som omfattes av styringsmodellen.

I kapittel 5 vurderes overholdelse av kravene i departementets policy, måloppnåelse og risiko for informasjonssikkerhetshendelser og personvernkrenkelser. Kapittelet inneholder også anbefalinger til tiltak på sektornivå.

VEDLEGG

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

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

Vedlegg 3:
spørsmålene (kartleggingsskjemaet) som ble benyttet i kartleggingen av direktoratene og selskapene.

Vedlegg 4:
rammeverket som ble benyttet ved vurdering av risiko for konkrete informasjonssikkerhets- og personvernhendelser.

[8] Se https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/.

KAPITTEL 1

DIGITALE VERDIER OG AVHENGIGHETER

DIGITALE VERDIER OG AVHENGIGHETER

INNLEDNING

Risiko er i stor grad en funksjon av avhengighet.[9] Jo mer avhengige virksomheter er av digitale verdier – data, programvare, datamaskiner, nettverksutstyr, sensorer, osv. – desto større er potensialet for skade dersom verdiene utsettes for uønskede hendelser (tilsiktede eller utilsiktede). Poenget er at virksomheter har begrenset risiko fra verdier eller ressurser de like gjerne kan klare seg foruten. Risikoen er desto større når det gjelder verdier som er avgjørende for å lykkes. Det betyr at dersom sårbarheter utnyttes slik at digitale verdier ødelegges, forringes, skades, manipuleres, blokkeres eller eksponeres for uvedkommende, kan dette redusere virksomhetenes evne til å utføre sine kjerneoppgaver på en effektiv, forsvarlig og tillitsvekkende måte.

Virksomhetene i UH-sektoren er i økende grad avhengig av digitale verdier for å frembringe og formidle kunnskap av høy kvalitet, og for å ivareta viktige forvaltningsoppgaver på forsvarlige måter. Og etter hvert som digitale verdier blir viktige ressurser i utdanning, forskning, formidling og forvaltning, stilles det høyere krav til virksomhetenes evne til å forhindre at uønskede hendelser får negative konsekvenser for virksomhetene selv, studenter, medarbeidere, samarbeidspartnere og deltakere i forskningsprosjekter. Omfanget av og kvaliteten på dette arbeidet må derfor styrkes i takt med at avhengigheten av digitale verdier øker – det som var godt nok i går er ikke nødvendigvis godt nok i dag eller i morgen.

I dette kapittelet antydes hvilke digitale verdier som UH-sektoren er avhengig av for å løse sitt samfunnsoppdrag. Dette «verdilandskapet» er sammensatt og uoversiktlig. Ambisjonen er derfor å gi en tentativ forståelse av hvilke digitale verdier det er snakk om. Dette vil gi et grunnlag for å vurdere om arbeidet med informasjonssikkerhet og personvern er tilpasset den risikoen som avhengigheten av digitale verdier innebærer.

HVILKE DIGITALE VERDIER?

Universitets- og høgskolesektoren kan sies å forvalte to hovedtyper digitale verdier. Disse er:

1. **Digitaliserte data og informasjon:**
   - Vitenskapelige data og faglig kunnskap, for eksempel forskningsdata/rådata, analyseresultater, vitenskapelige publikasjoner eller undervisningsmateriell. [10]
   - Personopplysninger, for eksempel opplysninger om søkere, studenter, ansatte, gjester, alumni og deltakere i forskningsprosjekter.

2. **Dataressurser:**
   - Digital infrastruktur, for eksempel datanettverk, tungregneanlegg, sensornettverk, forskningsdatabaser, laboratorieinstrumenter og audiovisuelt utstyr.
   - IT-systemer og -tjenester, for eksempel HR-systemer, studentadministrative systemer, undervisnings-plattformer og kommunikasjonsløsninger. [11]
   - Personlig IT-utstyr, for eksempel smarttelefoner eller stasjonære og bærbare datamaskiner.

I tillegg disponerer UH-sektoren andre verdier som kan medføre risiko i forbindelse med digitalisering, primært økonomiske midler. Økonomiske midler kan gjøre virksomhetene sårbare for trusselaktører, spesielt nettkriminelle grupper, som forsøker å berike seg på virksomhetenes bekostning.

DIGITALE VERDIER OG TREDJEPARTER

Digitale verdier i UH-sektoren driftes til dels av virksomhetene selv, men i økende grad av eksterne tjenesteleverandører. Dette kan være kommersielle selskaper i Norge eller i utlandet. Det kan også være statlige aktører i eller utenfor UH-sektoren, for eksempel Unit, Uninett, UiO, NSD eller DFØ.

---

[9] Se for eksempel Daniel E. Geer, Jr. (2010): «Cybersecurity and National Policy». I Harvard Law School National Security Journal, Volum 1, 7. april 2010.

[10] Dette omfatter også data som hentes fra andre sektorer, for eksempel registerdata fra nasjonale helseregistre eller medisinske kvalitetsregistre.

[11] Dette inkluderer tekniske løsninger som virksomhetene drifter selv, fellesløsninger som driftes av andre statlige aktører (for eksempel Unit, Uninett eller DFØ) og tjenester levert av kommersielle selskaper.

I 2020 oppga nær 2/3 av de statlige universitetene og høgskolene at 51 prosent eller mer av den samlede databehandlingen (i forskning, undervisning, administrasjon og formidling) nå skjer ved hjelp av eksterne tjenesteleverandører. Nesten halvparten rapporterte om at eksterne tjenesteleveranser sto for mer enn 80 prosent av den totale databehandlingen. Samtidig mente de øvrige institusjonene at bruken av tredjeparter i databehandlingen vil øke (til dels betydelig) i årene fremover.[12]

En viktig bakgrunn for flyttingen av databehandling fra egen kjeller til eksterne leverandører er at virksomhetene dermed får tilgang til dataressurser som ellers (sannsynligvis) ville vært utenfor rekkevidde (stordata, kunstig intelligens og maskinlæring er tre stikkord her[13]).

HVILKE AVHENGIGHETER?

Digitale verdier levert av virksomhetene selv eller av eksterne leverandører, understøtter viktige deler av kjerneoppgavene i UH-sektoren. Dette illustreres av omfanget av virksomhetenes system- og tjenesteportefølje: fra flere hundre systemer/tjenester hos de største universitetene til 40-50 hos enkelte av de minste høgskolene.

System- og tjenestemangfoldet innebærer at det er utfordrende for virksomhetene å skaffe seg oversikt over digitale avhengigheter. Det kan for eksempel være vanskelig å vite hvilke aktører som er involvert i tjenesteleveransene eller hvilke land som data overføres til.[14] På den annen side kan bruk av tredjeparter føre til at virksomhetene får tilgang til sikkerhets- og personvernfunksjonalitet som de ellers ikke ville hatt tilgang til.

Nedenfor gis noen eksempler på digitale avhengigheter innenfor kjerneområdene. Alle eksemplene er hentet fra virksomhetenes årsrapporter for 2020.[15]

FORMIDLING

Formidling er den kjerneoppgaven hvor virksomhetene i minst grad rapporterte om viktige digitaliseringsinitiativ. I årsrapportene legger imidlertid enkelte virksomheter vekt på viktigheten av å benytte digitale kanaler for å nå ut til store målgrupper med innhold tilpasset de ulike gruppene. Denne formen for profilering og synliggjøring skal blant annet bidra til å styrke virksomhetenes evne til å rekruttere studenter og å nå opp i konkurransen om forskningsmidler.

Videre handler digitale kanalvalg om forskningsformidling (åpen forskning), det vil si å tilgjengeliggjøre vitenskapelige publikasjoner og kunnskap for allmennheten. Norges idrettshøgskole (NIH) fremhever digitale kanaler og fagblogger som viktige virkemidler i forskningsformidlingen.[16] Slik formidling skjer også skje via nasjonale publiseringsløsninger (Nasjonalt vitenarkiv[17]).

For enkelte virksomheter er tilgjengeliggjøring av kultur- og naturhistoriske museumssamlinger en viktig del av den digitale formidlingsvirksomheten.

[12] Se «Temarapport 2020: Tjenesteutsetting av digitale systemer og tjenester» (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

[13] Se for eksempel Ben Williamson (2018): Big Data in Education. The Future of Learning, Policy and Practice. London: Sage Publications. Se også «Norwegian Artificial Intelligence Research Consortium» (https://www.nora.ai/) eller regjeringens strategi for kunstig intelligens (https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/).

[14] For diskusjon av informasjonssikkerhet ved ekstern drift, se for eksempel «Risikostyring i digitale verdikjeder. Rapport fra arbeidsgruppe ledet av Olav Lysne». Direktoratet for samfunnssikkerhet og beredskap (https://www.dsb.no/rapporter-og-evalueringer/risikostyring-i-digitale-verdikjeder/).

[15] Fremstillingen i resten av kapitlet baserer seg også på referater og saksdokumenter fra møtene i sektorens fagutvalg: fagutvalget for infrastruktur, mellomvare og data; fagutvalget for utdanning; fagutvalget for forskning; fagutvalg/tjenesteråd for administrative tjenester. Se https://www.unit.no/fagutvalgene.

[16] NIH årsrapport 2020, side 16.

[17] Se https://www.unit.no/aktuelt/enklere-tilgang-til-forskningsresultater-med-nasjonalt-vitenarkiv.

UTDANNING

På utdanningssiden vektlegger virksomhetene betydningen av at læringsmiljøene digitaliseres. Digitale læringsmiljøer skal for eksempel understøtte studentmobilitet, livslang læring, etter- og videreutdanning, hybrid undervisning og studentaktive læringsformer. I dette inngår også lagring og deling av læringsobjekter og undervisningsmateriell. Det fysiske læringsmiljøet skal tilpasses de nye krav som digitale læringsmiljøer stiller. Dette skal blant annet bidra til å øke læringsutbytte og styrke utdanningenes arbeidslivsrelevans.

I tillegg skal lagring og gjenbruk av data om læringsprosesser legge til rette for økt bruk av læringsanalyse.

Digital eksamen er i ferd med å erstatte tradisjonelle eksamensformer. I sine årsrapporter for 2020 oppgir for eksempel Universitetet i Sørøst-Norge (USN) at 1030 av ca. 1800 skoleeksamener ble gjennomført digitalt i 2019,[18] mens Høgskolen på Vestlandet (HVL) rapporterte om at ved enkelte fakulteter skjer 80 prosent av vurderingene digitalt.[19] Ved Høgskolen i Molde (HiMolde) leveres nesten 80 prosent av alle hjemmeeksamener digitalt,[20] og ved NTNU er mer enn 50 prosent av skriftlige eksamener digitalisert. Samtidig er store deler av eksamensprosessen ved NTNU digitalisert og automatisert, for eksempel inngåelse av masteravtale, oppgaveinnlevering, karakterføring og klage/begrunnelse.[21]

Norges miljø- og biovitenskapelige universitet (NMBU) viser til at de har digitalisert vitnemålsprosessen.[22] I tillegg er emneplanlegging og -evaluering i ferd med å bli digitalisert ved mange universiteter og høgskoler. Det samme gjelder håndtering av søknader om utvekslingsopphold, og samhandlingen mellom studie- og praksissted.

Universitetene og høgskolene har også iverksatt initiativ for å styrke tilbudet av nettbasert undervisning, inkludert bruk av MOOC.

ADMINISTRASJON

Også i den administrative virksomheten er avhengigheten av digitale verdier betydelig. Slike digitale verdier inkluderer sektortjenester som leveres av Unit eller som forvaltes av Unit på vegne av sektoren. Det gjelder for eksempel FS, Samordna opptak, biblioteksystemer, datavarehus, Nasjonal vitnemålsdatabase og en rekke andre løsninger. I tillegg leverer eller forvalter Unit sentrale løsninger innenfor andre kjerneområder, blant annet digital eksamen.[23]

På virksomhetsnivå fremheves også avhengigheten av digital administrasjon. Universitet i Oslo (UiO) legger i sin årsrapport vekt på betydningen av robotisering av administrative arbeidsprosesser, blant annet bruk av chatbot og nettskjema.[24] UiO nevner spesielt kvalitetssikring av regnskapsføringen som et område hvor automatisering har hatt betydning. Automatiseringen innebærer at kontroller kan benyttes tidligere i regnskapsprosessen enn tidligere, det vil si før transaksjoner blir bokført, og kan rettes inn mot særskilte risikoområder.[25] Også HVL nevner den økende betydningen av automatisering og robotisering av administrative oppgaver, særlig ved bruk av digitale skjema.[26] Det samme gjelder ved Høgskolen i Østfold (HiØ).[27]

NTNU opplyser i sin årsrapport om at 10 administrative prosesser, som i 2019 behandlet omkring 230 000 saker, er automatisert. Denne automatiseringen hadde frigjort ca. 240 ukesverk. Det har, ifølge NTNU, ført til en rekke andre gevinster: raskere saksbehandling, reduserte utgifter til vikarer, bedre tid til unntakshåndtering, mer kapasitet til nedprioriterte oppgaver og økt tilfredshet blant økonomimedarbeiderne.[28] Videre opplyser USN om at automatisert dokumentfangst og integrasjon av digitale skjemaløsninger har medført besparelser på 1000-1500 timer i året.[29]

I tillegg inneholder årsmeldingene en rekke andre eksempler på digitalisering og automatisering av administrative prosesser. Det gjelder for eksempel digital støtte til gjennomføring av rekrutteringsprosesser, blant annet med hensyn til vitenskapelige ansatte,[30] og for mottak av nye ansatte.[31] En av virksomhetene opplyste at digitalisering av rekrutteringsprosessen har ført til at den i snitt skjer 1,5 måneder raskere enn tidligere.[32]

Universitetet i Agder (UiA) rapporterer om at 110 administrative tjenester og prosesser har blitt digitalisert siden 2016.[33] Universitetet i Stavanger (UiS) har digitalisert studentekspedisjonen og etablert oppdrags-, bestillings- og samhandlingsportal.[34]

[18] USN årsrapport 2020, side 30.

[19] HVL årsrapport 2020, side 17.

[20] HiMolde årsrapport 2020, side 14.

[21] NTNU årsrapport 2020, side 42.

[22] NMBU årsrapport 2020, side 24.

[23] Se https://www.unit.no/tjenester.

[24] UiO årsrapport 2020, side 48.

[25] UiO årsrapport 2020, side 50.

[26] HVL årsrapport 2020, side 36-37.

[27] HiØ årsrapport 2020, side 112-114.

[28] NTNU årsrapport 2020, side 43.

[29] USN årsrapport 2020, side 28.

[30] NTNU årsrapport 2020, side 43.

[31] NMBU årsrapport 2020, side 24.

[32] NTNU årsrapport 2020, side 43.

[33] UiA årsrapport 2020, side 27.

[34] UiS årsrapport 2020, side 16.

Mange virksomheter har i tillegg etablert nye datavarehusløsninger. Dette har gjort styringsdata og nøkkeltall lettere tilgjengelig for ledere og bidratt til å styrke kvaliteten i styrings- og planleggingsarbeidet.

Universitetene i Bergen, Oslo, Trondheim og Tromsø (BOTT) er i ferd med å ta i bruk nye digitale løsninger for saksbehandling og arkiv, lønn og økonomi.[35]

FORSKNING

Avhengigheten av digitale verdier i forskningsprosesser – datainnsamling, analyse og publisering/formidling – er betydelig innenfor mange viktige forskningsfelt. Det gjelder for eksempel innenfor områder som data science, bioteknologi, nanoteknologi, klimaforskning og maritim forskning. Avhengigheten kommer blant annet til uttrykk gjennom at stadig flere virksomheter har etablert egne digitale forskningsinfrastrukturer, spesielt for behandling av sensitive data (ofte personopplysninger) i mindre forskningsprosjekter. I 2020 hadde både USN og NIH etablert egne «forskningssegmenter» i sine datanettverk for behandling av sensitive forskningsdata.

Andre virksomheter har etablert tilsvarende infrastrukturer. Dette gjelder for eksempel NTNU og Universitetet i Tromsø (UiT). NTNUs digitale forskningsinfrastruktur for sensitive data («NICE») tilbyr ulike typer tjenester – fra enkel fillagring til avanserte infrastruktur for klinisk forskning.[36] UiT på sin side jobber med videreutvikling av sin digitale infrastruktur, og ønsker å etablere en skyplattform for forskningstjenester. [37]

I tillegg til virksomhetenes egne digitale forskningsinfrastrukturer og tjenester, er digitale infrastrukturtjenester levert av tredjeparter avgjørende.[38] Særlig viktige i denne sammenheng er Uninett AS: forskningsnettet og ulike tjenester på toppen av forskningsnettet.[39] I tillegg tilbyr Uninett sitt datterselskap – Sigma2 – dataressurser for norsk forskning i form av systemer for tungregning og for lagring og deling av data.[40]

Av andre digitale verdier i forskning kan nevnes tjenester som leveres og driftes av UiO, spesielt «Tjenester for sensitive data» (TSD).[41] I kartleggingene som Unit har gjennomført i sektoren i 2018-2020 rapporteres det at stadig flere virksomheter benytter TSD, og at tjenesten er viktig for å gjøre forsvarlig forskning på særlige kategorier personopplysninger mulig.

Arkivering og publisering av forskningsdata for gjenbruk i senere forskningsprosjekter representerer en annen viktig del av forskningsinfrastrukturen i UH-sektoren (åpne data). Løsninger for dette tilbys av flere aktører, blant annet NSD. NSD tilbyr også bistand til forskningsprosjekter og virksomheter med hensyn til å ivaretakelse av personvernplikter,[42] og tjenester for analyse av registerdata (Microdata i samarbeid med SSB[43]).

ANDRE AVHENGIGHETER

Strukturendringer i UH-sektoren har medført at behovet for samhandling på tvers av lokasjoner (campus) har økt. Digitalisering er et viktig virkemiddel for å styrke denne samhandlingen. Høgskolen i Innlandet (HINN) fremhever for eksempel at «(...) en vellykket studiestedsutvikling er avhengig av digitalisering».[44] Det samme sier Nord universitet og HVL.[45] USN har etablert et eget digitaliseringsprosjekt («USN digital») hvor tettere sammenknytning av åtte lokasjoner er en viktig målsetting.[46]

I tillegg vektlegger flere virksomheter at digitalisering gir viktige bidrag til oppfølging av ABE-reformen. I denne sammenheng fremheves digitalisering som et virkemiddel for å styrke virksomhetenes økonomiske handlingsrom.

Korona-nedstengningen har medført at digitale kommunikasjons- og samhandlingstjenester har blitt viktigere for den daglige driften i sektoren. Det innebærer større avhengighet av tredjepartsleverandører, for eksempel Zoom, for at virksomhetene skal kunne videreføre sine kjerneoppgaver når det ikke er mulig å besøke campus eller kontorlokaler.

[35] Se for eksempel UiB årsrapport 2020, side 46.

[36] NTNU årsrapport 2020, side 43.

[37] UiT årsrapport 2020, side 30.

[38] Se for eksempel Norges forskningsråd: Norsk veikart for forskningsinfrastruktur (https://www.forskningsradet.no/siteassets/programmer/veikart/norskveikartforforskningsinfrastruktur2018-del1omradestrategier.pdf).

[39] Se https://www.uninett.no/tjenester.

[40] Se https://www.sigma2.no/om-sigma2.

[41] Se https://www.uio.no/tjenester/it/forskning/sensitiv/.

[42] Se https://www.nsd.no/personverntjenester/meldingsarkivet-for-ledelse-og-administrasjon/.

[43] Se https://microdata.no/.

[44] HINN årsrapport 2020, side 30.

[45] Nord universitet årsrapport 2020, side 24; HVL årsrapport 2020, side 36-37.

[46] USN årsrapport 2020, side 26-27.

EKSTERNE INTERESSENTER – SÆRSKILT OM FORSKNING

Avhengigheten av digitale verdier i forskning er ikke bare avgjørende for virksomhetenes evne til å fremstille kunnskap og tilby undervisning av høy kvalitet. Det er også andre aktører enn virksomhetene selv som har interesser i at denne avhengigheten forvaltes på en sikker og forsvarlig måte.

For det første er digitale verdier i forskning viktig for nasjonale forskningsmyndigheter. Dette kommer for eksempel til uttrykk gjennom forskningspolitiske prioriteringer. Slike prioriteringer antyder hvilke forskningsområder, og dermed også hvilke digitale verdier, som vurderes som særskilt betydningsfulle. Prioriteringene beskrives blant annet i «Langtidsplan for forskning og høyere utdanning 2019-2029».[47]

For det andre har lovgiver angitt hvilke digitale verdier som vurderes å være av spesiell betydning. Lovgiver har for eksempel bestemt at personopplysninger, blant annet om studenter, ansatte og deltakere i forskningsprosjekter, har særlig verdi for den enkelte og for samfunnet. Det samme gjelder opplysninger undergitt taushetsplikt eller data om enkeltpersoner som benyttes i medisinsk og helsefaglig forskning.

For det tredje kan digitale verdier være av betydning for Norges evne til å ivareta nasjonale interesser og internasjonale forpliktelser. Eksempler på dette er kunnskap eller teknologi som kan ha militære anvendelsesområder eller som har flerbrukspotensial (kan benyttes til både sivile og militære formål). Dette kan være tilfelle innenfor forskningsfelt som nano-, undervanns- og romteknologi, bioteknologi, kunstig intelligens (maskinlæring) og kryptologi. Innen slike felt kan enkelte forskningsresultater (kunnskap og teknologi) også være underlagt eksportkontrollrestriksjoner.[48]

For det fjerde kan forskningsresultater være av særskilt betydning fordi resultatene brukes som grunnlag for politikkutforming og forvaltning på viktige samfunnsområder. Eksempler er vær- og klimaforskning, maritim forskning, geologisk- og helseforskning.[49]

Til slutt kan det finnes aktører i privat sektor (samarbeidspartnere/industriaktører) som har interesse av forvaltningen av digitale verdier i UH-sektoren. Slike aktører kan selv bidra til forskningsvirksomheten, blant annet med finansiering.[50]

NY DIGITALISERINGSSTRATEGI

Forslaget til ny digitaliseringsstrategi for UH-sektoren[51] skisserer hvordan viktigheten og avhengigheten av digitale verdier kan komme til å utvikle seg de nærmeste årene.[52] Her fremheves det at digitaliseringen skal føre til dyptgripende (transformerende) endringer i undervisning, læring, forskning og administrasjon. Viktige målsettinger er å styrke kunnskapsutviklingen, innovasjonsevnen og verdiskapingen i sektoren.

Dette skal oppnås gjennom en rekke initiativ:

- utvikle tilbudet av fellestjenester som understøtter kjerneoppgavene;
- standardisering og harmonisering av data;
- datakilder og metadata som grunnlag for etablering av sammenhengende tjenester og helhetlig digitalisering;
- legge til rette for åpen forskning gjennom bedre tilgang til forskningsdata og avanserte analyseverktøy;
- etablering av nasjonale stordatasamlinger som skal muliggjøre bruk av stordataanalyse og kunstig intelligens;
- økt gjenbruk og deling av administrative data;
- produksjon og deling av læringsressurser.

[47] Her er satsningsområdene (i) hav, (ii) klima, miljø, miljøvennlig energi, (iii) fornyelse i offentlig sektor og bedre offentlige tjenester, (iv) muliggjørende og industrielle teknologier og (v) samfunnssikkerhet og samhørighet i en globalisert verden. Se https://www.regjeringen.no/no/dokumenter/meld.-st.-4-20182019/id2614131/.

[48] Se for eksempel https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/. Se også forslag til veileder utarbeidet av Råd for samfunnssikkerhet og beredskap i kunnskapssektoren: «Forebygging av ulovlig kunnskapsoverføring – en nasjonal veileder».

[49] Norge har noen av de lengste hydrologiske, oseanografiske og meteorologiske tidsseriene i verden. Tilsvarende tidsserier finnes innenfor andre fagområder. Eksempler fra helseområdet inkluderer Helseundersøkelsen i Nord-Trøndelag og Tromsøundersøkelsen.

[50] Universitetene og høgskolene nevnte flere eksempler på slike samarbeidspartnere/industriaktører, for eksempel Equinor, Huawei, Kongsberggruppen, Rolls Royce, Swiss Timing og Ulstein-gruppen.

[51] «Innovativ utdanning og fremragende forskning. Digitaliseringsstrategi for universitets- og høyskolesektoren (2021-2025)» (https://www.unit.no/aktuelt/ambisiost-utkast-til-ny-digitaliseringsstrategi-levert-til-kunnskapsdepartementet).

[52] Omkring halvparten av universitetene og høgskolene hadde egne digitaliseringsstrategier i 2020. Slike strategier er mindre vanlig hos direktoratene og selskapene. Lokale prioriteringer og satsninger på digitaliseringsområdet speiler i stor grad satsningene i den nasjonale strategien.

I tillegg skal fremtidig digitalisering legge til rette for livslang læring. Det skal blant annet skje gjennom utvikling av personaliserte studenttjenester og nye identitets- og tilgangsløsninger (gi studentene livslang tilgang til sine læringsressurser).

SEKTORKRITISK INFRASTRUKTUR

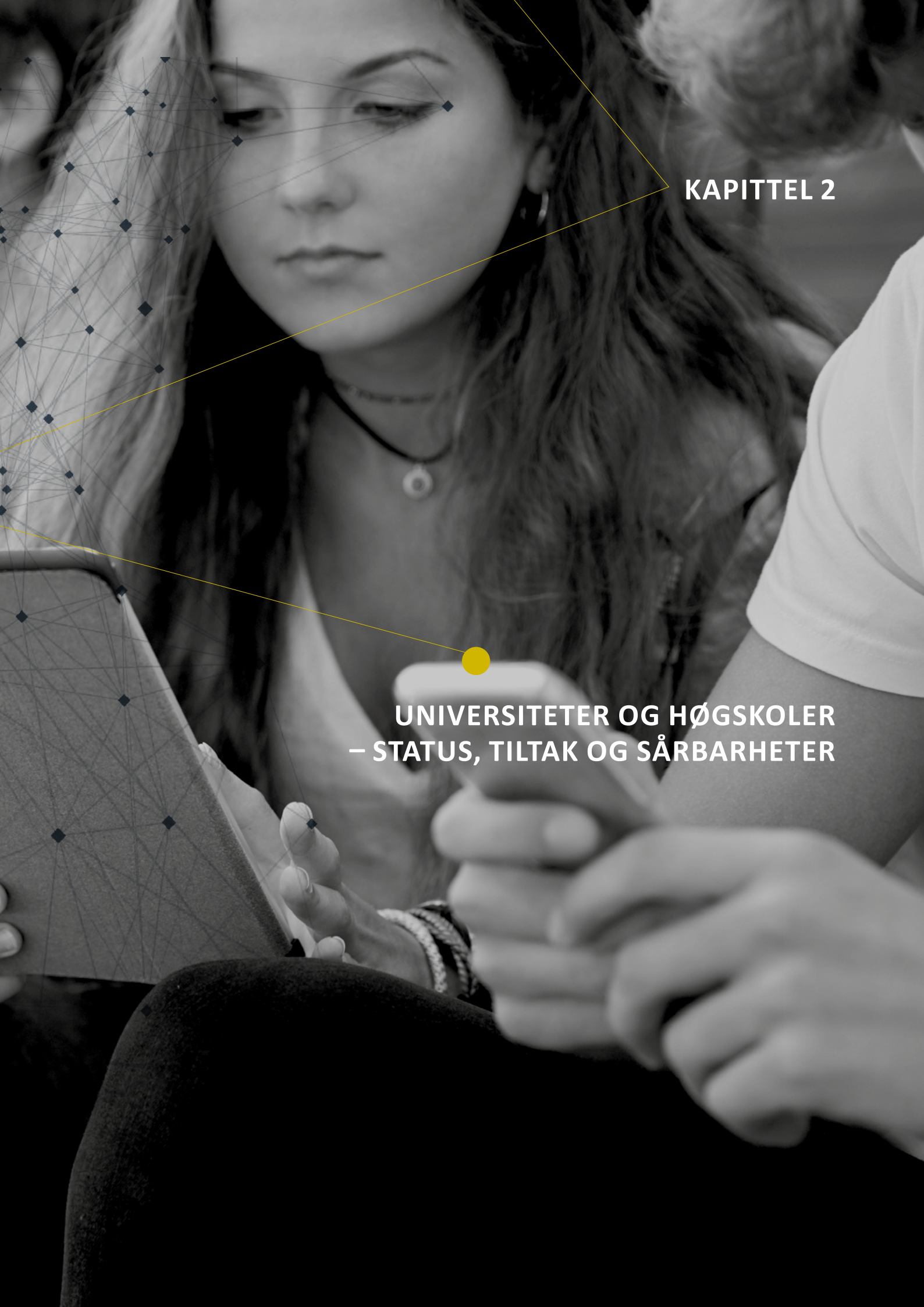
Fremstillingen ovenfor gir et ufullstendig og fragmentert øyeblikksbilde av digitaliseringen i sektoren. Hensikten har vært å illustrere at opptaket av digitale løsninger innenfor alle kjerneområder er såpass stort at det nå dreier seg om sektorkritisk infrastruktur – noe sektoren vanskelig kan klare seg foruten. Og økende kritikalitet betyr at det blir vanskeligere å akseptere risikoen for at digitaliseringen feiler på tilsiktede eller utilsiktede måter. Poenget er at feiltoleransen – digitale verdier ødelegges, skades, manipuleres, blokkeres eller eksponeres for uvedkommende – reduseres etter hvert som avhengigheten øker.

Dette kommer til uttrykk i forslaget til ny digitaliseringsstrategi. Her understrekes det at informasjonssikkerhet og personvern er «(…) grunnlaget for en ansvarlig digitalisering i UH-sektoren.»[53] Ansvarlig digitalisering innebærer at arbeidet med informasjonssikkerhet og personvern i sektoren settes i system, og at det iverksettes målrettede tiltak som styrker digitaliseringens gevinstpotensial og reduserer risikoen for problematiske omkostninger.

NESTE KAPITTEL

Systematiseringen av arbeidet og iverksatte tiltak i 2020 drøftes i neste kapittel.

[53] «Innovativ utdanning og fremragende forskning. Digitaliseringsstrategi for universitets- og høyskolesektoren (2021-2025)», side 19 (https://www.unit.no/aktuelt/ambisiost-utkast-til-ny-digitaliseringsstrategi-levert-til-kunnskapsdepartementet).



KAPITTEL 2

UNIVERSITETER OG HØGSKOLER – STATUS, TILTAK OG SÅRBARHETER

UNIVERSITETER OG HØGSKOLER – STATUS, TILTAK OG SÅRBARHETER

INNLEDNING

Økende avhengighet av digitale verdier betyr at sektoren må ha oversikt over sårbarheter som kan føre til at verdiene ødelegges, skades, forringes, manipuleres, blokkeres eller eksponeres for uvedkommende. Deretter må det iverksettes tiltak for å utbedre de viktigste sårbarhetene. Sektoren må derfor jobbe systematisk og helhetlig med informasjonssikkerhet og personvern.

I dette kapitlet behandles tre hovedspørsmål:

1) Hva var status for arbeidet med informasjonssikkerhet og personvern hos de 21 statlige universitetene og høgskolene i 2020 – hvor systematisk og helhetlig var dette arbeidet?

2) Hvilke viktige informasjonssikkerhets- og personverntiltak hadde universitetene og høgskolene iverksatt i 2020?

3) Hvilke sårbarheter mente universitetene og høgskolene at de fortsatt hadde behov for å utbedre?

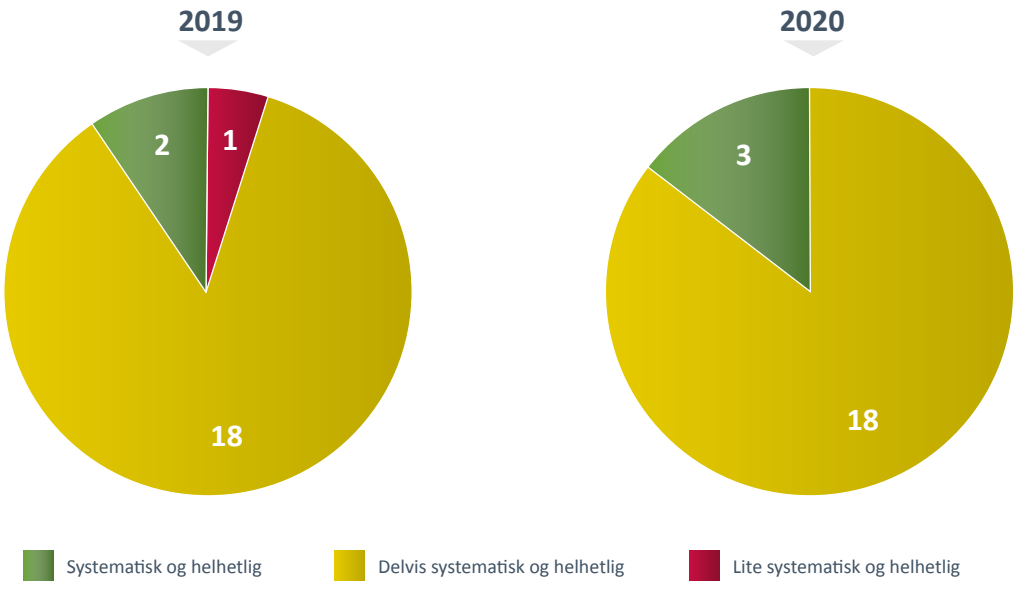
STATUS FOR ARBEIDET MED INFORMASJONSSIKKERHET OG PERSONVERN

Figurene 1-4 nedenfor oppsummerer statusen for arbeidet med informasjonssikkerhet og personvern hos de statlige universitetene og høgskolene i 2019 og 2020.

INFORMASJONSSIKKERHET

Figur 1 viser at tre virksomheter opplyste om at det var etablert et systematisk og helhetlig arbeid med informasjonssikkerhet. Disse virksomhetene har fortsatt en del avvik som må lukkes og mangler som må utbedres. Vår vurdering er likevel at informasjonssikkerhetsarbeidet omfatter alle deler av kjernevirksomheten og at det er tydelig forankret hos og prioritert av toppledelsen og styret.

Figur 1: Status for arbeidet med informasjonssikkerhet, 2019 og 2020



Figur 1 viser endringer i status på informasjonssikkerhetsområdet fra 2019 til 2020. Den viktigste endringen er at det ikke lenger er virksomheter som i liten grad jobber systematisk og helhetlig med informasjonssikkerhet.

OM STATUSVURDERINGENE

Statusvurderingene av arbeidet med informasjonsikkerhet er basert på følgende momenter: (i) tiltak for å avdekke og forebygge trusler mot sikkerheten til digitale verdier (risikostyring), (ii) tiltak for å håndtere eventuelle sikkerhetsbrudd som likevel oppstår (hendelseshåndtering) og (iii) tiltak for å gjenopprette normal drift etter større sikkerhetsbrudd (beredskap/kontinuitet). Det legges særlig vekt på hvor langt arbeidet med innføring av ledelsessystemer for informasjonssikkerhet er kommet og i hvilken grad toppledelsen stiller krav til og følger opp arbeidet.[54]

Statusvurderingene av arbeidet med personvern (GDPR) er basert på disse momentene: (i) oversikt over behandlinger av personopplysninger (protokoll), (ii) løsninger for ivaretakelse av de registrertes rettigheter og (iii) tiltak for økt bevissthet og kompetanse om personvernreglene og hvordan de kan etterleves. Det legges særlig vekt på hvor langt arbeidet med innføring av en helhetlig internkontroll for GDPR er kommet (jf. artikkel 24 i personvernforordningen).[55]

Det avgjørende er imidlertid at det er lagt et bærekraftig grunnlag for kontinuerlig forbedring av det forebyggende arbeidet, deteksjon og hendelseshåndtering og gjenoppretting.

De resterende 18 universitetene og høgskolene jobber delvis systematisk og helhetlig med informasjonssikkerhet. Det viktigste for disse virksomhetene i 2021, er å ferdigstille innføringen av ledelsessystemer for informasjonssikkerhet. Det inkluderer etablering av planverk for håndtering av alvorlige informasjonssikkerhetshendelser (beredskap/kontinuitet) og aktivering av medarbeidere med sentrale roller i det praktiske arbeidet, for eksempel system- eller tjenesteeiere. At slike medarbeidere er tilstrekkelig kjent med og har nødvendig kompetanse til å ivareta sine oppgaver og ansvar, er avgjørende for at arbeidet med informasjonssikkerhet skal kunne defineres som systematisk og helhetlig.

Risikostyringen hos de 18 siste virksomhetene er likevel styrket – de fleste av virksomhetene gjennomfører risikovurderinger periodisk og ved anskaffelse av nye IT-systemer eller digitale tjenester. Det er imidlertid utfordringer med hensyn til oppfølging av risikovurderingene. Det innebærer at sikringstiltak som vurderes som nødvendige ikke alltid blir etablert.

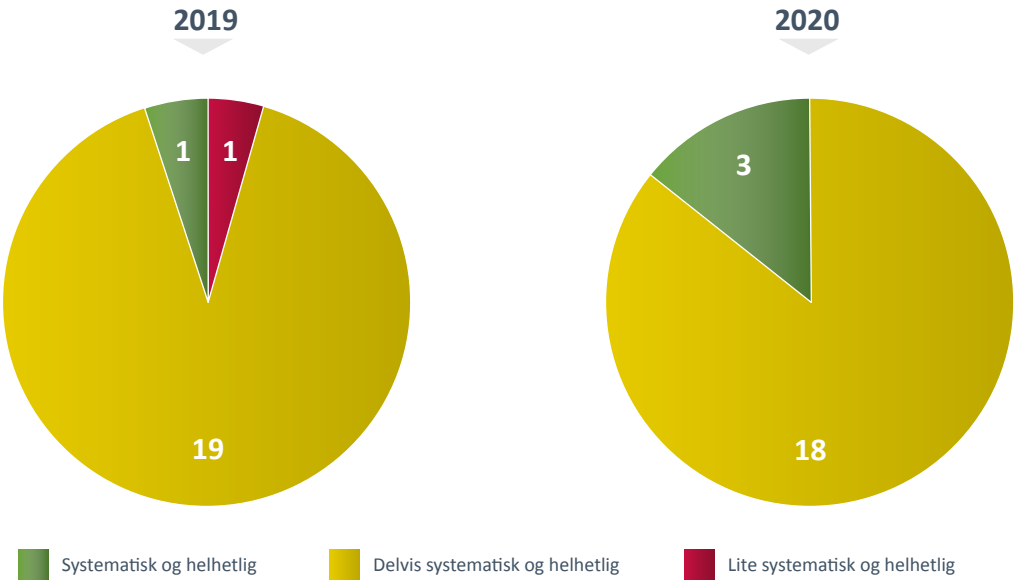
Videre er det positivt at arbeidet med informasjonssikkerhet hos de fleste av de 18 siste virksomhetene er forankret hos toppledelsen og styret. I enkelte virksomheter etterspør ledelsen mer informasjon om arbeidet og ønsker å styrke egen kompetanse med hensyn til informasjonssikkerhet. Styrene virker også å spille en mer aktiv rolle enn tidligere. Det kommer til uttrykk ved at enkelte styrer ber om at det gjennomføres revisjoner av arbeidet med informasjonssikkerhet.

Hos noen virksomheter er det behov for nærmere avklaringer knyttet til ledelsens rolle. Enkelte virksomheter er usikre på hvordan ledelsen best kan involveres i arbeidet og hvordan ledelsens gjennomgang kan gjennomføres. Det ble også reist spørsmål om hva som er den mest hensiktsmessige rollefordelingen mellom ledelsen og styret. Hos de fleste virksomhetene er rollefordelingen mellom toppledelsen og styret ordnet slik at styret orienteres om innholdet i og beslutninger fattet i ledelsens gjennomgang. I noen virksomheter behandler også styret årlige rapporter fra personvernombudet.

[54] Vurderingsmomentene er hentet fra NSMs «Grunnprinsipper for IKT-sikkerhet» (https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/).

[55] Se også Datatilsynets veiledningssider om internkontroll. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/.

Figur 2: Status for arbeidet med personvern (GDPR), 2019 og 2020



PERSONVERN (GDPR)

Figur 2 viser at status for virksomhetenes arbeid med personvern (GDPR) har endret seg noe mer fra 2019 til 2020. For det første fordi det i 2020 ikke lenger er virksomheter som i liten grad jobber systematisk og helhetlig med personvern. For det andre fordi antallet virksomheter som mener at de har lykkes med å etablere et systematisk og helhetlig personvernarbeid har økt – fra én til tre. Disse virksomhetene har fortsatt enkelte avvik og mangler som må utbedres. Men de har etablert et personvernarbeid som omfatter alle deler av kjernevirksomheten og som er tydelig forankret hos og prioritert av toppledelsen og styret. Disse virksomhetene har derfor et bærekraftig grunnlag for kontinuerlig forbedring av etterlevelsen av personvernregelverket.

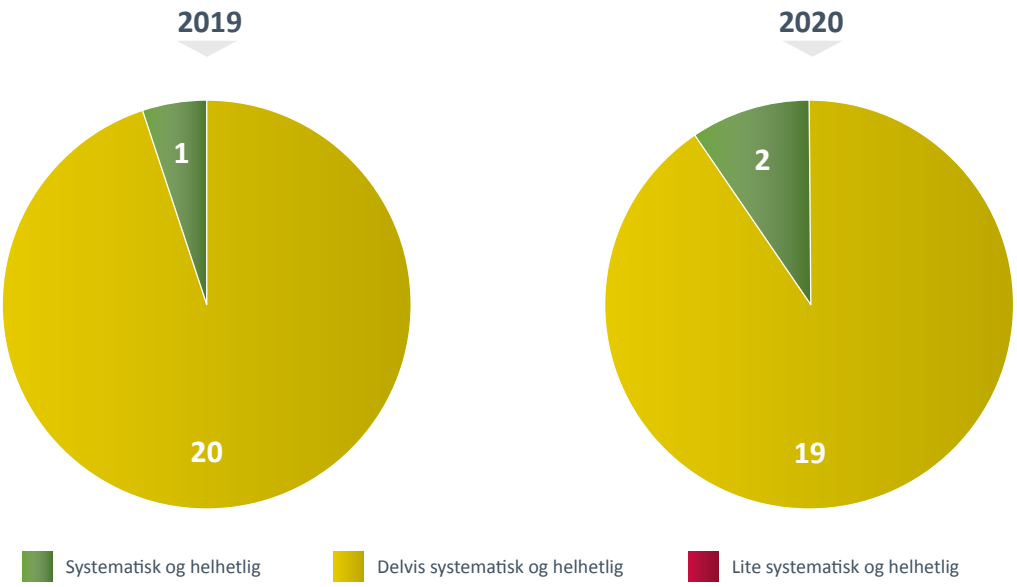
For de øvrige 18 universitetene og høgskolene ble det ikke funnet grunnlag for å endre deres 2019-status. Det betyr at disse virksomhetene jobber delvis systematisk og helhetlig med personvern (GDPR).

Den største utfordringen for disse virksomhetene er mangler knyttet til innføring av en systematisk intern-kontroll. Det ble også rapportert om utfordringer med opplæring av medarbeidere som er ment å utføre viktige oppgaver i internkontrollarbeidet. Flere virksomheter opplyste om at det i liten grad ble gjennomført slik opplæring i 2020. Andre virksomheter hadde gjennomført noe opplæring. Opplæringen var i hovedsak rettet mot vanlige brukere og besto for det meste av nanolæringskurs.

Det er imidlertid en rekke virksomheter (12) som mener at de har etablert fullstendige rutiner for ivaretakelse av de registrertes rettigheter. De øvrige virksomhetene har enten ikke etablert fullstendige rettighetsrutiner eller statusen for dette arbeidet fremstår som uklar.

Samtlige virksomheter mener at de har kommet relativt langt i arbeidet med behandlingsprotokoller (oversikt over personopplysninger). Det er likevel bare fire virksomheter som opplyser om at protokollen er fullstendig. Hos de øvrige virksomhetene gjenstår det fortsatt noe arbeid før behandlingsprotokollene deres er fullstendige.

Figur 3: Samlet status – informasjonssikkerhet og personvern, 2019 og 2020

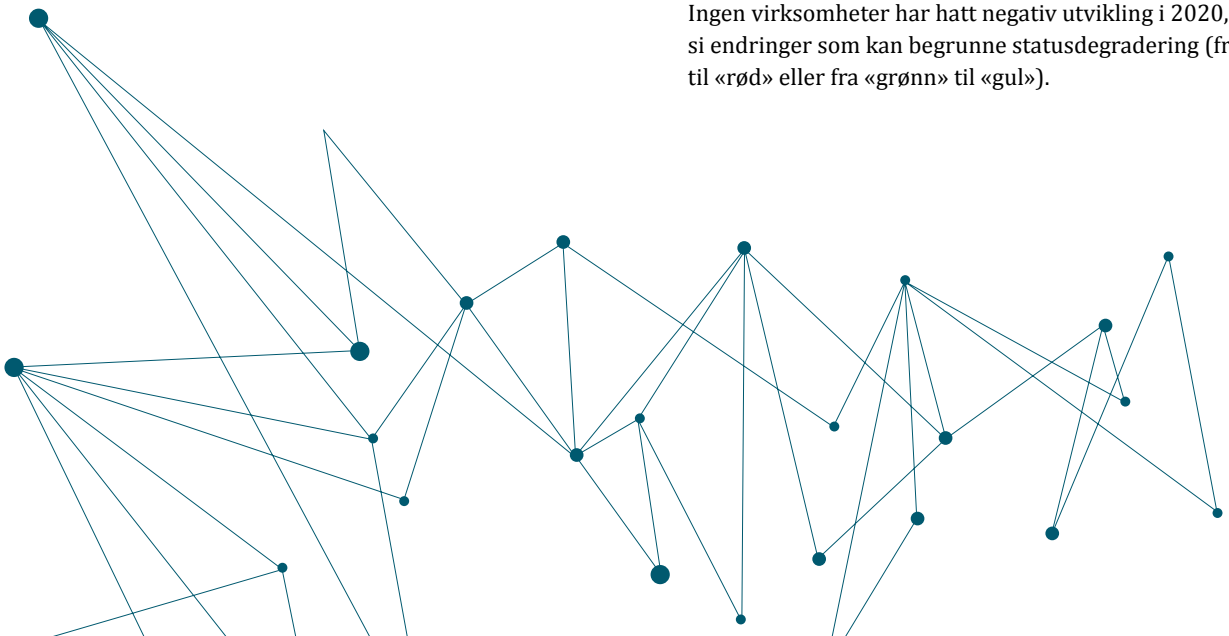


SAMLET STATUS
– INFORMASJONSSIKKERHET OG PERSONVERN
På bakgrunn av resultatene i figur 1 og 2 kan det gis en samlet vurdering for status med hensyn til informasjonssikkerhet og personvern – og hvordan statusen har endret seg sammenliknet med 2019.

Figur 3 viser at i 2020 har to virksomheter havnet i «grønn kategori» sammenliknet med én i 2019. Dette er virksomheter som har etablert et systematisk og helhetlig arbeid både med hensyn til informasjonssikkerhet og personvern, og som ivaretar kravene i departementets policy for informasjonssikkerhet og personvern på tilfredsstillende måter.

De øvrige virksomhetenes arbeid kategoriseres som delvis systematisk og helhetlig. De har derfor enkelte avvik som må lukkes og forbedringer som må gjennomføres for at kravene i departementets policy skal bli tilfredsstillende ivaretatt.

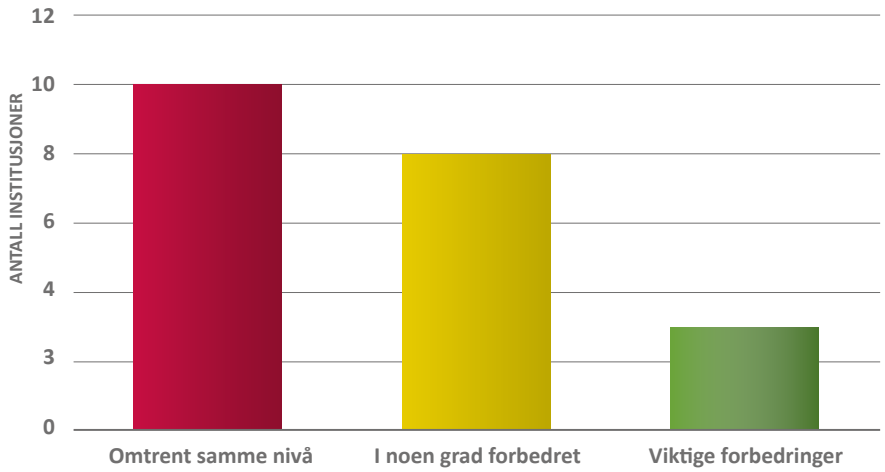
Ingen virksomheter har hatt negativ utvikling i 2020, det vil si endringer som kan begrunne statusdegradering (fra «gul» til «rød» eller fra «grønn» til «gul»).



FORBEDRINGER UTEN STATUSENDRING

Selv om virksomhetenes arbeid med informasjons-sikkerhet og personvern i 2020 ikke har medført omfattende endringer i status, har det likevel skjedd forbedringer som ikke synliggjøres i figur 3 ovenfor. Statusoversikten skjuler derfor enkelte forbedringer som det er viktig å kjenne til for å få et mer fullstendig bilde av sektorens arbeid med informasjonssikkerhet og personvern.
I figur 4 gis en oversikt over disse forbedringene.

Figur 4: Forbedringer i arbeidet med informasjonssikkerhet og personvern, 2020



Figur 4 viser at drøyt halvparten av universitetene og høgskolene (11) har forbedret sitt arbeid med informasjons-sikkerhet og personvern i 2020. De øvrige virksomhetene har ikke forbedret arbeidet vesentlig. I motsetning til under fjorårets kartlegging, opplyste ingen virksomheter om at arbeidet innen disse områdene er svekket.

Tre virksomheter har gjort viktige forbedringer i arbeidet med informasjonssikkerhet og personvern i 2020, men uten at forbedringene gir grunnlag for statusendring (grønn stolpe). Ytterligere åtte virksomheter hadde forbedret arbeidet i noen grad – arbeidet er preget av jevn og stødig fremdrift (gul stolpe). Til slutt er det 10 virksomheter som befinner seg på omtrent samme nivå som i 2019 (rød stolpe).

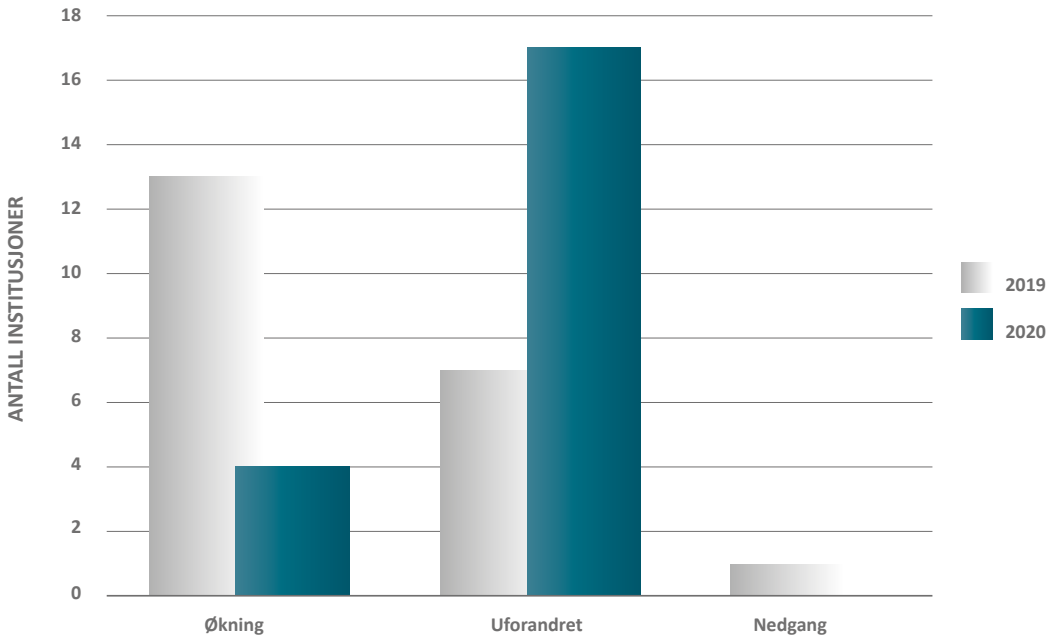
Hos de virksomhetene som ikke har gjort tydelige fremskritt i arbeidet i 2020, ble omprioritering av ressurser for å håndtere korona-situasjonen nevnt som den viktigste årsaken til dette.

PERSONALRESSURSER (ÅRSVERK)

Status for og prioritering av informasjonssikkerhet og personvern, henger sammen med ressursinnsatsen, det vil si hvor mange årsverk som er øremerket (helt eller delvis) til dette arbeidet.

Figur 5 viser antallet virksomheter som rapporterte om at ressursinnsatsen (målt som antall øremerkede årsverk) har økt, er uforandret eller er redusert fra 2019 til 2020. Oversikten inkluderer årsverkene for personvernombudene.

Figur 5: Endringer i personalinnsatsen (årsverk), 2019 og 2020



Figuren viser at økningen i virksomhetenes ressursinnsats er mindre fra 2019 til 2020 enn hva den var fra 2018 til 2019:

- Fire virksomheter opplyste om at ressursinnsatsen har økt fra 2019 til 2020. 13 virksomheter opplyste om at samme i 2019.
- 16 virksomheter opplyste om at ressursinnsatsen ikke har endret seg fra 2019 til 2020. Sju virksomheter rapporterte om det samme i 2019.
- Ingen virksomheter rapporterte om at ressursinnsatsen er svekket fra 2019 til 2020. I fjorårets kartlegging oppga én virksomhet om at innsatsen var redusert.

Det betyr at 0,22 prosent av alle årsverk hos de statlige universitetene og høgskolene, er øremerket til arbeidet med informasjonssikkerhet og personvern i 2020.[56]

Årsverkene er i hovedsak knyttet til informasjons-sikkerhetsansvarlig/-rådgiver (CISO) og personvernombud, eller til IT-avdelingene, HR- og økonomiavdelingene, og studie- og forskningsadministrasjonen.

Årsverksanslagene inkluderte i liten grad arbeidet med informasjonssikkerhet og personvern blant vitenskapelig ansatte. Det er grunn til å tro at anslagene ville blitt noe høyere dersom denne innsatsen hadde blitt inkludert.

[56] I 2020 var det samlede årsverkstallet for statlige universiteter og høgskoler 37 806 (https://dbh.nsd.uib.no/statistikk/rapport.action?visningId=137&visKode=false&admdebug=false&columns=arstall&index=1&formel=329&hier=insttype!9!instkode!9!fakkode!9!ufakkode!9!st_kode&sti=&param=arstall%3D2020!8!2019!8!2018!8!2017!8!2016!9!dep_id%3D1).

VIKTIGE TILTAK I 2020

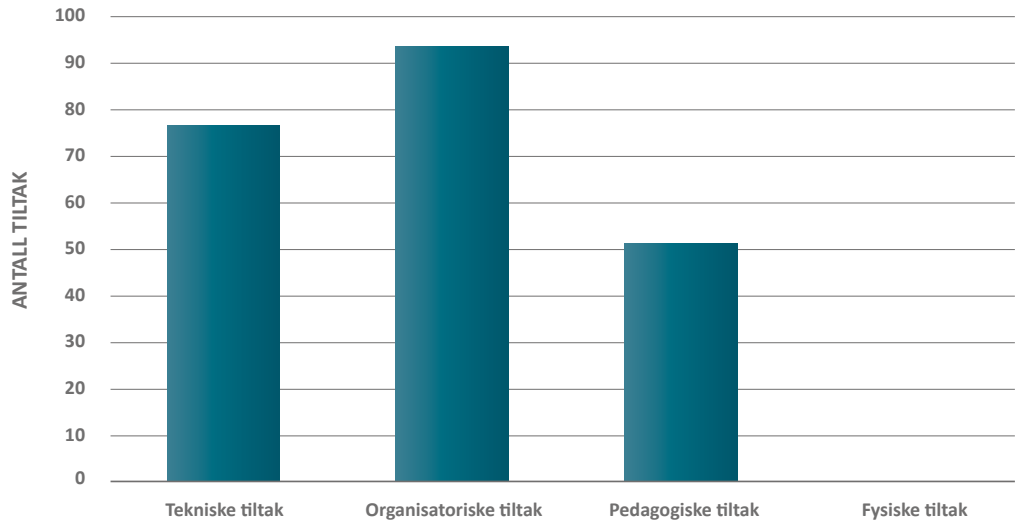
Hvilke viktige informasjonssikkerhets- og personverntiltak har universitetene og høgskolene iverksatt i 2020? Figur 6 gir en oversikt over de tiltakene som virksomhetene opplyste om.

OM TILTAKENE

Noen av tiltakene oppsummert i figuren nedenfor var konkrete sikrings- eller personverntiltak (slik som spesifisert i ISO/IEC 27001 vedlegg A eller ISO/IEC 27002). I tillegg handlet det om systemtiltak. Dette var tiltak som hadde til hensikt å etablere eller videreutvikle et systematisk og helhetlig informasjonssikkerhets- eller personvernarbeid (ledelses-systemer for informasjonssikkerhet og internkontroll for GDPR).

Det er også verdt å legge merke til at enkelte tiltak i figuren omfatter flere enkeltstående aktiviteter. Eksempler på dette er «kurs for ansatte i GDPR» eller «opplæring i risikovurderinger». Begge disse tiltakene kunne romme flere kurssamlinger eller mange enkeltkurs, men rapporteres likevel i figur 7 som kun to tiltak. Det betyr at den rapporterte tiltaksaktiviteten var noe større enn det som fremgår av figuren.

Figur 6: Hovedtyper informasjonssikkerhets- og personverntiltak, 2020



Figuren viser at universitetene og høgskolene totalt opplyste om 220 tiltak innenfor informasjonssikkerhets- og personvernområdet i 2020. Det betyr at tiltaksomfanget er omtrent på samme nivå som i 2019.

Også tiltaksprofilen – hvordan tiltakene fordeler seg mellom de ulike tiltakskategoriene (teknisk, organisatorisk, osv.) – er omtrent den samme som i 2019: flest organisatoriske tiltak (92) fulgt av tekniske tiltak (77) og pedagogiske tiltak (51).

DEFINISJONER

Organisatoriske tiltak:
Utarbeidelse, innføring eller praktisering av ledelsessystemer for informasjonssikkerhet og internkontroll for personvern (GDPR). Eksempler på dette kan være fordeling av ansvar og oppgaver, utarbeidelse av rutiner, gjennomføring av risikovurderinger, kartlegging av behandlinger eller utarbeidelse av kontinuitets- og beredskapsplaner.

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

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

Fysiske tiltak:
Planlegging eller iverksetting av tiltak for å sikre systemer og informasjonsverdier mot ulike typer miljøpåvirkning. Eksempler på dette kan være installasjon av nytt adgangskontrollsystem, kameraovervåking i resepsjonsområder eller anskaffelse av nye alarmer eller sensorer for å motvirke tyveri, brann eller fuktskader.

TILTAKSPROFILEN

Mange virksomheter rapporterte om at de har videreutviklet ledelsessystemet for informasjonssikkerhet eller internkontrollen for GDPR, eller begge deler. Tydeliggjøring av rollene i sikkerhetsorganisasjonen og revisjoner av sikkerhetsstrategier/-policyer er eksempler på dette. Anskaffelser av digitale verktøy for å styrke systematikken i arbeidet med ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR er et annet viktig tiltak som flere virksomheter har eller er i ferd med å gjennomføre.

Andre viktige organisatoriske tiltak inkluderer opprettelse av informasjonssikkerhetsforum eller nettverk av ressurspersoner på enhetsnivå (personvernkontakter). 15 virksomheter oppga at de har opprettet slike nettverk eller forum. Formålet med slike tiltak er å forankre arbeidet og involvere hele organisasjonen i innsatsen. Det ble også opplyst om tiltak for å styrke virksomhetenes hendelseshåndteringsteam (IRT).

Videre opplyste universitetene og høgskolene om mange enkeltstående aktiviteter som inngår i et systematisk og helhetlig informasjonssikkerhets- og personvernarbeid. Det handler typisk om utarbeidelse av rutiner for behandling av personopplysninger og retningslinjer for sikker forvaltning av informasjonsverdier, spesielt klassifisering og lagring av opplysninger. Andre slike tiltak omfatter kartlegging av IT-systemer og digitale tjenester, utarbeidelse av behandlingsprotokoller (personopplysninger), gjennomføring av risikovurderinger og gjennomgang av databehandleravtaler.

Flere virksomheter opplyste om at de har videreutviklet sine rutiner for tjenesteutsettelse (bruk av databehandlere). Disse tiltakene skjer i kjølvannet av Schrems II-dommen.[57] Formålet er å styrke kontrollen med overføring av personopplysninger til tredjeland, særlig USA.

[57] Se for eksempel https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/privacy-shield-avtalen-mellom-usa-og-eueos-er-opphevet/.

Som i 2019, ble det opplyst om to hovedtyper pedagogiske tiltak. For det første enkelte former for kompetanseheving rettet mot medarbeidere med viktige roller i informasjons-sikkerhets- eller personvernarbeidet. For det andre allmenne bevisstgjøringstiltak («folkeopplysning») rettet mot alle studenter og ansatte. Deltakelse i nasjonal sikkerhetsmåned, og bruk av de nanolæringskursene som inngår i denne årlige kampanjen, er et vanlig pedagogisk tiltak.[58]

Et pedagogisk tiltak som mange virksomheter rapporterte om i 2019, var øvelser på håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser.[59] I 2020 har mange virksomheter nedprioritert slike øvelser. Disse virksomhetene mente at det ikke var nødvendig å øve på krisehåndtering når de sto midt i en reell krise (håndtering av korona-situasjonen).

Når det gjelder tekniske sikringstiltak opplyste omkring halvparten av virksomhetene (10) at de enten hadde eller er i ferd med å innføre totrinnsinnlogging for administrativt og vitenskapelige ansatte. Enkelte virksomheter har innført (eller planlegger å innføre) totrinnsinnlogging også for studenter.

Andre viktige tekniske tiltak gjelder sky- og klientsikkerhet. Det handler blant annet om kjøp av lisenser for bruk av sikkerhetstjenester hos tjenesteleverandører, og skybasert funksjonalitet for beskyttelse av personlig IT-utstyr hos fjernpåloggede medarbeidere. I tillegg ble det opplyst om økt bruk av VPN, opprettelse av nettverkssoner for behandling av sensitive data (særlig i forskning), anskaffelser av nye brannmurløsninger og styrking av rettighetsstyringen.

Enkelte av tiltakene i 2020 ble hasteinnført på grunn av korona-situasjonen. Dette gjelder for eksempel nye rutiner for bruk av videokonferanse- og samhandlingsløsninger og for informasjonssikkerhet på hjemmekontor.

I 2019 ble det rapportert om fysiske sikringstiltak, for eksempel fysisk adgangskontroll eller oppgradering av reservestrømløsning på maskinrom. Det ble ikke opplyst om fysiske tiltak i 2020.

OM VDI I SEKTOREN

Flere virksomheter i sektoren har tatt i bruk NSM sin tjeneste for varsling av «koordinerte og alvorlige» dataangrep – VDI (Varslingssystem for digital infrastruktur).[60]

Disse virksomhetene mente at VDI har vært en nyttig investering: systemet har oppdaget og varslet om flere alvorlige sikkerhetshendelser og inntrengingsforsøk i 2020.

FORTSATT SÅRBARHETER

Tiltakene viser hvilke forbedringsområder universitetene og høgskolene har prioritert i 2020. Virksomhetene opplyste også om hva de fortsatt er bekymret for – sårbarheter som kan føre til uønskede hendelser eller avvik.

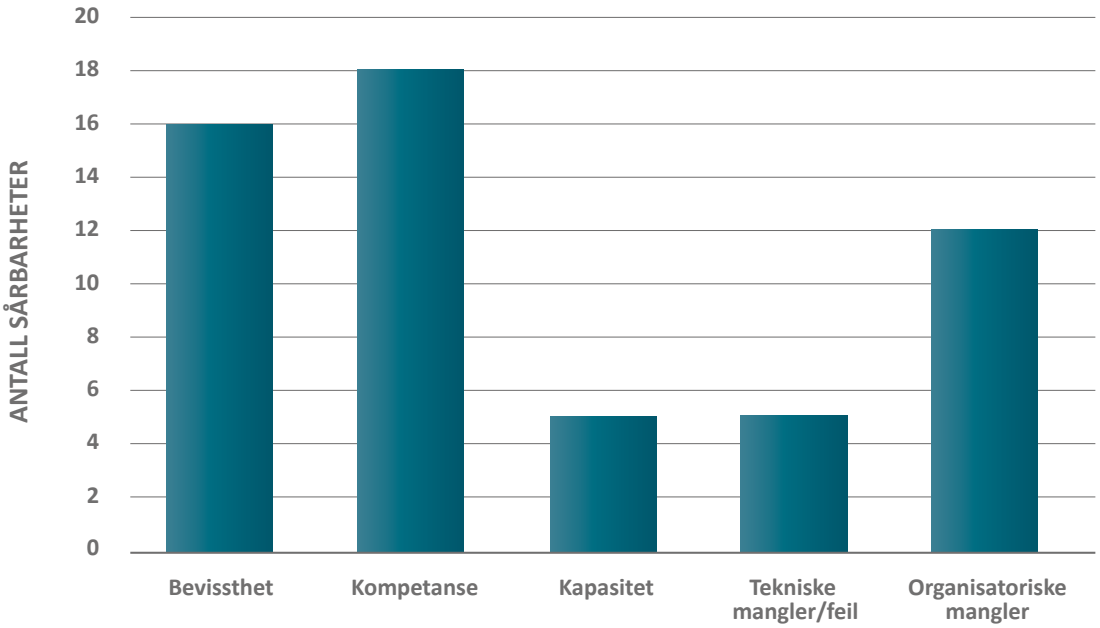
Figur 7 viser sårbarhetsprofilen for denne delen av UH-sektoren, det vil si hvor mange virksomheter som mente at deres arbeid var kjennetegnet av fem hovedtyper sårbarheter.

[58] Se https://norsis.no/nsm2020/.

[59] Se «Temarapport 2020 – kontinuitet, beredskap og øvelser» (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

[60] Se https://nsm.no/tjenester/varslingssystem-vdi/.

Figur 7: Rapporterte sårbarheter i 2020



Sårbarhetsprofilen er omtrent den samme som i 2019.[61] Det innebærer at kompetanse (om hvordan informasjonssikkerhets- og personvernarbeidet best kunne utføres) og bevissthet (om hvilke informasjonssikkerhets- og personvernutfordringer virksomhetene står overfor) ble vurdert som de viktigste utfordringene.

Organisatoriske mangler, spesielt uklar organisering av arbeidet eller manglende rutiner/retningslinjer, ble vurdert som den tredje viktigste sårbarheten. Dette er det samme som i 2019.

Manglende kapasitet (personalressurser) og tekniske sårbarheter ble nevnt av færrest virksomheter. Også dette speiler svarene fra fjorårets kartlegging.

Ut over dette har det siden 2018 vært en gjennomgående sårbarhet i denne delen av sektoren at det mangler planverk for håndtering av og videre drift ved alvorlige informasjonssikkerhets- eller personvernhendelser. Enkelte virksomheter har dette på plass, men det er fortsatt mange virksomheter som enten ikke har eller har ufullstendige planverk. Dette er ikke unikt for UH-sektoren.[62]

SÅRBARHETER OG TILTAK

De klart vanligste sårbarhetene – bevissthet og kompetanse – kan håndteres ved hjelp av pedagogiske tiltak. I figur 6 så vi imidlertid at dette var den tredje vanligste tiltakstypen. Det kan derfor stilles spørsmål ved om det var tilfredsstillende sammenheng mellom rapporterte sårbarheter og gjennomførte tiltak.

Virksomhetene mente likevel at bevisstheten og kompetansen hadde forbedret seg de siste årene. Spesielt personvernombudene oppga at bevisstheten om informasjonssikkerhet og personvern blant administrativt og vitenskapelige ansatte er økende.

Organisatoriske sårbarheter, særlig manglende rutiner/retningslinjer eller uklar fordeling av ansvar og oppgaver, ble oppgitt å være den tredje viktigste sårbarheten. Samtidig er organisatoriske tiltak den vanligste tiltakstypen i 2020, jf. figur 6. Også her kan det se ut til å være en noe mangelfull sammenheng mellom rapporterte sårbarheter og gjennomførte tiltak.

[61] Se «Risiko- og tilstandsvurdering 2020», side 19-22 (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

[62] Se rapport fra Helsetilsynet 2/2021: «Forsvarlig pasientbehandling uten IKT? Risikovurderinger, nødrutiner og forbedringsarbeid ved 17 sykehus» (https://www.helsetilsynet.no/tilsyn/tilsyn-med-ikt/).

KAPASITETSMANGLER
Kapasitetsmangel (personalressurser) ble nevnt som en sårbarhet av relativt få virksomheter. Dette til tross for den beskjedne økningen i antallet årsverk som universitetene og høgskolene har øremerket til arbeidet med informasjonssikkerhet og personvern. Samtidig rapporterte enkelte virksomheter om at personalmangel kunne gjøre det utfordrende å gjennomføre nødvendige informasjonssikkerhets- eller personverntiltak (primært organisatoriske og pedagogiske tiltak[63]). Det kan stilles spørsmål ved om den samlede kapasiteten hos universitetene og høgskolene er tilstrekkelig.

Det er flere måter å håndtere manglende kapasitet på enn ved å øke antallet øremerkede årsverk. Et alternativ er å styrke koordineringen av egen innsats, for eksempel gjennom opprettelse av informasjonssikkerhetsforum eller nettverk av ressurspersoner på enhetsnivå (personvernkontakter). Ovenfor har vi sett at dette er tiltak/ordninger som mange av universitetene og høgskolene har etablert.

Styrket koordinering av ressursinnsatsen kan også skje på tvers av virksomheter. Flere virksomheter forsøker å håndtere sine kapasitetsutfordringer gjennom samarbeid med andre virksomheter i sektoren.

TEKNISKE SÅRBARHETER
Det er få virksomheter som opplyste om at de er bekymret for tekniske sårbarheter. Dette er overraskende sett i lys av at tekniske sårbarheter og kvalitetsfeil i programvare er vanlige kilder til sikkerhetsbrudd og personvernkrenkelser. Samtidig kan det tenkes at tiltaksaktiviteten innenfor dette området gjør at virksomhetene opplever at andre typer sårbarheter er mer presserende.

Enkelte virksomheter mente likevel at det er behov for ytterligere tiltak for å styrke robustheten i eget datanettverk. Dette handler om at dersom en trusselaktør lykkes med å skaffe seg tilgang til virksomhetens datanettverk, er det få interne sikkerhetsbarrierer som kan forsinke laterale bevegelser (trusselaktøren skaffer seg tilgang til nye deler av nettverket) og hindre at kontoer med utvidede rettigheter kompromitteres. Det ble derfor etterlyst tiltak som styrker motstandsdyktigheten i det lokale datanettverket, og som gjør det mulig å oppdage og håndtere sikkerhetsbrudd før virksomheten påføres alvorlig skade.

Revisjoner av informasjonssikkerheten hos virksomheter i andre sektorer[64] antyder at motstandsdyktigheten i digital infrastruktur er en problemstilling som kan kreve ytterligere oppmerksomhet også i UH-sektoren.

NESTE KAPITTEL
I neste kapittel drøftes i hvilken grad sårbarheter førte til uønskede informasjonssikkerhets- eller personvernhendelser og -avvik i 2020.

[63] Enkelte institusjoner rapporterte om at oppfølging av tekniske sikringstiltak kan lide under personellmangel. Dette gjelder blant annet kontroll og analyse av logger.

[64] Se spesielt «Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer.» Rapportvedlegg til Dokument 3:2 (2020-2021) (https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer/).

KAPITTEL 3

UNIVERSITETER OG HØGSKOLER – UØNSKEDE HENDELSER OG AVVIK

UNIVERSITETER OG HØGSKOLER – STATUS, TILTAK OG SÅRBARHETER

INNLEDNING

Uønskede hendelser og avvik kan påvirke sektorens evne til å ivareta sitt samfunnsoppdrag og personvernet til den enkelte. Brudd på informasjonssikkerheten og personvernkrenkelser kan også avdekke viktige sårbarheter som virksomhetene bør utbedre.

OM UØNSKEDE HENDELSER OG AVVIK

Med informasjonssikkerhetehendelser menes to hovedtyper uønskede hendelser. For det første hendelser som faktisk fører til brudd på informasjons- eller personopplysningssikkerheten, det vil si uautorisert tilgang til digitale verdier eller at slike verdier skades, ødelegges, endres, slettes eller er utilgjengelige.[65] For det andre hendelser som innebærer en reell fare for brudd på informasjons- og personopplysningssikkerheten.

Med personvernhendelser menes hendelser som fører til at opplysninger om enkeltpersoner ikke blir håndtert på en lovlig og forsvarlig måte. Dette inkluderer andre hendelser enn brudd på personopplysningssikkerheten, for eksempel manglende vurdering av behandlingsgrunnlag, gjenbruk av opplysninger til uforenelige formål (formålsbegrensning), behandling av unødvendige opplysninger (dataminimering) eller manglende sletting (lagringsbegrensning).

Med avvik menes brudd på virksomhetenes egne rutiner/retningslinjer for sikker behandling av digitale verdier, eller manglende etterlevelse av reglene i personvernlovgivningen (personopplysningsloven og personvernforordningen – GDPR).

Informasjonssikkerhets- og personvernhendelser eller -avvik utløses av «kilder til fare» (trusselkilder[66]). Når det gjelder informasjonssikkerhet (inkludert personopplysningssikkerhet) kan det dreie seg om eksterne trusselkilder, for eksempel tilsiktede hendelser hvor nettkriminelle aktører eller APT-grupper[67] står bak.

Men det kan også dreie seg om interne trusselkilder, for eksempel utilsiktede hendelser eller avvik som skyldes manglende personvernrutiner eller utilstrekkelig sikkerhetskompetanse hos egne ansatte.

---

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

[66] Definisjonen er fra Direktoratet for digitalisering sin begrepsliste (https://internkontroll-infosikkerhet.difi.no/begrepsliste#Trusler%20eller%20trusselkilder).

[67] APT er, ifølge Kaspersky, trusselaktører som "(…) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences" (https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats). Det kan derfor dreie seg om statlige eller statsstøttede hackergrupper, men også om nettkriminelle grupper. I denne rapporten benyttes APT kun om statlige eller statsstøttede grupper. Se også Kristian Malmkvist Eie (2020): «Trusler og etterretning». I Håkon Bergsjø, Ronny Windvik og Lasse Øverlier (red.): Digital sikkerhet. En innføring. Oslo: Universitetsforlaget. Side 154-155.

RESTEN AV KAPITLET
Nedenfor gis først en gjennomgang av trusselbildet i UH-sektoren, nasjonalt og internasjonalt. Deretter gis en oversikt over hvilke uønskede hendelser og avvik som universitetene og høgskolene opplyste om i 2020.

TRUSSELBILDET INTERNASJONALT

Internasjonalt ser det ut til at trusselbildet i UH-sektoren har samme struktur som beskrevet i fjorårets rapport.[68] Enkelte av truslene synes imidlertid å ha forsterket seg i 2020. Det er i særlig grad knyttet til økt bruk av skadevare (løsepengevirus).[69]

Også andre forhold kan ha bidratt til et mer utfordrende trusselbilde, for eksempel bruk av hjemmekontor og nettundervisning i forbindelse med pandemihåndteringen,[70] og risiko for datatyveri hos universiteter som driver vaksineforskning (Covid-19).[71]

I USA har informasjonssikkerhet og personvern lenge vært blant de viktigste fokusområdene i UH-sektoren.[72] I EDUCAUSE sin årlige rangering av de 10 viktigste IT-områdene i høyere utdanning og forskning, blir informasjonssikkerhet rangert som det viktigste. Personvern blir rangert som det nest viktigste området.[73]

I Storbritannia gjennomførte National Cyber Security Center (NCSC) i 2019 en egen trusselvurdering for høyere utdanning og forskning.[74] NCSC mener det er svært sannsynlig at britiske universiteter vil være viktige mål for nettkriminelle grupper i årene fremover, og at det er høy grad av sannsynlighet for at universitetssektoren vil være mål for statlig eller statsstøttet dataspionasje/kunnskapstyveri (APT-grupper).

Jisc – det britiske tjenesteleveranseorganet på digitaliseringsområdet – gjennomfører hvert år en modenhetskartlegging av informasjonssikkerheten i høyere utdanning og forskning. 2020-kartleggingen[75] viser at i den britiske UH-sektoren er nettfiske den største trusselen mot informasjonssikkerheten. Deretter følger manglende sikkerhetsoppdateringer, menneskelige feil/uhell og skadevare, spesielt løsepengevirus.[76] I mars 2021 måtte 80 britiske skoler og universiteter utsette undervisningen på grunn av løsepengevirus.[77]

Sikkerhetsselskaper vurderer også trusselbildet i kunnskapssektoren. Det amerikanske selskapet Verizon legger i sin rapport for 2020 vekt på at kunnskapssektoren er særlig utsatt for tilsiktede sikkerhetsbrudd hvor motivet er økonomisk vinning. Ifølge Verizon, utgjør dette 96 prosent av alle registrerte tilsiktede sikkerhetsbruddene i sektoren. Dataspionasje og kunnskapstyveri representerer omkring tre prosent av tilsiktede sikkerhetsbrudd. Nettfiske, feil/uhell og skadevare fremheves som viktige trusler.[78]

[68] Se «Risiko- og tilstandsvurdering 2020», side 23-36 (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

[69] Se for eksempel "BlackBaud and Beyond – Educational Sector Targeted Consistently in Cyberattacks" (https://cyware.com/news/blackbaud-and-beyond-educational-sector-targeted-consistently-in-cyberattacks-df5a3aee); "Hackers Eye Students Returning to Virtual Classrooms as Easy Targets" (https://thehill.com/policy/cybersecurity/513022-hackers-eye-students-returning-to-virtual-classes-as-easy-targets?&web_view=true); "University of Utha Pays in Cyber Extortion Scheme" (https://www.darkreading.com/attacks-breaches/university-of-utah-pays-in-cyber-extortion-scheme/d/d-id/1338721?&web_view=true); "Newcastle University Cyber Attack to Take Weeks to Fix" (https://www.bbc.com/news/uk-england-tyne-54047179?&web_view=true).

[70] Se for eksempel Kaspersky: Digital Education: The Cyber Risks of the Online Classroom (https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/).

[71] Se for eksempel https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory.

[72] Se for eksempel EDUCAUSE Review Special Report: Top 10 IT Issues 2011 (https://er.educause.edu/articles/2011/5/topten-it-issues-2011).

[73] EDUCAUSE Review Special Report: Top 10 IT Issues 2020 (https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2020).

[74] National Cyber Security Center (2019): The Cyber Threat to Universities (https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities).

[75] Se https://www.jisc.ac.uk/blog/cyber-security-in-universities-and-colleges-is-improving-but-theres-no-room-for-complacency-20-oct-2020.

[76] En studie av sikkerhetsselskapet Redscan konkluderer med at 54 prosent av britiske universiteter opplevde minst ett sikkerhetsbrudd i løpet av en 12-månedersperiode i 2019-2020. Redscan: The State of Cyber Security Across UK Universities (https://www.redscan.com/news/state-of-cybersecurity-uk-universities-foi-report/).

[77] Se https://www.bbc.com/news/technology-57084943.

[78] Verizon: 2021 Data Breach Investigations Report, side 73-74 (https://www.verizon.com/business/resources/reports/dbir/).

Sikkerhetsselskapet BlueVoyant, konkluderer også med at økonomisk motiverte aktører utgjør den største trusselen mot universiteter og høgskoler.[79] Ødeleggelses-angrep (spesielt løsepengevirus) og datatyveri (spesielt personopplysninger og innloggingsdata) fremheves som de viktigste utfordringene. Selskapet viser til at på verdensbasis har omkring 200 universiteter vært utsatt for APT-operasjoner de siste to årene.

Tilsvarende trender identifiseres i studier gjennomført av andre sikkerhets- eller IT-selskaper.[80]

TRUSSELBILDET NASJONALT

Det nasjonale trusselbildet ser ut til å følge internasjonale trender – det er blitt mer utfordrende. Mens norske virksomheter i begrenset grad har vært utsatt for store og ødeleggende dataangrep, spesielt løsepengevirus, endret dette seg i 2020-21. Hurtigruten AS,[81] Østre Toten kommune,[82] Akva Group[83] og Vard[84] ble utsatt for slike angrep i 2020. Andre norske virksomheter, for eksempel Vinmonopolet, ble også rammet av ødeleggelsesangrep (tjenestenekt) i desember 2020.[85]

I 2021 ble blant annet Tietoevry,[86] Drammen kommune[87] og Volue[88] utsatt for dataangrep.

Størst oppmerksomhet fikk datainnbruddet på Stortinget i august/september 2020.[89] I mars 2021 ble Stortinget utsatt for et nytt datainnbrudd.[90] Virksomheter i UH-sektoren i Norge og utlandet ble også berørt.[91]

NASJONALE RISIKO- OG TRUSSELVURDERINGER

Norske politi-, sikkerhets- og etterretningsmyndigheter har blitt mer eksplisitte i sine vurderinger av digitale sikkerhetstrusler i UH-sektoren.[92]

I NSM sin risikovurdering for 2021 vies problemstillinger som er særlig relevante i høyere utdanning og forskning stor oppmerksomhet.[93] NSM fremhever at forskning om nordområdene, arktisk klima og polarforskning er utsatt for ulike typer etterretningsvirksomhet, inkludert nettverks-operasjoner.[94] Det samme gjelder forskning som både har militære og sivile anvendelsesområder.

PST fremhever ulovlig kunnskapsoverføring som en trussel i akademia og norsk forskning.[95] Romforskning, maritim

[79] BlueVoyant: Cybersecurity in Higher Education 2021 (https://www.bluevoyant.com/resources/cybersecurity-in-higher-education/).

[80] Se for eksempel Microsoft Digital Defense Report, 2020 (https://www.microsoft.com/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/); CrowdStrike Services Cyber Front Lines Report 2020 (https://www.crowdstrike.com/resources/reports/crowdstrike-services-cyber-front-lines-2020/); Fire-Eye: M-Trends 2021 (https://www.fireeye.com/blog/threat-research/2021/04/m-trends-2021-a-view-from-the-front-lines.html).

[81] Se for eksempel https://www.nrk.no/nordland/hurtigruten-rammet-av-dataangrep-med-losepengevirus-1.15288150.

[82] Se for eksempel https://www.nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398.

[83] Se for eksempel https://e24.no/hav-og-sjoemat/i/2dP17R/akva-group-har-faatt-kontroll-paa-omfattende-dataangrep.

[84] Se https://e24.no/naeringsliv/i/Vb0QL6/verftskonsernet-vard-utsatt-for-dataangrep.

[85] Se https://www.cw.no/artikkel/dataangrep/vinmonopolets-nettsider-utsatt-dataangrep.

[86] Se for eksempel https://e24.no/boers-og-finans/i/dlkKLB/tietoevry-utsatt-for-loesepenge-angrep-vi-anser-dette-som-en-alvorlig-kriminell-handling.

[87] Se for eksempel https://drm24.no/nyheter/hackerangrep-mot-kommunens-vann-systemer-2121938.

[88] Se for eksempel https://www.securityweek.com/green-energy-company-volue-hit-ransomware?&web_view=true.

[89] Se for eksempel https://www.nrk.no/norge/stortinget-utsatt-for-et-omfattende-it-angrep-1.15143406.

[90] Se for eksempel https://e24.no/naeringsliv/i/GawL8V/nsm-et-titalls-norske-bedrifter-kan-vaere-rammet-av-dataangrepet?referer=https%3A%2F%2Fwww.vg.no.

[91] Se for eksempel https://khrono.no/utsatt-for-hackere-som-krever-losepenger-alt-arbeid-stopper-opp/561879 eller https://khrono.no/oppdaget-uregelmessigheter-e-post-ute-av-spill-i-to-dager/561841.

[92] Se for eksempel https://www.dn.no/magasinet/dokumentar/politiets-sikkerhetstjeneste/ntnu/tekna/pst-hudfletter-universitetene-fullstendig-blaoyde-og-veldig-veldig-naive/2-1-919171.

[93] NSM: Risiko 2021 (https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler).

[94] NSM: Risiko 2021, side 26-27.

[95] PST: Nasjonal trusselvurdering 2021, side 2 og 12 (https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf).

teknologi og undervannsteknologi er områder som PST mener er mest utsatt for forsøk på dataspionasje og kunnskapstyveri. Også E-tjenesten legger vekt på problemstillinger knyttet til ulovlig kunnskapsoverføring, spesielt kunnskap og teknologi som kan ha militære anvendelsesområder (masseødeleggelsesvåpen).[96]
Det understrekes at forskning innenfor andre områder, for eksempel nordområdene, er gjenstand for oppmerksomhet fra utenlandsk etterretning.

Økokrim, på sin side, fokuserer på nettkriminalitet.[97]
Her sies det at den daglige kriminaliteten preges av massebedragerier i digitale rom, misbruk av person-opplysninger og bruk av kryptovaluta som betalingsmiddel. Det påpekes at en liten del av nettkriminaliteten anmeldes til politiet.[98]

MOTSTRIDENDE HENSYN

Vurderingene til norske politi-, sikkerhets- og etterretnings-myndigheter kan stå i et visst spenningsforhold til viktige målsettinger og verdier i høyere utdanning og forskning, for eksempel åpenhet, forskningsfrihet, kunnskapsdeling og internasjonalt samarbeid.

Dette spenningsforholdet har i løpet av 2020-21 fått større politisk og medial oppmerksomhet.[99]

INFORMASJONSSIKKERHET – UØNSKEDE HENDELSER OG AVVIK

Totalt rapporterte universitetene og høgskolene om ca. 2000 uønskede hendelser og avvik på informasjons-sikkerhetsområdet i 2020. 20 av 21 universiteter og høgskoler opplyste om at de hadde vært utsatt for uønskede hendelser eller avvik med hensyn til informasjonssikkerhet i 2020.

Det totale antallet hendelser og avvik er noe lavere enn det som ble rapportert i 2019. Nedgangen skyldes endringer i måten vi regner hendelser og avvik på. Reduksjonen reflekterer derfor ikke substansielle endringer i hendelsesomfanget.

Totaltallet på ca. 2000 hendelser og avvik inkluderer ikke rapporteringer hvor antall hendelser ble oppgitt på en svært omtrentlig måte, for eksempel «gjentatte forsøk på nett-fiske». Det inkluderer kun hendelser eller avvik hvor det ble oppgitt et konkret antall eller hvor det ble gitt presise nok anslag til å få et tydelig bilde av hendelsesomfanget.

Enkelte virksomheter inkluderte sårbarheter (sikkerhets-hull) i systemer og tjenester i sine oversikter over hendelser og avvik. De fleste virksomhetene rapporterte ikke om slike sårbarheter med mindre de hadde ført til sikkerhetsbrudd.

OM HENDELSES- OG AVVIKS-RAPPORTERINGEN

I kartleggingen for 2020 ble ikke virksomhetene bedt om å rapportere på forhåndsdefinerte hendelses- eller avvikskategorier. Det eneste vi ba om var at virksomhetene ga en oversikt over hvilke hendelser og avvik de hadde vært utsatt for. Det førte til at det oppsto en viss tvil om hvordan enkelte hendelser eller avvik skal kategoriseres. Presentasjonen nedenfor gir likevel et dekkende bilde av sektortilstanden, slik den ble rapportert til oss.

[96] E-tjenesten: Fokus 2021, side 40 (https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf).

[97] Økokrim: Trusselvurdering 2020, side 38-47 (https://www.okokrim.no/trusselvurdering-2020.6304950-411472.html). Se også Europol: Internet Organized Crime Threat Assessment 2020 (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020).

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

[99] Se for eksempel https://www.vg.no/nyheter/innenriks/i/41LGVE/frp-roy-frykter-oekt-studentutveksling-fremmer-spionasje og https://www.vg.no/nyheter/innenriks/i/pAGd4X/hoeyre-haarek-vil-hindre-universitets-spionasje.

Som tidligere år, er det totale antallet hendelser og avvik skjevt fordelt mellom universitetene og høgskolene. Det skyldes at NTNU og UiO har opprettet egne IT-sikkerhetsmiljøer: NTNU SOC i Seksjon for digital sikkerhet og UiO CERT ved Universitetets senter for informasjonsteknologi (USIT).

De øvrige virksomhetene har ikke opprettet tilsvarende spesialiserte IT-sikkerhetsmiljøer. De har derfor heller ikke den samme oppdagelses- og analysekapasiteten som NTNU og UiO.

GENERELT OM INFORMASJONSSIKKERHETSHENDELSER OG -AVVIK

Det store flertallet av rapporterte hendelser og avvik på informasjonssikkerhetsområdet i 2020 handler om IT-sikkerhet, spesielt nettbaserte hendelser (digital sikkerhet). Dette er tilsiktede hendelser hvor motivet enten er økonomisk vinning eller hvor det trolig dreier seg om statlig eller statsstøttet kunnskapstyveri/dataspionasje.

De resterende hendelsene handler om utilsiktede feil/uhell, inkludert avvik fra rutiner for sikker behandling av personopplysninger og tekniske feil. Det dreier seg også om ulike typer hendelser eller avvik som ikke passer inn i de nevnte kategoriene.

TILSIKTEDE HENDELSER – ØKONOMISK VINNING

Ifølge enkelte beregninger, finnes det flere enn 1900 aktive trusselaktører som opererer på internettet.[100] De fleste av disse er enten nettkriminelle grupper eller grupper med uklar/ukjent motivasjon. Ovenfor har vi sett at andre kartlegginger indikerer at over 90 prosent av digitale sikkerhetshendelser i kunnskapssektoren internasjonalt er økonomisk motivert.[101]

Dette stemmer godt med det vi har funnet i den norske UH-sektoren, både i årets og ved tidligere års kartlegginger. Det betyr at også i 2020 er det trolig at omkring (eller noe i underkant av) 90 prosent av alle rapporterte brudd på informasjonssikkerheten er økonomisk motivert. Det betyr ikke at alle disse hendelsene kan føres tilbake til nettkriminelle grupper – også APT-grupper (statlige eller statsstøttede trusselaktører) kan være motivert av økonomisk vinning.[102] Det er likevel sannsynlig at det store flertallet av dem kan det.

Nettfiske og sosial manipulasjon er de mest brukte metodene som anvendes av trusselaktører hvor økonomisk vinning trolig er motivet. Antallet uønskede hendelser hvor brukerkontoer kompromitteres på grunn av nettfiske – medarbeidere eller ledere lures til å oppgi innloggingsdata (brukernavn og passord) til trusselaktørene – er omtrent på samme nivå som i 2019.

To virksomheter opplyste om at antallet vellykkede kompromitteringsforsøk er færre i 2020 enn tidligere. Det ble forklart med innføring av totrinnsinnlogging eller nye krav til bruk av sterke passord.

Masseutsendelse av epost er den vanligste bruken av kompromitterte kontoer. Men kompromitterte brukerkontoer kan også anvendes til andre formål, spesielt distribusjon av skadevare. I 2020 ble det rapportert om flere tilfeller av skadevarehendelser hvor formålet er misbruk av lokale dataressurser til utvinning av kryptovaluta (Bitcoin). Hos én virksomhet hadde datakraften i et lokalt tungregneanlegg blitt misbrukt på denne måten over en lengre periode. Antallet rapporterte hendelser med denne typen skadevare virker imidlertid å være noe lavere enn i 2019.

Hos enkelte virksomheter ble det opplyst om at det i 2020 er registrert en viss økning i antallet hendelser som gjelder annen type skadevare. Her ble det spesielt pekt på trusselen fra nye nettkriminelle tjenestemodeller – nettkriminalitet-som-en-tjeneste.[103] Emotet[104] og Ryuk[105] er to slike tjenester (henholdsvis botnet og løsepengevirus) som er observert i sektoren i 2020.

---

[100] Fire-Eye: M-Trends 2021, side 20 (https://www.fireeye.com/blog/threat-research/2021/04/m-trends-2021-a-view-from-the-front-lines.html).

[101] CrowdStrike oppgir at 63 prosent av alle hendelser sikkerhetsselskapet registrerte i 2020 var økonomisk motivert. Se CrowdStrike Services Cyber Front Lines Report 2020 (https://www.crowdstrike.com/resources/reports/crowdstrike-services-cyber-front-lines-2020/).

[102] Samtidig kan APT-aktivitet – statlig eller statsstøttet dataspionasje/kunnskapstyveri – fremstå som nettkriminalitet. Sikkerhetsselskapet FireEye mener for eksempel at i opp mot 10 prosent av hendelser som innebærer kompromittering av datanettverk, er dataspionasje/kunnskapstyveri den virkelige motivasjonen. M-Trends 2021, side 19 (https://www.fireeye.com/blog/threat-research/2021/04/m-trends-2021-a-view-from-the-front-lines.html).

[103] Se for eksempel Ben Collier et al. (2020): Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. Workshop on the Economics of Information Security, 14.-15. December 2020 (https://doi.org/10.17863/CAM.53769).

[104] Se https://www.malwarebytes.com/emotet/.

[105] Se https://www.malwarebytes.com/ryuk-ransomware/.

Sosial manipulasjon, særlig forsøk på direktør- eller fakturasvindel ved bruk av epost, er fortsatt vanlig i UH-sektoren. Dette handler om at medarbeidere mottar epost hvor trusselaktøren utgir seg for å være leder i virksomheten, og hvor det bes om at det foretas en hasteutbetaling (pengene overføres til trusselaktørens bankkonto).

Også i 2020 ble det rapportert om et titalls vellykkede forsøk på direktørsvindel. Men i motsetning til i 2019, har det ikke skjedd utbetaling av større beløp. Der hvor utbetaling ble gjennomført dreide det som om at medarbeidere ble lurt til å kjøpe gavekort (tilsynelatende etter forespørsel fra leder) med verdi på mellom 3000 og 10 000 kroner.

Til slutt ble det opplyst om hendelser hvor sårbarheter i programvare, for eksempel kode- eller designfeil, har blitt utnyttet. Motivet bak disse hendelsene er enten ukjent eller det handler trolig om økonomisk vinning. Hos én virksomhet ble en sårbarhet i virksomhetens VPN-løsning utnyttet. Hendelsen fikk en viss medieoppmerksomhet høsten 2020.[106] Sårbarheten ga trusselaktøren tilgang til enkelte brukerkontoer, men uten at det førte til alvorlige skadevirkninger.

TILSIKTEDE HENDELSER – KUNNSKAPSTYVERI (APT-HENDELSER)

APT-aktivitet er, som nevnt ovenfor, dataspionasje/kunnskapstyveri som enten utføres av statlige hackergrupper eller av nettkriminelle grupper som jobber på oppdrag fra eller i samforstand med statlige myndigheter.[107]

Ettersom APT-grupper benytter mange av de samme kompromitteringsmetodene, spesielt nettfiske, og utnytter mange av de samme sårbarhetene som nettkriminelle aktører, kan det være vanskelig å skille APT-aktivitet fra nettkriminell aktivitet. Flere av hendelsene i 2020 er derfor mistenkte APT-hendelser.

I 2020 ble det rapportert om seks-sju APT-hendelser. Dette er noen flere enn det som ble rapportert for 2019 (tre).

Én av virksomhetene i sektoren opplyste om at den har vært utsatt for to APT-hendelser i 2020. Hendelsene gjelder forsøk på industrispionasje og etterretningsvirksomhet rettet mot teknologimiljøer, blant annet informatikk.

Hos en annen virksomhet ble det opplyst om at det er registrert inntrengingsforsøk fra den samme aktøren som sto bak datainnbruddet på Stortinget i august 2020. Det dreier seg altså, ifølge PST, om en hackergruppe tilknyttet russisk militæretterretning.[108] I motsetning til på Stortinget, lyktes ikke inntrengingsforsøket hos den aktuelle UH-institusjonen.

Hos en tredje virksomhet ble det opplyst om en hendelse som involverer en kjent statsstøttet hackergruppe i Iran («Silent Librarian»[109]). Gruppen har spesialisert seg på datainnbrudd i UH-sektoren og motivet er tyveri av vitenskapelige publikasjoner. Hendelsen ble oppdaget da det ble registrert innlogginger fra Iran på lokale brukerkontoer. Dette ble oppdaget i august 2020, men kompromitteringen skjedde trolig noen måneder tidligere.

En fjerde virksomhet rapporterte om et IT-sikkerhetsbrudd hvor det er uavklart om det dreier seg om APT eller nettkriminell aktivitet. Hendelsen ble oppdaget og varslet av NSM etter treff på signaturer (IP-adresser) i virksomhetens VDI-sensor. De aktuelle IP-adressene hadde tidligere blitt benyttet av en «større trusselaktør». Aktøren hadde hatt tilgang til deler av det lokale datanettverket i minst ett år.

Andre hendelser gjelder bruk av programvare med sårbarheter som utnyttes av APT-grupper. Én slik hendelse dreier seg om et nettadministrasjonsverktøy levert av det amerikanske selskapet SolarWinds. I 2019/20 ble oppdateringsserveren til denne programvaren kompromittert av det som antas å være en russisk APT-gruppe.[110] Kompromitteringen innebar at omkring 18 000 av SolarWinds kunder verden over ble sårbare for datainntrengning, inkludert minst én av virksomhetene i norsk UH-sektor. Denne virksomheten oppga at sårbarheten ikke har blitt utnyttet og at bruken av programvaren ble avsluttet etter at sårbarheten ble kjent.

---

[106] Se for eksempel https://e24.no/teknologi/i/mRX2Gp/internasjonalt-dataangrep-mot-nhh.

[107] Enkelte APT-grupper har også andre mål med sin virksomhet, for eksempel dataødeleggelse, tjenesteforringelse, sabotasje (fysisk skade) eller økonomisk vinning. Se for eksempel Ben Buchanan (2020): The Hacker and the State: Cyber Attack and the New Normal of Geopolitics. Cambridge, Mass.: Harvard University Press, eller Luca Follis og Adam Fish (2020): Hacker States. Cambridge, Mass.: The MIT Press. Se også Verizon: Cyber-Espionage Report, 2020-2021 (https://www.verizon.com/business/resources/reports/cyber-espionage-report/).

[108] Se https://pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/.

[109] «Silent Librarian» (eller «The Mabna Institute») er en privat nettkriminell gruppe i Teheran som koordinerer deler av sin virksomhet med iranske myndigheter (revolusjonsgarden). Se US Department of Justice (2018): Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guard Corps (https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic). Se også https://www.nrk.no/norge/pst_-_-iran-bak-hacking-av-norske-universiteter-1.14044442.

[110] Se for eksempel https://www.insidehighered.com/news/2021/01/06/unraveling-solarwinds-hacks-fallout-higher-ed?&web_view=true eller https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols.

Etter at årets kartlegging var avsluttet, ble en annen virksomhet utsatt for et mulig sikkerhetsbrudd via en sårbarhet i virksomhetens eposttjeneste (Microsoft Exchange). Den aktuelle sårbarheten har blitt utnyttet av en kinesisk APT-gruppe.[111] Tre andre virksomheter i UH-sektoren ble også berørt av denne sårbarheten, men uten at det medførte sikkerhetsbrudd. Uninett CERT[112] (sammen med andre nasjonale aktører[113]) varslet sektoren om problemet, og om viktigheten om at tilgjengelige sikkerhetsoppdateringer benyttes.

Den mest alvorlige mistenkte APT-hendelsen ble avdekket i desember 2020, og fikk en viss medieoppmerksomhet.[114] Her har en trusselaktør fått tilgang til brukerkontoer hos den aktuelle virksomheten. Derfra har aktøren tatt seg videre inn i det lokale datanettverket. Datainntrengingen hadde pågått i drøyt 90 dager før virksomheten ble varslet. Aktøren virker å ha vært særlig interessert i forskning om nordområdene og internasjonalisering. Saken er under etterforskning.

UTILSIKTEDE HENDELSER – FEIL OG UHELL

Utilsiktede hendelser, det vil si tekniske eller menneskelige feil og uhell, utgjør i underkant av ti prosent av de hendelsene som universitetene og høgskolene rapporterte om i 2020. Dette er dermed den nest største hendelseskategorien.

Tekniske hendelser inkluderer både feil i egen-driftede digitale løsninger og feil hos eksterne leverandører av digitale systemer eller tjenester.

I enkelte tilfeller har slike feil ført til uautorisert eksponering av personopplysninger. Den vanligste typen hendelser er imidlertid manglende tilgjengelighet til digitale systemer eller tjenester. Mange av disse hendelsene skyldes ikke feil hos virksomhetene selv, men hos eksterne leverandører (databehandlere).

Med menneskelige feil eller uhell menes hendelser eller avvik som skyldes manglende kompetanse, bevissthet eller hastverk. Det kan også skyldes mer systematiske avvik, spesielt manglende rutiner for sikker håndtering av informasjonsverdier og personopplysninger.

Som i tidligere år, fører menneskelige feil eller uhell ofte til uautorisert eksponering av personopplysninger. Dette handler spesielt om feil publisering av dokumenter som inneholder personopplysninger. Opplysningene publiseres enten på internettet (offentlig postjournal eller hjemmesider) eller via interne publiserings- og delingsområder, for eksempel læringsplattformer.

Det ble i tillegg opplyst om en del hendelser som gjelder feilsending av elektroniske meldinger (SMS eller epost). Også disse sikkerhetsbruddene fører til uautorisert eksponering av personopplysninger.

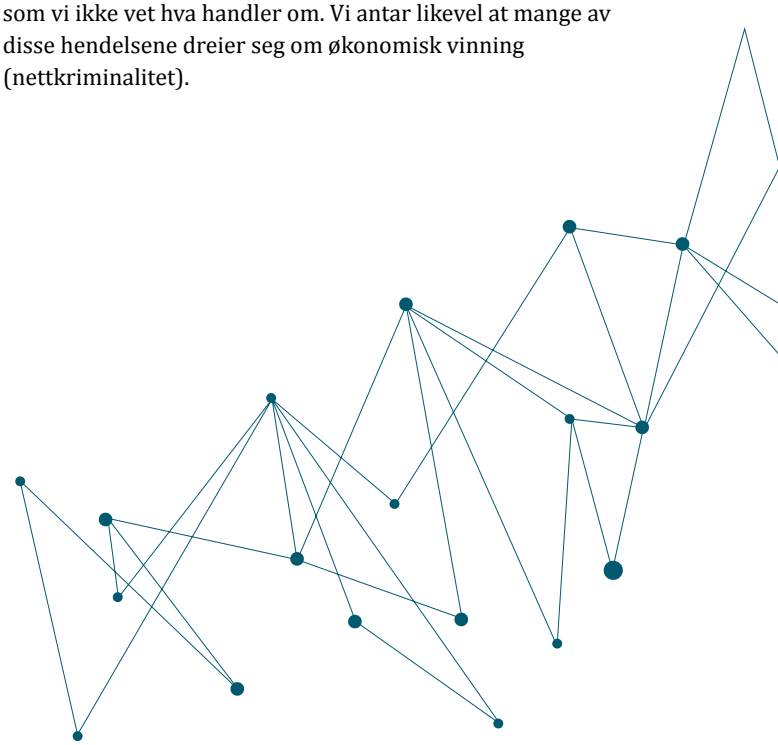
Hendelser som skyldes menneskelige feil eller uhell impliserer ofte avvik fra lokale rutiner for sikker behandling av informasjon/opplysninger.

ANDRE TYPER HENDELSER

Denne restkategorien gjelder hendelser eller avvik som ikke hører til i kategoriene ovenfor, eller som vi ikke vet nok om til å kunne kategorisere.

Kategorien inneholder noen få saker som gjelder tyveri av IT-utstyr (datamaskiner, nettbrett, osv.).

Den inneholder også omkring 50 IT-sikkerhetshendelser som vi ikke vet hva handler om. Vi antar likevel at mange av disse hendelsene dreier seg om økonomisk vinning (nettkriminalitet).



[111] Se for eksempel https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

[112] Se for eksempel https://www.uninett.no/pagaende-e-postangrep-i-kunnskapssektoren-kjent-sarbarhet.

[113] Se https://nsm.no/aktuelt/oppdater-microsoft-exchange-snarest.

[114] Se for eksempel https://www.tv2.no/a/11841152/

HENDELSER IKKE RAPPORTERT
Som tidligere år er det også i 2020 enkelte typer hendelser som vi forventet å motta rapporter på, men som bemerket seg med sitt (relative) fravær. Dette gjelder særlig tjenestenektangrep og løsepengevirus.

Bare én virksomhet hadde registrert forsøk på løsepenge-virusangrep i 2020. I resten av sektoren ble det ikke rapportert om dette.

Tjenestenektangrep er en gjenganger i kategorien «fraværende hendelser». Verken i 2020, 2019 eller 2018 ble det rapportert om større angrep av denne typen.

UH-SEKTORENS RESPONSMILJØ – UNINETT CERT
UH-sektorens responsmiljø – Uninett CERT – har ansvaret for å oppdage og varsle om uønsket aktivitet (digitale sikkerhetshendelser og sårbarheter) i forskningsnettet. Som tidligere år, har vi innhentet hendelsesdata fra Uninett CERT.

OM HENDELSER REGISTRERT AV UNINETT CERT

Det vil trolig være et visst sammenfall mellom de hendelsene og sårbarhetene som rapporteres av virksomhetene selv og de som registreres hos Uninett CERT. Det er derfor ikke slik at alle hendelser og sårbarheter registrert hos Uninett CERT kommer i tillegg til de som virksomhetene opplyste om – det vil være noe dobbeltregistrering.

Vi har ikke mulighet til å avgjøre graden av dobbeltregistrering.

Fra 2018 til 2019 registrerte Uninett CERT en nedgang i antallet digitale sikkerhetshendelser og sårbarheter: 965 hendelser i 2018 og 792 i 2019. I 2020 har antallet registrerte hendelser og sårbarheter økt noe igjen – til 867.

Uninett CERT mente at det i 2020 ikke har skjedd vesentlige endringer i typer registrerte hendelser og sårbarheter sammenliknet med 2019 og 2018.

Den vanligste sårbarheten i 2020 er «DDOS amplifiers». Dette er datamaskiner som kan misbrukes til gjennomføring av tjenestenektangrep.

I tillegg har Uninett CERT registrert følgende vanlige hendelser og sårbarheter i 2020:

- Kompromitterte systemer: trusselaktører får tilgang til lokale IT-systemer, vanligvis på grunn av brukerfeil.
- Kompromitterte brukerkontoer: trusselaktører får tilgang til én eller flere kontoer, vanligvis som følge av brukernavn og passord på avveie.
- Nettfiske: kategorien er overlappende med kompromittert brukerkontoer og systemer, men spesifiserer angrepsvektoren – metoden som trusselaktører benyttet for å få skaffe seg tilgang.
- Skanning og innloggingsforsøk: kartlegging av sårbarheter i lokale dataressurser. Dette inkluderer kompromitterte datamaskiner i UH-sektoren som misbrukes til å skanne etter sårbarheter hos andre virksomheter. Innloggingsforsøk gjelder «brute force»-angrep (automatisert brukernavn- og passordgjetting).
- Infiserte systemer (skadevare): systemer som har blitt utsatt for ulike typer «ondsinnet kode». Uninett CERT har ikke informasjon om hvilke typer skadevare det dreier seg om.
- Sårbare systemer: systemer som var eksponert mot internettet og som ikke er sikkerhetsoppdatert. Uninett CERT mener at deres statistikk ikke gir et riktig bilde av omfanget – antallet sårbare systemer er trolig langt høyere enn hva deres tall indikerer.

Uninett CERT oppga i tillegg at de har registrert en viss nedgang i svindelforsøk i 2020 (direktør- og fakturasvindel).

På bakgrunn av statistikken for 2020, mener Uninett CERT at nettfiske var den største trusselen mot informasjons-sikkerheten i UH-sektoren i 2020, og at dette vil være tilfelle også i 2021.

Uninett CERT observerer at sektoren kjennetegnes av store angrepsflater, det vil si mange mulige måter å bryte informasjonssikkerheten på.

PERSONVERN – UØNSKEDE HENDELSER OG AVVIK

Universitetene og høgskolene opplyste om hvilke personvernhendelser og -avvik de har registrert i 2020. Dette inkluderer også andre krenkelser av personvernet eller avvik fra lovpålagte plikter (reglene i person-opplysningsloven og personvernforordningen) enn brudd på personopplysningssikkerheten.

Mange saker som gjelder personopplysningssikkerheten, ble likevel rapportert som personvernhendelser, blant annet sikkerhetsbrudd som ble meldt til Datatilsynet.

GENERELT OM PERSONVERNHENDELSER OG -AVVIK
Hos enkelte virksomheter ble personvernhendelser og -avvik rapportert uten at det ble oppgitt et bestemt antall. Det er derfor noe utfordrende å gi et presist tall for slike hendelser og avvik i 2020. Vårt anslag er at det totalt dreide seg om mellom 150 og 200 hendelser og avvik. Dette er noen flere enn det som ble rapportert i 2019 (ca. 140).

Økningen skyldes primært flere rapporter om manglende sluttmelding til eller registrering av forsknings- og student-prosjekter hos Norsk senter for forskningsdata (NSD) (se nedenfor).

TYPER HENDELSER OG AVVIK
De vanligste hendelsene handler om brudd på konfidensialiteten, det vil si uautorisert eksponering av eller tilgang til personopplysninger. Dette er saker hvor det har skjedd reelle personvernkrenkelser (uvedkommende har fått tilgang til opplysningene).

Andre saker handler om risiko for brudd på konfidensialiteten, men hvor slike brudd ikke har skjedd. Eksempler på dette er mangelfull anonymisering eller pseudonymisering av opplysninger som behandles i forskningsprosjekter.

I tillegg til hendelser og avvik gjeldende konfidensialiteten til personopplysninger, ble det rapportert om fire andre hovedtyper personvernhendelser og -avvik:

- Manglende behandlingsgrunnlag. Sakene dreier seg om at det ikke blir gjort vurderinger av lovlig grunnlag for behandlinger av personopplysninger, for eksempel samtykke eller lovhjemmel, eventuelt at feil behandlingsgrunnlag blir lagt til grunn.
- Manglende registrering hos NSD. Sakene dreier seg om to forhold. Enten at forskningsprosjekter eller studentprosjekter som behandler personopplysninger ikke registreres i meldingsarkivet hos og blir vurdert av NSD. Eller tilfeller hvor registrering hos NSD er påbegynt, men ikke sluttført.
- Manglende sluttmelding til NSD. Sakene handler om at forskningsprosjekter eller studentprosjekter som behandler personopplysninger ikke er bekreftet avsluttet i meldingsarkivet til NSD. Det er derfor uklart om opplysningene har blitt slettet eller forsvarlig anonymisert ved prosjektslutt.
- Overføringer til tredjeland. Sakene gjelder overføringer av personopplysninger til land utenfor EU/EØS.[115] Dette er saker hvor overføring har skjedd i strid med de nye kravene til landvurderinger og etablering av beskyttelsestiltak, jf. Schrems II-dommen[116] – eller hvor det er usikkert om dette har skjedd. Samtidig er det uklart hvilke krav som gjelder ved slike overføringer, for eksempel om det åpnes for en risikobasert tilnærming eller om tilnærmingen vil være rettighetsbasert. [117]

Det ble også rapportert om andre typer avvik. Eksempler på slike avvik er manglende databehandleravtaler med eksterne leverandører, feil lagring av personopplysninger og manglende registrering av nye behandlinger i virksomhetenes behandlingsprotokoller.

I tillegg ble det opplyst om virksomheter som enten ikke har sluttført arbeidet med utarbeidelse av protokoll over behandlinger av personopplysninger, eller som mener at behandlingsprotokollen må kvalitetssikres/oppdateres.

[115] Se https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/.

[116] Se https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-edpb-veiledning-om-schrems-ii/.

[117] For diskusjon, se for eksempel https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/. Se også Raphael Gellert (2020): The Risk-Based Approach to Data Protection. Oxford: Oxford University Press.

MELDINGER TIL DATATILSYNET
Alvorlige personvernhendelser eller -avvik, det vil si saker som innebærer risiko for krenkelser av personvernet, skal meldes til Datatilsynet. Enkelte av disse sakene skal også meldes til berørte personer («de registrerte»).[118]

Det ble rapportert om totalt 30 meldte personvernhendelser og -avvik i 2020. Dette er en dobling sammenliknet med 2019. Da ble totalt 14 hendelser og avvik meldt til Datatilsynet.

De 30 meldte sakene fordelte seg på 12 av 21 universiteter og høgskoler. Ni virksomheter rapporterte om at de ikke har registrert hendelser eller avvik som er meldepliktige til Datatilsynet.

MELDINGSTYPER
Den typiske meldingen til Datatilsynet i 2020 gjelder brudd på konfidensialiteten til personopplysninger. Konfidensialitetsbruddene skyldes ulike forhold, for eksempel feil hos tjenesteleverandør eller datainntrengning. Dette inkluderer også hendelser hvor det er mistanke om at APT-grupper står bak.

De vanligste årsakene til konfidensialitetsbrudd meldt til Datatilsynet, er likevel feilsending av epost og feil publisering av personopplysninger. Feil lagring av slike opplysninger, det vil si på lagringsområder som er tilgjengelige for mange ansatte eller studenter, er også en vanlig grunn til at Datatilsynet ble varslet.

Det ble i tillegg rapportert om flere tilfeller hvor Datatilsynet ble varslet om behandlinger uten gyldig behandlingsgrunnlag.

Det ble ikke opplyst om meldte hendelser som berører et stort antall registrerte. De mest alvorlige hendelsene gjelder feilsending eller feilaktig publisering av særlige kategorier opplysninger, for eksempel politiattester eller helseopplysninger. Disse hendelsene gjelder én eller noen få registrerte.

SKADEVIRKNINGER

Universitetene og høgskolene opplyste om at de aller fleste informasjonssikkerhets- og personvernhendelsene og -avvikene har resultert i små eller ingen nevneverdige skadevirkninger. Dette mønsteret – mange hendelser/avvik, få alvorlige skadevirkninger – har vi sett i tidligere kartlegginger.

De virksomhetene som hadde flest hendelser og avvik, opplyste ikke om flere hendelser med alvorlige skadevirkninger enn virksomheter som hadde få hendelser og avvik.

De vanligste skadevirkningene i 2020 er:

- Personvernkrenkelser. Brudd på konfidensialiteten til personopplysninger som følge av for eksempel feilpublisering på hjemmesider, feilsending av eposter eller IT-sikkerhetsbrudd.
- Manglende overholdelse av rettslige plikter: Avvik fra regler om lovlig og sikker behandling av person-opplysninger og andre informasjonsverdier, for eksempel brudd på personopplysningsloven og personvernforordningen.
- Direkte økonomisk tap. Økonomiske utlegg i forbindelse med nettsvindel, spesielt direktørsvindel.
- Tapt arbeidstid. Perioder med produksjonstap på grunn av manglende eller ustabil tilgang til digitale systemer eller tjenester.
- Oppryddingskostnader. Ekstraarbeid og innleie av sikkerhetseksperter i forbindelse med håndtering av hendelser og avvik, og anskaffelse av nye tekniske løsninger til erstatning for sårbare systemer.
- Uautorisert bruk av dataressurser. Bruk av kompromitterte kontoer til masseutsendelse av epost, bruk av kompromitterte systemer til utvinning av krypto-valuta eller til gjennomføring av nettverksoperasjoner rettet mot andre virksomheter.

[118] Jf. EUs personvernforordning (GDPR) artikkel 33 og 34.

SKADEVIRKNINGER – ENDRINGER I 2020

Omdømmekostnader er en skadevirkning som i liten grad ble nevnt i 2020. Dette er en endring fra 2019. Samtidig registrerte Unit 18 medieoppslag i 2020 som gjelder uønskede hendelser og avvik hos universitetene og høgskolene. Oppslagene kan ha medført en viss omdømmekostnad for de berørte virksomhetene og for sektoren som sådan.

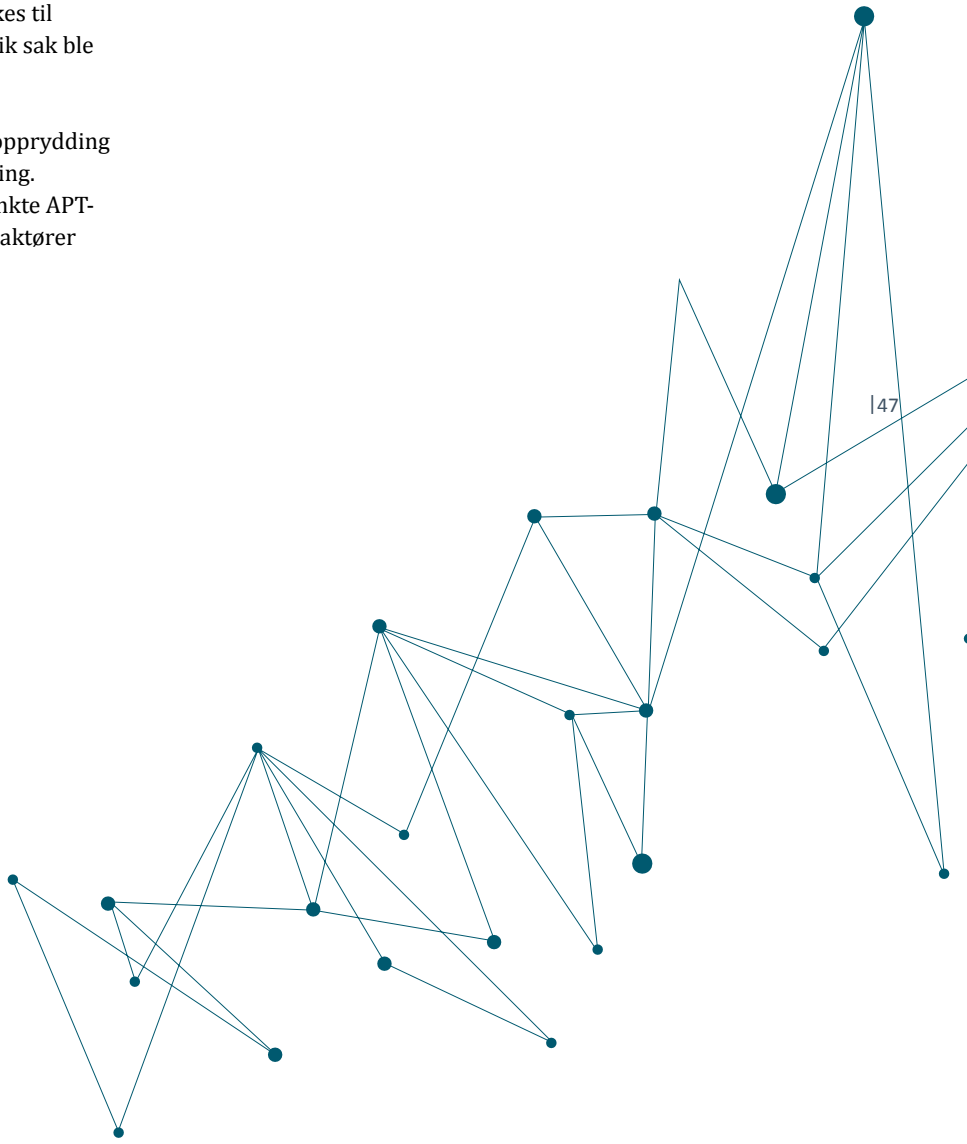
Noen færre tilfeller med direkte økonomisk tap er et annet endringstrekk sammenliknet med 2019.[119] Det ble ikke meldt om saker med mulige brudd på eksportkontroll-restriksjoner, det vil si tyveri av kunnskap eller teknologi som har flerbrukspotensial eller som kan brukes til fremstilling av masseødeleggelsesvåpen. Én slik sak ble registrert i 2019.[120]

Større kostnader knyttet til håndtering av og opprydding etter IT-sikkerhetshendelser er en tredje endring. Dette gjelder primært i bekreftede eller mistenkte APT-endelser, men også i enkelte saker hvor andre aktører trolig var involvert.

Til slutt er det, som vi har sett, en dobling av antallet meldinger til Datatilsynet i 2020. Det indikerer økte skadevirkninger knyttet til personvern og brudd på person-vernregelverket. Økningen kan bety at flere hendelser og avvik oppdages og meldes.

NESTE KAPITTEL

I neste kapittel gis en gjennomgang av arbeidet med informasjonssikkerhet og personvern hos de ni direktoratene og selskapene som omfattes av departementets styringsmodell.



[119] Se for eksempel https://khrono.no/misbrukte-uis-rektorens-navn-i-svindelforsok/526319.

[120] Saken fikk stor medieoppmerksomhet i januar 2020. Se for eksempel https://www.vg.no/nyheter/innenriks/i/jd73bb/to-ntnu-forskere-siktet-av-pst og https://www.nrk.no/trondelag/ntnu-begynte-a-mistenke-de-to-siktede-forskerne-allerede-for-ett-ar-siden-1.14869687.
Se også https://www.dn.no/magasinet/dokumentar/politiets-sikkerhetstjeneste/ntnu/tekna/pst-hudfletter-universitetene-fullstendig-blaoyde-og-veldig-vel-dig-naive/2-1-919171.

KAPITTEL 4

DIREKTORATER OG SELSKAPER

DIREKTORATER OG SELSKAPER

INNLEDNING

Ni direktorater og selskaper underlagt Kunnskapsdepartementet omfattes av styringsmodellen for informasjonssikkerhet og personvern. Dette gjelder følgende virksomheter:

Direktoratet for internasjonalisering og kvalitetssikring i høyere utdanning (Diku), Norges forskningsråd (NFR), Nasjonalt organ for kvalitet i utdanningen (NOKUT), Norsk senter for forskningsdata (NSD), Simula AS, Uninett AS, Norsk utenrikspolitisk institutt (NUPI), De nasjonale forskningsetiske komiteene (FEK) og Universitetssenteret på Svalbard (UNIS).[121]

I dette kapitlet følger først en kort gjennomgang av viktige oppgaver og digitale verdier som denne delen av UH-sektoren forvalter.

Deretter følger en oversikt over personalressurser og uønskede informasjonssikkerhets- og personvernhendelser.

Til slutt gis en oversikt over (i) status for ledelsessystemer for informasjonssikkerhet og internkontroll GDPR, (ii) sårbarheter i arbeidet og (iii) viktige tiltak som virksomhetene har iverksatt.

VIRKSOMHETENE OG DIGITALE VERDIER

De ni direktoratene og selskapene har til sammen omkring 1250 ansatte i 2019/2020. Flest ansatte har NFR (ca. 460[122]). Det er bare UNIS som har vitenskapelig ansatte og studenter (743 studenter i 2019[123]). NUPI og Simula har vitenskapelige ansatte (forskere).

Størrelsen på de ni virksomhetene gjør at de fleste forvalter færre digitale verdier – informasjon/data og dataressurser (datamaskiner, programvare, nettverksutstyr, osv.) – enn universitetene og høgskolene. Men også disse virksomhetene forvalter betydelige økonomiske midler. Dette kan gjøre dem sårbare for nettkriminalitet.

Tidligere har vi sett at NSD forvalter viktige digitale verdier på sektornivå (spesielt i forskning), og leverer tjenester til sektoren på personvernområdet. Dette gjelder i enda større grad for Uninett, som leverer og administrerer forskningsnettet i Norge og utvikler/forvalter andre sentrale digitale verdier, blant annet gjennom datterselskapet Sigma2.

Samtidig blir utviklingen av direktoratenes forvaltningsoppgaver mer avhengig av digitale verdier. NFR oppgir for eksempel at automatisering og bruk av kunstig intelligens vil bidra til økt forvaltningskvalitet, bedre kundeorientering og økt produktivitet. I 2019 testet NFR ut slike løsninger i deler av søknadsbehandlingen – robotteknologi ble benyttet til å løse rutineoppgaver.[124] NFR har også digitalisert anskaffelsesprosessen.[125]

NOKUT har digitalisert og automatisert søknads- og saksbehandlingsprosesser i 2019 (gjennom søknadsportalen). Dette gjelder blant annet søknader om godkjenning av bachelorgrader fra utlandet.[126] Digitaliseringen og automatiseringen har medført at saksbehandlingstiden er halvert.[127]

I tillegg gjennomfører enkelte av virksomhetene forskning innenfor viktige kunnskapsområder. For Simula og NUPI dreier det seg blant annet om områder som kryptologi, sikkerhets- og forsvarsstudier og andre områder som er viktige for norsk utenrikspolitikk.

UNIS driver forskning innenfor områder som biologi, geologi, geofysikk og arktisk teknologi.[128]

---

[121] Unit omfattes også av styringsmodellen for informasjonssikkerhet og personvern i UH-sektoren. Kartleggingen av Units arbeid med informasjonssikkerhet og personvern utføres av Kunnskapsdepartementet.

[122] NFR årsrapport 2019, side 19.

[123] Se https://www.unis.no/unis-annual-report-2019/.

[124] NFR årsrapport 2019, side 10.

[125] NFR årsrapport 2019, side 21.

[126] NOKUT årsrapport 2019, side 35.

[127] NOKUT årsrapport 2019, side 10.

[129] Se «Temarapport 2020: Tjenesteutsetting av digitale systemer og tjenester» (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

DIGITALE VERDIER OG TREDJEPARTER
I kapittel 1 så vi at en stor og økende andel av universitetenes og høgskolenes digitale verdier er satt ut til og driftes av tredjeparter, enten kommersielle selskaper (norske og utenlandske) eller aktører i offentlig sektor. Direktoratene og selskapene opplyste om den samme trenden – digitale verdier flyttes fra egen kjeller til tredjeparter.

Tre virksomheter rapporterte at i 2020 skjer 90-100 prosent av deres databehandling ved hjelp av tredjeparter. For en annen virksomhet dreier seg om ca. 60 prosent. To øvrige virksomheter mente at det handler om en forholdsvis liten andel av den totale databehandlingen, henholdsvis 20 prosent og 5 prosent. Den ene av disse virksomhetene opplyste om at omfanget av ekstern drift vil øke til omkring 95 prosent i 2021.

De to siste virksomhetene mente at omfanget av ekstern databehandling er «stor» eller «økende».[129]

Det betyr at også for direktoratene og selskapene forvaltes stadig flere digitale ressurser i verdikjeder bestående av mange ulike eksterne aktører.

PERSONALRESSURSER

Det samlede antallet årsverk øremerket til informasjons-sikkerhets- og personvernarbeidet hos de ni virksomhetene har økt noe i 2020. Personvernombudene utgjør omkring 25 prosent av det samlede årsverksantallet.

Én av virksomhetene rapporterte ikke om øremerkede årsverk til dette arbeidet. Her ble det opplyst om at fremtidige ressursbehov er under vurdering.

Sju av ni virksomheter hadde utpekt personvernombud. De to virksomhetene som ikke hadde personvernombud, mente enten at de ikke har plikt til det eller at spørsmålet om ombud er noe de vil utrede nærmere.
Hos flere av virksomhetene er det ikke knyttet en fast stillingsprosent til ombudsrollen. Ombudsoppgavene er derfor noe som kom i tillegg til disse medarbeidernes ordinære arbeidsoppgaver. To virksomheter har engasjert et eksternt personvernombud.

De resterende årsverkene er i hovedsak knyttet til IT-avdelingene og arbeidet med IT-sikkerhet. Hos enkelte virksomheter ble det i tillegg opplyst om ansatte med juridisk bakgrunn som i noen grad jobbet med etterlevelse av personvernregelverket. Det vanligste er likevel at GDPR-arbeidet foregår i regi av personvernombudene.

UØNSKEDE HENDELSER OG AVVIK

Alle direktoratene og selskapene opplyste om at de har vært utsatt for to eller flere uønskede hendelser eller avvik i 2019-2020. Til sammen ble det rapportert om 95 uønskede informasjonssikkerhets- og personvernhendelser og -avvik. Dette er en dobling sammenliknet med 2018-19. Da var det totalt antall rapporterte hendelser og avvik 42.

Én av virksomhetene opplyste om klart flere uønskede hendelser og avvik enn de øvrige (52). Men selv om vi holder denne virksomheten utenfor, er det samlede antallet hendelser og avvik høyere enn det som ble rapportert i 2018-19.

HENDELSESPROFILEN
88 av de uønskede hendelsene gjelder brudd eller nesten-brudd på informasjonssikkerheten og avvik fra virksomhetenes egne sikkerhetsrutiner. Dette tallet inkluderer brudd på personopplysningssikkerheten.
De fleste av de 88 hendelsene handlet om avvik fra egne rutiner snarere enn om reelle sikkerhetsbrudd eller personvernkrenkelser.

I tillegg ble det rapportert om sju avvik fra andre rutiner for behandling av personopplysninger, det vil si rutiner som ikke gjelder sikring av slike opplysninger. Disse sakene handler primært om manglende registrering eller sletting av personopplysninger. Det ble også rapportert om ett tilfelle av manglende anonymisering av personopplysninger.

Sju virksomheter oppga at de hadde vært utsatt for én eller flere hendelser som kan kategoriseres som utilsiktede feil og uhell (menneskelige eller tekniske). De vanligste hendelsene gjelder også her avvik, spesielt feil i tilgangs-styringen, manglende tilgangsstyring eller nedetid på tjenester driftet av tredjeparter. Feil førte også til at personopplysninger ble publisert online.

[128] Se UNIS Strategy 2025 (https://www.unis.no/wp-content/uploads/2019/04/UNIS_Strategy_2025_web.pdf).

Det ble i tillegg rapportert om enkelte andre typer avvik: manglende sikkerhetsoppdatering av programvare og mangelfulle rutiner for sikker behandling av personopplysninger.

Fire virksomheter oppga at de hadde vært utsatt for tilsiktede hendelser hvor økonomisk vinning er det sannsynlige motivet (nettkriminalitet). Dette dreier seg i første rekke om forsøk på faktura- og direktørsvindel og kompromitterte brukerkontoer (brukt til masseutsendelse av epost). Det ble rapportert om ett tilfelle av datainntrenging og enkelte mislykkede forsøk på dette.

Ingen av virksomhetene oppga at de har vært utsatt for løsepengevirusangrep eller sikkerhetsbrudd på grunn av annen type skadevare, for eksempel misbruk av dataressurser til utvinning av kryptovaluta. Det ble ikke opplyst om tjenestenektangrep. Heller ikke i 2018-19 ble det opplyst om alvorlige hendelser med løsepengevirus, tjenestenekt eller kryptovalutautvinning.

I motsetning til i 2018-19, ble det ikke rapportert om mistanker om statlig eller statsstøttet dataspionasje/kunnskapstyveri (APT-hendelser).

SKADEVIRKNINGER

Virksomhetene mente at hendelsene og avvikene ikke hadde medført vesentlige skadevirkninger. Det innebærer for eksempel at faktura- og direktørsvindel ikke har ført til urettmessige utbetalinger.

I forbindelse med hendelsene som gjelder feilaktig publisering av personopplysninger online, er det imidlertid snakk om mindre krenkelser av personvernet. Her dreier det seg om relativt små mengder personopplysninger og ikke om særlige kategorier opplysninger. Det forekom tilsvarende krenkelser av personvernet i forbindelse med feil tilgangsstyring.

Ut over dette ble skadevirkningene definert som ekstraarbeid og noe tapt arbeidstid.

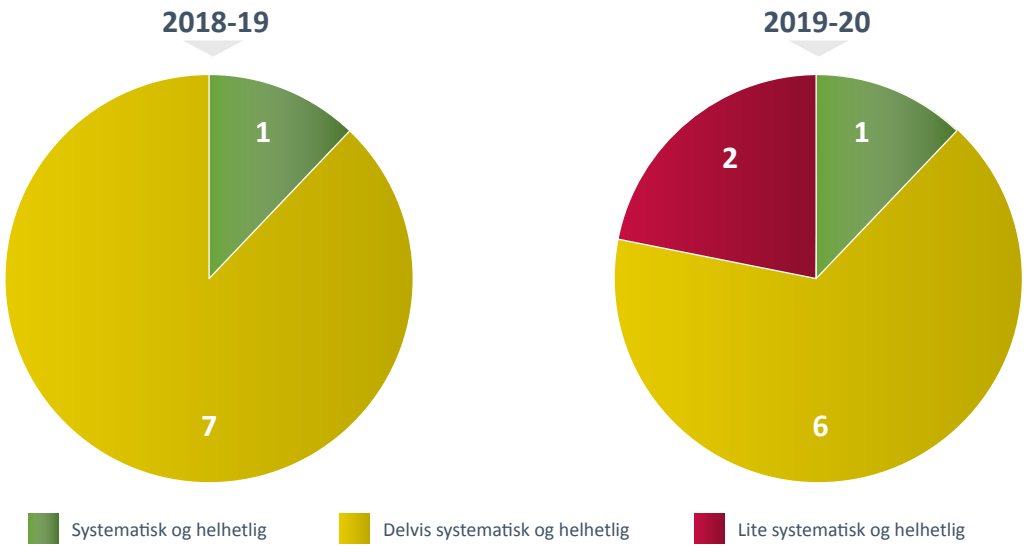
LEDELSESSYSTEMER FOR INFORMASJONSSIKKERHET OG INTERNKONTROLL FOR GDPR

Ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR skal bidra til at uønskede informasjonssikkerhets- og personvernhendelser forebygges, eller at slike hendelser oppdages, håndteres og normal driftstilstand gjenopprettes.

I kartleggingen ble direktoratene og selskapene spurt om status for arbeidet med ledelsessystemer og internkontroll.

Figuren nedenfor gir en oversikt over status for dette arbeidet i 2018-19 og 2019-20.

Figur 8: Status for arbeidet med informasjonssikkerhet og personvern, 2018-19 og 2019-20



Figuren viser at i 2018-19 opplyste én av virksomhetene om at det var etablert et systematisk og helhetlig arbeid med informasjonssikkerhet og personvern, det vil si at både ledelsessystemet for informasjonssikkerhet og internkontrollen for GDPR var utarbeidet og ble praktisert i virksomheten (markert som grønn).

Sju virksomheter opplyste om at de var i ferd med å utvikle et slikt arbeid, men at det fortsatt gjensto enkelte avvik som måtte lukkes (markert som gule).

Ingen av virksomhetene rapporterte om at status for arbeidet var at det ikke hadde begynt eller at det det var i startfasen.

Ved kartleggingen i 2019-20 har dette bildet endret seg noe. Det er fortsatt én virksomhet som har etablert et systematisk og helhetlig informasjonssikkerhets- og personvernarbeid (markert som grønn). I tillegg var det seks virksomheter som delvis har etablert et systematisk og helhetlig arbeid (markert som gule).

Til slutt er det to virksomheter som rapporterte at de enten ikke har kommet særlig langt i dette arbeidet, eventuelt at arbeidet med informasjonssikkerhet og personvern er preget av tilbakeslag (markert som røde). Årsakene til dette ble oppgitt å være at arbeidet ikke ble prioritert i det foregående året og avgang av ressurspersoner med sentrale roller i arbeidet.

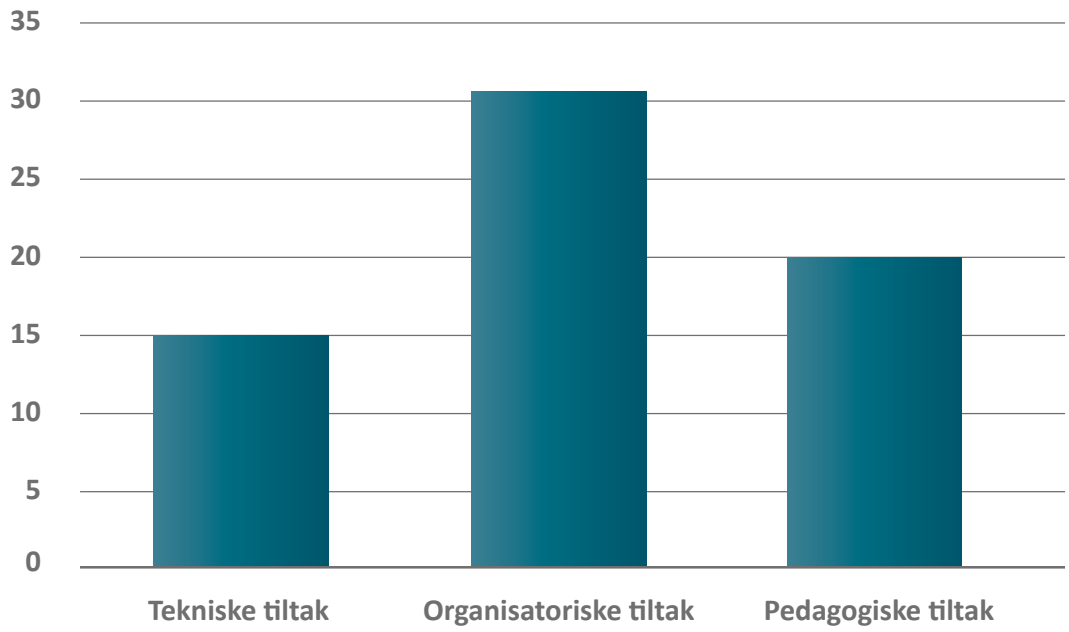
Begge virksomhetene har iverksatt tiltak for å rette på avvikene.

TILTAK OG TILTAKSPROFIL

Direktoratene og selskapene ble bedt om å gjøre rede for viktige tiltak i 2019-2020 for å styrke informasjonssikkerheten og personvernet, inkludert arbeidet med ledelsessystemer og internkontroll for GDPR.

Figuren nedenfor gir en samlet oversikt over hovedtyper tiltak som det ble opplyst om.

Figur 9: Rapporterte informasjonssikkerhets- og personverntiltak, 2019-20



Figuren viser at direktoratene og selskapene samlet sett iverksatte eller gjennomførte 66 informasjonssikkerhets- eller personverntiltak i 2019-20. Organisatoriske initiativ var den hyppigst forekommende tiltakstypen, fulgt av pedagogiske og tekniske tiltak.

TILTAKSPROFIL
Tiltaksprofilen varierte noe mellom virksomhetene. De fleste har iverksatt eller gjennomført ett eller flere tiltak innenfor hver av de tre tiltakskategoriene i figur 9.

Enkelte virksomheter rapporterte om at det ikke ble gjennomført tekniske eller pedagogiske tiltak i 2019-20. Disse virksomhetene har i større grad enn de øvrige vektlagt organisatoriske tiltak. Eksempler på dette er etablering av ny rutine for sikkerhetsoppdateringer og utarbeidelse av rutiner for behandling av personopplysninger i forvaltningsprosesser.

Andre virksomheter har fokusert spesielt på tekniske tiltak. Det omfatter blant annet tiltak for å oppdage uønsket nettverksaktivitet og etablering av nye løsninger for ekstern lagring av sikkerhetskopi.

Til sist er det virksomheter som opplyste om at de har jobbet mest med pedagogiske tiltak. Dette handler primært om opplæring av og informasjon til egne brukere. Det inkluderer også øvelser på håndtering av uønskede informasjonssikkerhets- eller personvernhendelser.

SYSTEMATIKK OG TILTAK
Ovenfor har vi sett at én av direktoratene og selskapene opplyste om at det er etablert et systematisk og helhetlig informasjonssikkerhets- og personvernarbeid. Det betyr at tiltakene som de øvrige virksomhetene rapporterte om i 2019-20 i varierende grad har skjedd innenfor rammen av et strukturert informasjonssikkerhets- og personvernarbeid.

Hos flere av disse virksomhetene fremsto derfor deler av tiltaksaktiviteten som noe ad hoc.

SÅRBARHETER

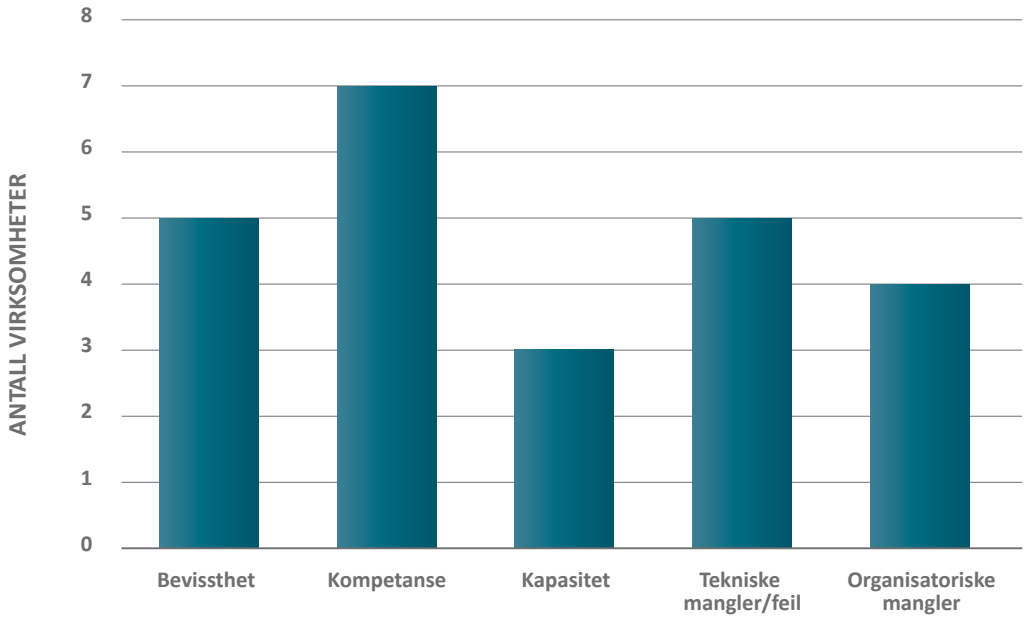
Tiltakene drøftet ovenfor er ment å utbedre sårbarheter. Direktoratene og selskapene ble derfor bedt om å gjøre rede for hvilke sårbarheter de har behov for å gjøre noe med.

Tabellen nedenfor gir en samlet oversikt over kategorier sårbarheter som virksomhetene rapporterte om. Ettersom hver virksomhet kunne oppgi flere ulike typer sårbarheter, viser stolpene i tabellen antallet virksomheter som mener at de ulike sårbarhetskategoriene representerer viktige utfordringer for dem.

Figuren viser at manglende informasjonssikkerhets- og personvernkompetanse er den sårbarheten som oppgis av flest virksomheter. Deretter følger brukerbevissthet, tekniske mangler, organisatoriske mangler og kapasitet/ressurser.

Kompetanse handler dels om manglende kunnskap om informasjonssikkerhet og personvern blant virksomhetenes sluttbrukere. Men det handler også om tilsvarende mangler hos medarbeidere som er ment å spille sentrale roller i arbeidet med informasjonssikkerhet og personvern, spesielt system- eller tjenesteeiere/tjenesteansvarlige. Det ble i liten grad nevnt at IT-medarbeidere kan ha behov for å styrke egen kompetanse med hensyn til informasjonssikkerhet og personvern.

Figur 10: Sårbarheter i arbeidet med informasjonssikkerhet og personvern, 2019-20



Brukerbevissthet handler primært om liten oppmerksomhet om problemstillinger knyttet til informasjonssikkerhet og personvern. Det gjelder for eksempel grunnleggende forståelse for hva informasjonssikkerhet og personvern handler om og manglende risikoerkjennelse, for eksempel hvordan uønskede hendelser og avvik kan skje og hvilke skadevirkninger dette kan medføre.

Tekniske mangler dreier seg blant annet om bekymringer knyttet til ustabil tilgang til IT-systemer eller digitale tjenester, manglende sikkerhet på personlig/privat IT-utstyr, feil hos tjenesteleverandører og «teknisk gjeld» (utdaterte applikasjoner eller operativsystemer).

Organisatoriske mangler handler i all hovedsak om uklare ansvars- og oppgavefordeling eller manglende retningslinjer/rutiner for lovlig og sikker behandling av personopplysninger.

Med kapasitetsmangler siktes det til at omfanget av personalinnsatsen ikke står i et rimelig forhold til utfordringsbildet og oppgavemengden.

I tillegg er det også i denne delen av sektoren en gjennomgående sårbarhet at det ikke er utarbeidet eller ferdigstilt planverk for håndtering av og videre drift ved alvorlige informasjonssikkerhets- og personvernhendelser.

SÅRBARHETSPROFIL

Som når det gjelder tiltak, har de forskjellige virksomhetene noe ulik sårbarhetsprofil.

Ingen av virksomhetene oppgir at de har vesentlige sårbarheter innenfor alle fem sårbarhetskategorier i figuren ovenfor. Motsatt er det heller ingen virksomheter som oppgir at de ikke har noen sårbarheter.

Virksomhetene skiller lag når det gjelder hvor mange og hvilke typer sårbarheter de oppgir at de har. Tre virksomheter opplyste for eksempel om vesentlige sårbarheter innenfor fire av de fem kategoriene. Ytterligere tre virksomheter opplyste om sårbarheter innenfor tre kategorier. Én virksomhet mente at den bare har vesentlige sårbarheter innenfor én av kategoriene.

Profilvariasjonene avspeiler ikke nødvendigvis forskjeller i kvaliteten på arbeidet med informasjonssikkerhet og personvern (de som oppgir få sårbarheter er bedre enn de som oppgir mange). Variasjonene avspeiler trolig andre forskjeller mellom virksomhetene, for eksempel knyttet til størrelse, oppgaver, organisering og system-/tjeneste-portefølje (teknisk kompleksitet).

SÅRBARHETER OG TILTAK

Dersom vi sammenlikner de tiltak og sårbarheter som virksomhetene rapporterte om i 2019-20, ser vi at pedagogiske sårbarheter (bevissthet og kompetanse) rapporteres av klart flest virksomheter. Deretter følger tekniske og organisatoriske sårbarheter. Likevel rapporterte virksomhetene om at det ble gjennomført flest organisatoriske tiltak, nest flest pedagogiske tiltak og færrest tekniske tiltak.

Dette indikerer et visst misforhold mellom rapporterte sårbarheter og iverksatte tiltak. Det betyr at det kan være rom for å styrke systematikken i informasjonssikkerhets- og personvernarbeidet.

KAPITTEL 5

VURDERINGER OG ANBEFALINGER

VURDERINGER OG ANBEFALINGER

INNLEDNING

I dette kapitlet følger først en vurdering av sannsynligheten for at sektoren i løpet av 2021 skal oppnå kravene som departementet stiller til informasjonssikkerhet og personvern.[130] På bakgrunn av disse vurderingene, vil vi også vurdere om målene for arbeidet med informasjonssikkerhet og personvern i sektorens digitaliseringsstrategi[131] kan oppnås før utgangen av strategiperioden (2021).

Deretter følger en overordnet vurdering av risiko knyttet til uønskede hendelser eller avvik som vi mener sektoren bør være særlig oppmerksomme på i 2021. Rammeverket som ble benyttet beskrives i vedlegg 4.

Vurderingene av både sannsynlighet og risiko bygger på funnene fra årets kartlegging, se kapitlene 1-4. Vurderingene av risiko er i tillegg basert på virksomhetenes egne vurderinger av hvilke hendelser eller avvik de er mest bekymret for.

Avslutningsvis gis enkelte anbefalinger om hvilke tiltak som kan iverksettes på sektornivå for å håndtere risikoen og styrke etterlevelsen av departementets policy.

SANNSYNLIGHET FOR ETTERLEVELSE AV POLICYEN

Departementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning inneholder 12 hovedpunkter. Punktene oppsummerer de rettslige forpliktelser som gjelder for UH-sektorens arbeid med informasjonssikkerhet og personvern.

OM SANNSYNLIGHETSVURDERINGENE

Vi har tatt utgangspunkt i sannsynlighetsverdiene som PST anvender i sine årlige trusselvurderinger når vi har vurdert sannsynlighet for etterlevelse av kravene i departementets policy. Det innebærer at vi benytter følgende sannsynlighetsverdier:

- **Meget sannsynlig:** det er meget god grunn til å forvente at sektoren vil kunne overholde kravene i policyen ved utgangen av 2021 (mer enn 90 prosent sannsynlighet).
- **Sannsynlig:** det er grunn til å forvente at sektoren vil kunne overholde kravene i policyen ved utgangen av 2021 (mellom 60 og 90 prosent sannsynlighet).
- **Mulig:** det er like sannsynlig som usannsynlig at sektoren vil kunne overholde kravene i policyen ved utgangen av 2021 (mellom 40 og 60 prosent sannsynlighet).
- **Lite sannsynlig:** det er liten grunn til å forvente at sektoren vil kunne overholde kravene i policyen ved utgangen av 2021 (mellom 10 og 40 prosent sannsynlighet).
- **Svært lite sannsynlig:** det er svært liten grunn til å forvente at sektoren vil kunne overholde kravene i policyen ved utgangen av 2021 (mindre enn 10 prosent sannsynlig).

Sannsynlighetsvurderingene er en prognose for arbeidet med informasjonssikkerhet og personvern i 2021. Den estimerte utviklingen (prognosen) gjøres med grunnlag i 2020-tilstanden i sektoren, jf. foregående kapitler.

[130] Kravene er kommunisert til sektoren i rundskriv F-04-20. Se https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning.

[131] Digitaliseringsstrategi for universitets- og høyskolesektoren 2017-2021, se https://www.regjeringen.no/contentassets/779c0783ffee461b88451b9ab71d5f51/no/pdfs/digitaliseringsstrategi-for-universitets--og-hoysk.pdf. Ny digitaliseringsstrategi for UH-sektoren vil bli fastsatt i løpet av 2021.

Policyen stiller krav om systematikk og helhet, det vil si at det innføres ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR. Når disse kvalitetssystemene er innført og praktiseres på en tilfredsstillende måte, vil det være etablert et bærekraftig grunnlag for kontinuerlig forbedring av informasjonssikkerheten og personvernet.

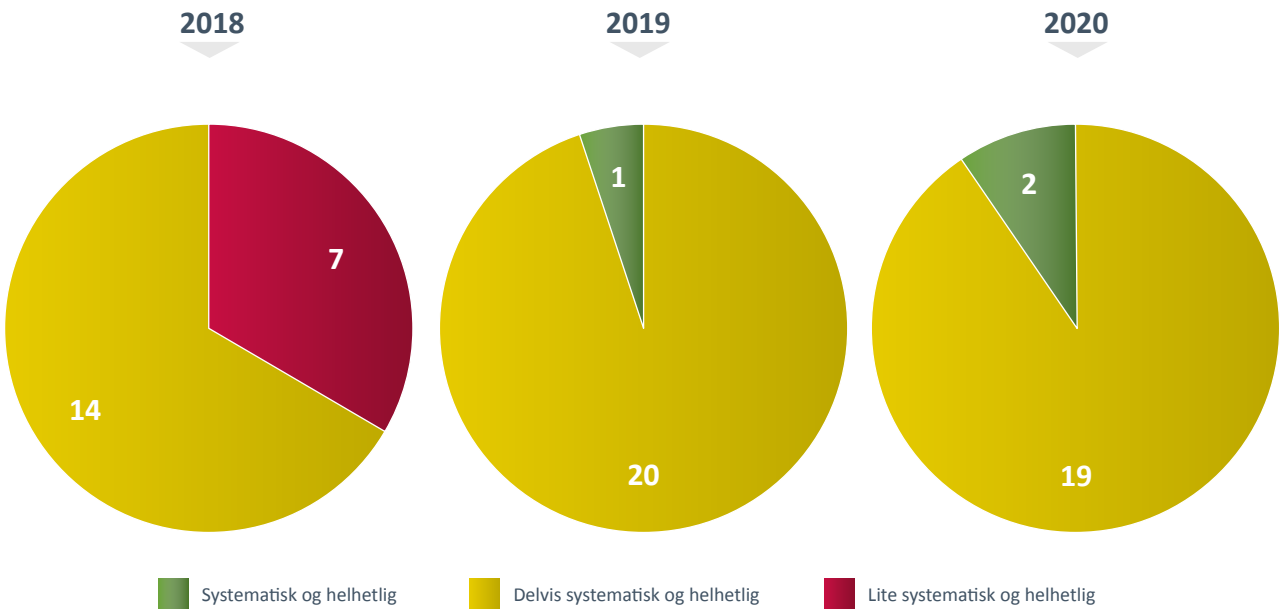
I tillegg inneholder policyen mer detaljerte krav til de viktigste aktivitetene som inngår i slike kvalitetssystemer, for eksempel oversikt over digitale verdier, forebygging og risikostyring, hendelseshåndtering og kontinuitet, leverandørkontroll, personvernrettigheter og grunnkrav til behandling av personopplysninger, kompetanseheving og dokumentasjon.

ETTERLEVELSE – UNIVERSITETER OG HØGSKOLER

Vår overordnede vurdering er at det er svært lite sannsynlig at samtlige universiteter og høgskoler som omfattes av departementets styringsmodell vil overholde kravene i policyen for informasjonssikkerhet og personvern i løpet av 2021.

Figur 11 nedenfor viser imidlertid at sektoren har gjort viktige fremskritt fra 2018 til 2020. Samtidig indikerer den at det totalt sett gjenstår for mange avvik fra kravene i policyen til at det kan forventes at alle er lukket ved utgangen av inneværende år.

Figur 11: Endringer i arbeidet med informasjonssikkerhet og personvern hos universitetene og høgskolene, 2018-2020



Som figuren viser, har den største fremgangen i universitetenes og høgskolenes arbeid med informasjonssikkerhet og personvern skjedd fra 2018 til 2019. Likevel har denne delen av sektoren beveget seg i riktig retning også i 2020 – flere av virksomhetene har i noen grad eller i vesentlig grad styrket sin etterlevelse av departementets policy. Vi mener imidlertid at det er urealistisk å anta at de 19 virksomhetene som i 2020 er markert som «gule» vil skifte status til «grønne» i 2021.

Nedenfor utdyper vi hvilken utvikling vi mener det er realistisk å forvente i 2021.

MEGET SANNSYNLIG

To virksomheter har etablert et bærekraftig grunnlag for kontinuerlig forbedring av arbeidet med informasjonssikkerhet og personvern. Det betyr at de har innført og praktiserer hovedaktivitetene i ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR på tilfredsstillende måter.

Vi mener det er meget sannsynlig at disse virksomhetene vil forsterke dette arbeidet i 2021. De vil dermed styrke sin overholdelse av kravene i departementets policy, og bør derfor kunne beholde og befeste sin status som «grønne» virksomheter.

SANNSYNLIG
Ytterligere én virksomhet har jobbet godt og målrettet med informasjonssikkerhet og personvern over flere år, både på organisatorisk og teknisk side.

Vi mener det er sannsynlig at denne virksomheten kan etablere et bærekraftig grunnlag for kontinuerlig forbedring og overholde kravene i departementets policy i 2021. Slik vi ser det, bør denne virksomheten derfor ha gode muligheter til å endre status fra «gul» til «grønn» i inneværende år.

MULIG
Fire virksomheter har siden 2018 rapportert om jevn fremgang i arbeidet med innføring og praktisering av ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR. Disse virksomhetene har også økt ressursinnsatsen i løpet av de tre siste årene.

Vår vurdering er at det er mulig for disse virksomhetene å overholde kravene i departementets policy på tilfredsstillende måter i 2021. De vil i så fall endre status fra «gule» til «grønne» virksomheter.

LITE SANNSYNLIG
Når det gjelder sju av virksomhetene mener vi det er lite sannsynlig at de i løpet av 2021 vil kunne overholde kravene i departementets policy på tilfredsstillende måter. Flere av disse virksomhetene rapporterte imidlertid om god fremgang i 2020.

Vår vurdering er likevel at det gjenstår noe arbeid før det er etablert et bærekraftig grunnlag for kontinuerlig forbedring, det vil si at ledelsessystemer for informasjonssikkerhet og/eller internkontrollen for GDPR er tilfredsstillende innført og praktisert. Vi tror derfor ikke det er realistisk at disse virksomhetene skal skifte status fra «gult» til «grønt» i 2021.

SVÆRT LITE SANNSYNLIG
De siste sju virksomhetene opplyste om begrenset fremgang i 2020, delvis fordi knappe ressurser har blitt omprioritert til håndtering av korona-situasjonen. Flere av disse virksomhetene har derfor fått et etterslep i arbeidet med informasjonssikkerhet og personvern. Enkelte av virksomhetene opplyste om at de har iverksatt eller planlegger tiltak som vil gi arbeidet et tiltrengt løft.

Alt i alt mener vi at det er svært lite sannsynlig at de sju siste virksomhetene vil kunne overholde kravene i departementets policy i 2021. Hos enkelte av virksomhetene kan det virke som at fremgangen har flatet noe ut – nådd et platå – og at det kan være utfordrende å komme videre.

ETTERLEVELSE – DIREKTORATER OG SELSKAPER

Fra 2019 til 2020 har de ni direktoratene og selskapene samlet sett ikke gjort vesentlige fremskritt i arbeidet med informasjonssikkerhet og personvern. Vår overordnede vurdering er derfor at det er svært lite sannsynlig at alle direktorater og selskaper vil overholde kravene i departementets policy allerede i 2021.

Gjennomgangen i kapittel 4 viste likevel at én virksomhet rapporterte om et systematisk og helhetlig informasjonssikkerhets- og personvernarbeid. Vår vurdering er at denne virksomheten overholder kravene i departementets policy på en tilfredsstillende måte.

Ytterligere én virksomhet har prioritert informasjonssikkerhet og personvern høyt de siste årene. Vi mener det er sannsynlig at denne virksomheten kan lykkes med å ivareta kravene i policyen allerede i inneværende år.

Tre virksomheter rapporterte ikke om vesentlig fremgang i arbeidet med informasjonssikkerhet og personvern i 2020. Disse virksomhetene er likevel i ferd med å gjennomføre tiltak som trolig vil gi arbeidet større fremdrift i 2021. På denne bakgrunn mener vi det kan være mulig for de tre virksomhetene å ivareta kravene i policyen på tilfredsstillende måter i løpet av inneværende år.

Tre andre virksomheter rapporterte om at arbeidet med informasjonssikkerhet og personvern enten ikke ble tilfredsstillende prioritert i 2020 eller at de mangler erfaring med ledelsessystemer og internkontroll. Vi mener det er lite sannsynlig at disse virksomhetene vil forbedre seg nok i 2021 til å etterleve kravene i departementets policy.

Én virksomhet påbegynte arbeidet med overholdelse av de rettslige kravene oppsummert i departementets policy i siste halvdel av 2020. Vi anser det som svært lite sannsynlig at virksomheten vil kunne ivareta alle kravene i policyen i løpet av 2021.

ETTERLEVELSE – OPPSUMMERT

Samlet sett innebærer vurderingene ovenfor følgende:

- Tre virksomheter ivaretar kravene i departementets policy på en tilfredsstillende måte. Disse har etablert et bærekraftig grunnlag for kontinuerlig forbedring, det vil si at de har innført og praktiserer ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR på tilfredsstillende måter.

- Ni virksomheter har satt seg selv i en posisjon hvor det er sannsynlig eller mulig at de kan gjøre det samme i løpet av inneværende år. Vi tror ikke det er realistisk å forvente at alle ni vil lykkes med å overholde policyens krav i 2021.

- For 10 virksomheter mener vi det er lite sannsynlig at de vil overholde policyens krav på tilfredsstillende måter allerede i 2021. Flere av disse virksomhetene har imidlertid vist god fremgang i 2020.

- For åtte virksomheter mener vi det er svært lite sannsynlig at de vil forbedre seg nok til å overholde kravene i policyen ved utgangen av 2021.

Det betyr at 12 av 30 virksomheter ivaretar allerede policyens krav eller er i posisjon til å kunne gjøre det i 2021.

Samtidig er det behov for forbedringer hos 18 av 30 virksomheter. Dette er virksomheter hvor tilfredsstillende overholdelse av policyen i 2021 vurderes som lite eller svært lite sannsynlig.

MÅLOPPNÅELSE – VURDERING

Gjeldende digitaliseringsstrategi for universitets- og høgskolesektoren inneholder fire hovedmål for arbeidet med informasjonssikkerhet og personvern:

1. Virksomhetene skal etablere helhetlig styring og ledelse av arbeidet med informasjonssikkerhet og personvern.

2. Virksomhetenes arbeid med styrking av informasjonssikkerheten og personvernet skal være systematisk.

3. Nivået på informasjonssikkerheten og personvernet skal være høyere enn de nasjonale minstekravene (blant annet rettslige krav).

4. Studenter og ansatte skal bevisstgjøres problemstillinger knyttet til informasjonssikkerhet og personvern.

De tre første målsettingene avhenger av at virksomhetene har innført og praktiserer ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR. Arbeidet skal være bærekraftig over tid og føre til kontinuerlig forbedring.

Ovenfor har vi sett at vi mener det er lite eller svært lite sannsynlig at 18 av 30 virksomheter vil være i stand til å oppnå dette før strategiperiodens utløp (2021). Vår vurdering er derfor at de tre første målsettingene ikke vil oppnås.

Vi mener imidlertid at det er iverksatt mange viktige bevisstgjøringstiltak i sektoren, dels rettet mot ansatte og dels mot studenter. Virksomhetene opplyser også om økt bevissthet om informasjonssikkerhet og personvern, blant annet at de mottar flere henvendelser og spørsmål om dette.

Vi mener derfor at bevisstheten blant ansatte og studenter er styrket. Det betyr at målsetting fire vil bli realisert.

RISIKO – OVERORDNET VURDERING

Forbedringene i sektoren fra 2018 innebærer at sårbarhetene er færre enn tidligere. Isolert sett tilsier færre sårbarheter lavere risiko for uønskede hendelser og avvik. Men risiko påvirkes også av to andre forhold: sektorens avhengighet av digitale verdier og de trusler som sektorens digitale verdier står overfor. Når vi tar hensyn til disse to forholdene kan risikoen øke selv om arbeidet med å utbedre sårbarheter er forbedret.

Vi mener at en liknende dynamikk har preget utviklingen i 2020 – trusselbildet ser ut til å ha skjerpet seg mer enn sektorens arbeid med utbedring av sårbarheter. Med bakgrunn i endringene i trusselbildet, diskutert i kapittel 3 og 4, mener vi derfor at risikoen for uønskede hendelser og avvik er noe større i 2021 enn i 2020.

Vi begrunner dette med følgende tendenser og observasjoner:

- Det nasjonale trusselbilde virker å være mer utfordrende. Flere virksomheter i ulike sektorer og bransjer har vært utsatt for alvorlige digitale sikkerhetshendelser i 2020 enn i 2018-19.

- Dobling i det totale antallet hendelser og avvik hos direktoratene og selskapene fra 2019 til 2020. Hos universitetene og høgskolene har det totale antallet rapporterte hendelser og avvik vært forholdsvis stabilt.

- Flere virksomheter i UH-sektoren har vært utsatt for alvorlige eller potensielt alvorlige digitale sikkerhetshendelser i 2020 enn tidligere.
- Noen flere tilfeller av datainntrengning hvor det mistenkes at statlige eller statsstøttede hackergrupper (APT) står bak.
- Oppdagelsestiden – antall dager fra første indikasjon på kompromittering av datanettverket til hendelsen oppdages – er i noen tilfeller lengre enn hva vi har sett tidligere.
- Reparasjonstiden – antall dager fra hendelsen oppdages til normal tilstand er gjenopprettet – er i enkelte tilfeller lengre enn hva vi har sett tidligere.
- Flere tilfeller av at sårbarheter i digitale løsninger har blitt utnyttet av trusselaktører, eller sårbarheter har medført økt risiko for uønskede hendelser.
- Dobling i antallet hendelser og avvik som universitetene og høgskolene meldte til Datatilsynet i 2020 sammenliknet med 2019.
- Nasjonale sikkerhetsmyndigheter, spesielt NSM, mener at norsk forskning er mål for APT-grupper. Ulovlig kunnskapsoverføring fremheves som en særlig utfordring.

Samtidig ser vi at virksomheter som utsettes for alvorlige eller potensielt alvorlige hendelser eller avvik har vilje til å iverksette kraftfulle tiltak – både kort- og langsiktige forbedringer.

RISIKO FOR UØNSKEDE HENDELSER

Nedenfor følger en vurdering av risiko for de vanligste informasjonssikkerhets- og personvernhendelsene diskutert i kapittel 3.

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

SKADEVARE, SPESIELT LØSEPENGEVIRUS – HØY RISIKO
Risikoen for skadevarehendelser, særlig større løsepengevirusangrep, ble i fjorårets rapport vurdert som middels. Det ble begrunnet med at antallet slike hendelser i UH-sektoren spesielt og i Norge var lavt i 2019. Heller ikke i år rapporterte virksomheter i UH-sektoren om alvorlige hendelser med løsepengevirus.

I det siste året har vi imidlertid sett at flere norske virksomheter er blitt utsatt for større løsepengevirusangrep, jf. kapittel 3. Trusselen har derfor kommet nærmere UH-sektoren samtidig som skadevirkningene er de samme, blant annet tjenesteavbrudd, omdømmetap og personvernkrenkelser.

Skadevare, særlig løsepengevirus, er også den trusselen som flest virksomheter uttrykte bekymring for i årets kartlegging. I tillegg ble trusselen som nettkriminelle tjenestemodeller representerer – skadevare-som-en-tjeneste – fremhevet.[132]

Risikoen for skadevare kan reduseres ved innføring av nye sikringstiltak, for eksempel rask innføring av sikkerhetsoppdateringer, bedre kontroll med tjenester som eksponeres mot internettet, totrinnsinnlogging, regelmessig back-up og økt brukerbevissthet om nettfiske. Det ble rapportert om at slike tiltak er gjennomført i 2020. Vi mener likevel det er gode grunner til å heve risikonivået når det gjelder skadevare, spesielt løsepengevirus, fra middels i 2020 til høyt i 2021.[133] Flere norske virksomheter utsettes for løsepengevirusangrep nå enn tidligere, angrepene innebærer stadig oftere dobbel utpressing,[134] de kan i vesentlig grad forringe virksomhetenes evne til å utføre sine kjerneoppgaver og betaling av løsepenger garanterer ikke at alle data gjenopprettes.[135]

KOMPROMITTERTE KONTOER – HØY RISIKO
Risikoen for kompromitterte kontoer ble i fjorårets rapport vurdert som høy. Det ble begrunnet med at kontoer på avveie kan være utgangspunkt for kompromittering av hele eller viktige deler av virksomhetenes datanettverk. Skadevirkningene kan derfor bli alvorlige, både med hensyn til tjenesteavbrudd, personvernkrenkelser, økonomisk tap, tap av omdømme/tillit og skader på nasjonale interesser.

[132] Trusselen fra løsepengevirus blir tatt på stadig større alvor internasjonalt.
Se for eksempel https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

[133] Dette har også skjedd internasjonalt, for eksempel i Storbritannia. Der har det nasjonale cybersikkerhetssenteret (NCSC) nylig advart kunnskapssektoren om at trusselen fra løsepengevirus er økende.
Se https://www.ncsc.gov.uk/files/NCSC-Alert-Further-targeted-ransomware-attacks-education-sector-March-2021.pdf.

[134] Dobbel utpressing betyr at trusselaktører krever penger for å (i) de-kryptere virksomhetens systemer og data/opplysninger og (ii) for ikke å offentliggjøre eller selge data/opplysninger som stjeles før de krypteres.

[135] Ifølge sikkerhetsselskapet Kaspersky, greide ikke 29 prosent av de som ble utsatt for løsepengevirus i 2020 å gjenopprette alle sine data. Dette til tross for at over 50 prosent av alle som ble rammet betalte løsepenger (https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned).

Kompromitterte kontoer er relativt vanlige hendelser i UH-sektoren. I 2020 ble det rapportert om opp mot 300 tilfeller av kontoer på avveie. På den annen side opplyste omkring halvparten av universitetene og høgskolene at de har innført eller planlegger å innføre totrinnsinnlogging for ansatte (og, i noen tilfeller, for studenter). Dette vil redusere risikoen. Likevel mener vi det fortsatt er mange virksomheter som er sårbare for slike hendelser.

Vi anser derfor at det fortsatt er høy risiko knyttet til kompromitterte kontoer. Kompromitterte kontoer var også blant de hendelsene som virksomhetene uttrykte mest bekymring for.

DIREKTØR- OG FAKTURASVINDEL – MIDDELS RISIKO
Risikoen for faktura- og direktørsvindel ble vurdert som høy i fjorårets rapport. Dette ble begrunnet med enkelte større svindelhendelser, og at svindelforsøkene var blitt mer målrettede og troverdige.

Skadevirkningene av faktura- og direktørsvindel trenger ikke å være veldig alvorlige, men kan i enkelte tilfeller medføre betydelige økonomiske tap. Slike hendelser kan også ramme virksomhetenes omdømme/tillit.

I årets kartlegging har vi registrert færre svindelsaker enn i 2019. Det var også relativt få virksomheter som pekte på direktør- eller fakturasvindel som en særskilt bekymring. Uninett CERT har registrert færre tilfeller av slik svindel enn i 2019.

Vi mener derfor at risikoen for direktør- eller fakturasvindel er noe redusert sammenliknet med 2019. Det betyr at risikoen vurderes som middels. Vi mener likevel at dette er en trussel som sektoren fortsatt må ha høy bevissthet om.

UTILSIKTEDE HENDELSER (FEIL OG UHELL) – MIDDELS RISIKO
Risikoen for utilsiktede hendelser eller avvik – menneskelige eller tekniske feil og uhell – ble i fjorårets rapport vurdert som middels til høy. Dette ble begrunnet med at slike hendelser var relativt vanlig og at det ble rapportert om (potensielt) alvorlige skadevirkninger.

Også i 2020 ble det opplyst om forholdsvis mange utilsiktede hendelser. Enkelte av hendelsene ble meldt til Datatilsynet, for eksempel feil publisering av personopplysninger.
Det ble også opplyst om kortere perioder med utilgjengelige tredjeparttjenester. Skadevirkningene knyttet seg særlig til tapt arbeidstid og mulige krenkelser av personvernet.
Det siste gjaldt imidlertid feil eller uhell som rammet få personer (som regel én) og som bare i noen få tilfeller førte til potensiell eksponering av særlige kategorier personopplysninger.

Vi mener at risikoen for utilsiktede hendelser synes å være på omtrent samme nivå som i 2019. Få rapporter om feil eller uhell som førte til vesentlige skadevirkninger fører likevel til at vi justerer risikoen litt ned – fra middels-til-høy til middels.

TJENESTENEKT – LAV RISIKO
I fjorårets rapport ble risikoen for større tjenestenektangrep i UH-sektoren vurdert som lav. Begrunnelsen var at få virksomheter opplyste om at de har vært utsatt for slike angrep. Heller ikke i 2020 ble det rapportert om større tjenestenektangrep. Også Uninett CERT opplyste om at tjenestenekt er noe de sjeldent har observert i UH-sektoren i den senere tid.

Vi mener derfor at risikoen for større hendelser av denne typen fortsatt er lav. Vi mener likevel at sektoren må være oppmerksomme på risikoen for at egne dataressurser kompromitteres og misbrukes i tjenestenektangrep mot andre virksomheter. Denne risikoen er trolig større enn risikoen for selv å bli utsatt for slike angrep.

SÆRSKILT OM APT

Vi vil også i år fremheve at risikoen for APT-hendelser (statlig eller statsstøttet dataspionasje/kunnskapstyveri) trolig er ujevnt fordelt i sektoren – visse virksomheter kan være mer utsatt enn andre. Variasjoner i risiko beror, ifølge nasjonale etterretnings- og sikkerhetstjenester, på faglig profil, for eksempel hvilke typer forskning som bedrives.[136]

Hvert år siden 2018 har det vært rapportert om enkelte bekreftede eller mistenkte APT-hendelser. I 2020 ble det rapportert om noen flere og mer alvorlige tilfeller enn tidligere år. Skadevirkningene av slike hendelser knytter seg særlig til nasjonale interesser, for eksempel ulovlig kunnskapsoverføring, og tap av omdømme/tillit. Slike hendelser kan også medføre økonomiske omkostninger der hvor oppryddingsarbeidet er omfattende.

Vi mener at risikoen kan være høy for virksomheter med en faglig profil eller forvaltningsoppgaver som er interessante for slike aktører. Det kan i første rekke gjelde enkelte av universitetene og noen av direktoratene/selskapene.

For andre deler av sektoren mener vi at risikoen er lav. Det kan imidlertid tenkes at APT/statsaktører benytter seg av kompromitterte dataressurser hos disse virksomhetene i forbindelse med operasjoner rettet mot andre virksomheter i eller utenfor UH-sektoren.

Det kan også tenkes at noen av disse virksomhetene er mål for APT-grupper som opererer mer som nettkriminelle grupper. Dette kan for eksempel være grupper som er ute etter ressurser som alle universiteter og høgskoler forvalter, spesielt vitenskapelige publikasjonsløsninger og bibliotekstjenester.[137]

NETTFISKE

Nettfiske fremheves av virksomhetene selv og Uninett CERT som den viktigste metoden som anvendes ved forsøk på kompromittering av lokale datanettverk. Denne vektoren benyttes både av nettkriminelle og APT-grupper.

Effektivt forsvar mot nettfiske og nettfiskesider vil bidra til å redusere risikoen for flere av hendelsestypene ovenfor, blant annet kompromitterte brukerkontoer, skadevare/løsepengevirus og APT-aktivitet.

FORSLAG TIL OPPFØLGING PÅ SEKTORNIVÅ

På bakgrunn av sannsynlighets- og risikovurderingene ovenfor, ønsker vi å peke på noen sektortiltak som vi mener bør iverksettes. Formålet med tiltakene er å styrke policy-etterlevelsen og å redusere risikoen for hendelser med middels risiko eller høyere.

Vurderingene av etterlevelse og risiko understreker viktigheten av tiltak beskrevet i «Handlingsplan for digitalisering i høyere utdanning og forskning, 2019 til 2021».[138] Tiltakene gjelder etableringen av en rådgivnings- og veiledningstjeneste for informasjonssikkerhet og personvern og initiativ for å heve informasjonssikkerhets- og personvernkompetansen i sektoren. Tiltakene finansieres av programmet for informasjonssikkerhet i universitets- og høgskolesektoren.[139]

Handlingsplanens og programmets tiltak har nå materialisert seg gjennom etableringen av «Cybersikkerhets-senteret for forskning og utdanning».[140] Senteret er lokalisert hos Uninett, og er et samarbeid mellom Uninett, NTNU, UiO og NSD. Fra 1. januar 2021 vil det være en del av Kunnskaps-sektorens tjenesteleveranseorgan.

Vi mener at de tjenester som cybersikkerhetssenteret tilbyr, både med hensyn til digital sikkerhet, kvalitets- og risiko-styring og personvernrett, er viktige og nødvendige sett i lys av vurderingene ovenfor. Tjenestene vil være særlig nyttige for virksomheter hvor utsiktene for tilfredsstillende overholdelse av kravene i departementets policy i 2021 vurderes som lite eller svært lite sannsynlig.

Videre mener at cybersikkerhetssenteret bør utvikle følgende nye tjenester for å redusere risikoen for uønskede hendelser eller avvik og styrke policyetterlevelsen:

[136] Det kan for eksempel gjelde forskningsmiljøer som arbeider med kjernefysikk, fysikk, kjemi, biologi, toksikologi, farmasi, undervanns- og dypvannsteknologi, kontrollsystemer, styringssystemer, autonome fartøy, mønstergjenkjenning (maskinlæring), ingeniørdesign, nanoteknologi, satellitt- og missilteknologi og teknologi tilpasset arktiske forhold.

[137] Se for eksempel https://blog.malwarebytes.com/malwarebytes-news/2020/10/silent-librarian-apt-phishing-attack/ eller https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

[138] Se https://www.unit.no/sites/default/files/media/filer/2019/10/Handlingsplan-digitalisering-2019.pdf.

[139] Se https://www.uninett.no/sikkerhetssatsingen-i-utdanning-og-forskning.

[140] Se https://www.uninett.no/cybersikkerhetssenteret.

- Senteret tilbyr i dag revisjon av virksomhetenes etterlevelse av personvernregelverket (GDPR-revisjon). Senteret bør raskt kunne etablere et tilsvarende tilbud gjeldende informasjonssikkerhet. Et slikt tilbud bør på sikt ikke bare inkludere systemrevisjoner, men også testing av sikringstiltak. Sårbarhetsskanning av IT-sikkerheten i sektoren, som ble utført av Norsk helsenett på bestilling fra cybersikkerhetssenteret, kan være et første steg mot etablering av tjenester for sikkerhetstesting.

- Senteret tilbyr i dag kurs for medarbeidere i sektoren med særlig ansvar for digitale sikkerhet, inkludert lokale hendelseshåndteringsteam (IRT). Det er viktig at dette kurstilbudet styrkes slik at virksomhetene tilføres oppdatert kompetanse innen et fagområde i rask utvikling og hvor truslene er komplekse. Møteplasser i sektoren, spesielt CISO-forum og IRT-chat, ivaretar i dag noe av denne rollen. Mange virksomheter i sektoren har imidlertid pekt på behovet for ytterligere opplæring og kompetanseheving.

- Senteret tilbyr assistanse til planlegging og gjennomføring av IKT-beredskapsøvelser. I forlengelsen av dette tilbudet er det viktig at senteret kan bistå virksomhetene med etablering og revisjon av beredskaps- og kontinuitetsplaner. Vi mener dette er særlig viktig ettersom slike planverk er en gjennomgående mangel i deler av sektoren. Tilstanden har bare i noen grad forbedret seg siden 2018.

Med bakgrunn i enkelte av IT-sikkerhetshendelsene som sektoren har vært utsatt for i 2020, mener vi det er avgjørende at erfaringer fra disse hendelsene kommer hele sektoren til gode. Dette er erfaringer og kompetanse som det også vil være nyttig for sektormyndigheter å ta del i. Cybersikkerhetssenteret bør derfor systematisere og formidle erfaringer fra slike hendelser. Formidlingen bør tilpasses ulike målgrupper i sektoren, både operativt personell og ledere.

Videre bør Direktoratet for høyere utdanning og kompetanse benytte erfaringer fra håndtering av nevnte IT-sikkerhetshendelser til evaluering og eventuelt forbedring av rammeverket for håndtering av alvorlige IKT-sikkerhetshendelser i UH-sektoren.[141] Det bør gis tilbud til virksomhetene i sektoren om anskaffelse av VDI-sensor.

Cybersikkerhetssenteret bør utarbeide og formidle beste praksis med hensyn til håndtering av IT-sikkerhetshendelser. I samarbeid med Direktoratet for høyere utdanning og kompetanse, bør senteret også etablere et felles rammeverk for kategorisering av uønskede hendelser og avvik. Rammeverket bør kunne brukes av virksomheter uten spesialistmiljøer innen informasjonssikkerhet, inkludert digital sikkerhet, og personvern.

OPPFØLGING AV DEN ENKELTE VIRKSOMHET

Alle virksomheter har også i år mottatt brev fra Unit med anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern.

Den viktigste og vanligste anbefalingen er at virksomhetene styrker systematikken og bærekraften i eget arbeid med informasjonssikkerhet og personvern. I dette ligger at virksomhetene fullfører innføringen av ledelsessystemer for informasjonssikkerhet og internkontroll for personvern (GDPR). Det inkluderer også kompetanseheving for ansatte som er ment å ha sentrale roller i informasjonssikkerhets- og personvernarbeidet.

I tillegg ble det gitt tre andre gjennomgående anbefalinger:

- Styrke risikostyringen på informasjonssikkerhets- og personvernområdet.

- Utarbeide en plan for håndtering av og videre drift ved alvorlige informasjonssikkerhets- eller personvernhendelser.

- Gjennomføre øvelser på håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser.

Funnene fra årets kartlegging følges opp av departementet i styringsdialogen med den enkelte virksomhet.

[141] Se https://www.unit.no/rammeverk-handtering-av-ikt-sikkerhetshendelser-i-uh-sektoren.

VEDLEGG 1: DATAGRUNNLAGET OG ARBEIDET MED RAPPORTEN

Denne rapporten bygger primært på informasjon innhentet gjennom kartleggingsmøter i sektoren. Slike møter ble gjennomført med hver av de 21 statlig eide universitetene og høgskolene, og de ni direktorater og selskaper som omfattes av styringsmodellen for informasjonssikkerhet og personvern i UH-sektoren.

Kartleggingsmøtene med universitetene og høgskolene ble gjennomført i perioden fra tidlig januar til midten av mars 2021.

Kartleggingsmøtene med direktorater og selskaper ble gjennomført i perioden mai-juni 2020.

FORBEREDELSE OG KONTAKT

Virksomhetene mottok først et brev fra Unit om kartlegging. Brevene til universitetene og høgskolene ble sendt ut i november 2020, mens tilsvarende brevene til direktoratene og selskapene ble sendt ut i april 2020.

I brevene ble det opplyst om at Unit ville gjennomføre besøk hos hver enkelt virksomhet for å kartlegge statusen i arbeidet med informasjonssikkerhet og personvern (GDPR).

Et sett med spørsmål om arbeidet med informasjonssikkerhet og personvern (kartleggingsskjema) var vedlagt brevene fra Unit. Kartleggingsskjemaene finnes i vedlegg 2 og 3.

I forberedelsene til kartleggingen ble det også gjennomført samtaler med Unit sin representant i fagutvalget infrastruktur, mellomvare og data. Hensikten var å få oversikt over viktige digitaliseringsinitiativ i sektoren.

DELTAKELSE OG DELTAKERE

Virksomhetenes deltakelse på kartleggingsmøtene varierte noe, men omfattet vanligvis tre til åtte representanter (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 1,5 timer til besvarelse av spørsmålene i kartleggingsskjemaet. Ved enkelte universiteter og høgskoler tok gjennomgangen noe lengre tid enn berammet.

Alle kartleggingsmøter ble avholdt som videokonferanser.

Fra to universitet mottok Unit skriftlige besvarelser på spørsmålene i kartleggingsskjemaet. De skriftlige svarene ble gjennomgått under møtet med disse virksomhetene.

Ved de øvrige 28 virksomhetene ble svarene på spørsmålene i kartleggingsskjemaet gitt muntlig i møtet. Svarene ble fortløpende notert av deltakerne fra Unit.

ETTERARBEID OG TILBAKEMELDINGER

I etterkant av møtene utarbeidet Unit et kartleggingsreferat som oppsummerte virksomhetenes svar på spørsmålene i skjemaet. Referatene ble sendt tilbake til den enkelte virksomhet for kommentarer og kvalitetssikring.

Etter at Unit har mottatt kommentarer og innspill fra alle virksomhetene, vil Unit utarbeide et anbefalingsbrev til den enkelte virksomhet. Her vil det bli gitt anbefalinger om hva vi mener virksomhetene 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; årsrapportene for de aktuelle virksomhetene i UH-sektoren; risiko- eller trusselvurderinger fra nasjonale myndigheter; risiko- eller trusselvurderinger fra internasjonale aktører og forskningslitteratur innenfor relevante fagområder.

I tillegg inngår informasjon fra regelmessige møter som Unit har med Uninett CERT og rådgivingstjenesten i cybersikkerhetssenteret i datagrunnlaget.

METODISKE BEGRENSNINGER

Rapporten bygger primært på hva Unit ble fortalt i kartleggingsmøtene. Utsagn og påstander fra virksomhetenes side ble ikke forsøkt verifisert, for eksempel ved å be om tilgang til skriftlige beskrivelser av styrende, gjennomførende og kontrollerende del av ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR.

Virksomhetene rapporterte om konkrete informasjonssikkerhets- og personverntiltak som de har iverksatt i 2020. Ut over å be om egenevalueringer av tiltakene, ble det ikke gjennomført kontroller eller testet for å avdekke om tiltakene er tilfredsstillende innført og virker som forutsatt.

Hos universitetene og høgskolene var det i stor grad administrativt ansatte som besvarte spørsmålene i kartleggingsskjemaet. Dersom flere vitenskapelig ansatte hadde vært blant informantene, kan det tenkes at enkelte av svarene hadde blitt annerledes.

VEDLEGG 2: KARTLEGGINGSSKJEMA – UNIVERSITETER OG HØGSKOLER

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

2. Hvilke brudd på informasjonssikkerheten, inkludert personopplysningssikkerheten, og avvik fra egne sikkerhetsrutiner har virksomheten registrert i 2020?
   - Anslagsvis antall og hovedtyper sikkerhetsbrudd eller rutineavvik.
   - Noen eksempler på mulige typer sikkerhetsbrudd og rutineavvik: løsepengevirus, direktør- eller fakturasvindel, tjenestenektangrep, brukerkontoer på avveie, informasjonstyveri, misbruk av dataressurser, brudd på rutiner/retningslinjer for tildeling eller avslutning av brukertilganger, misbruk av brukertilganger.

3. Hvilke andre typer personvernhendelser og rutineavvik enn brudd på personopplysningssikkerheten og avvik fra sikkerhetsrutiner har virksomheten registrert i 2020?
   - Anslagsvis antall og hovedtyper personvernhendelser eller rutineavvik.
   - Noen eksempler på typer hendelser/avvik: manglende vurdering av behandlingsgrunnlag, brudd på sletterutiner, opplysninger oppbevares lengre enn nødvendig, vanskelig å ivareta rettigheter (innsyn, retting, sletting, osv.) eller mangelfull behandlingsprotokoll.

4. Hva er de viktigste årsakene til at brudd på informasjonssikkerheten eller uønskede personvernhendelser oppsto i 2020 (eventuelt årsaker til at uønskede hendelser kan skje i fremtiden)?
   - Noen eksempler på årsaker til brudd og hendelser: uhell, teknisk svikt, mangelfull brukerkompetanse/bevissthet, begrensede ressurser (tid, personell, økonomi), uklar ansvars- eller oppgavefordeling, vanskelig regelverk, feil hos leverandør eller manglende sikkerhetsoppdatering.

5. Hvilke initiativ/tiltak ble gjennomført i 2020 for å styrke/videreutvikle arbeidet med informasjonssikkerhet og ledelsessystemet for informasjonssikkerhet?
   - Eventuelle endringer i status for arbeidet med informasjonssikkerhet og ledelsessystemet siden forrige kartlegging.
   - Områder (forskning, utdanning, administrasjon og formidling) hvor virksomheten mener at arbeidet med informasjonssikkerhet og ledelsessystemet bør styrkes.

6. Hvilke initiativ/tiltak ble gjennomført i 2020 for å styrke/videreutvikle arbeidet med personvern og etterlevelsen av personopplysningsloven/GDPR?
   - Eventuelle endringer i status for innføring/drift av internkontrollen for personopplysningsloven/GDPR siden forrige kartlegging.
   - Områder (forskning, utdanning, administrasjon og formidling) hvor virksomheten mener at arbeidet med personvern og internkontrollen for personopplysningsloven/ GDPR bør styrkes.

7. I hvilken grad ble det gjennomført risikovurderinger av informasjonssikkerheten i 2020? Ble vurderingene fulgt opp med nødvendige sikringstiltak?

8. Hvilke initiativ/tiltak ble gjennomført i 2020 for å oppdage og håndtere uønskede informasjonssikkerhets- og personvernhendelser?
   - Noen eksempler på ordninger eller tiltak: styrket hendelseshåndteringsteamet (IRT), rutiner for håndtering av sikkerhetshendelser/-avvik, anskaffet nytt avviksmeldings-system, rutiner for varsling av Datatilsynet/de registrerte, sikkerhetsovervåking/ -monitorering.

9. I hvilken grad har virksomheten en plan for håndtering av alvorlige informasjonssikkerhets- og personvernhendelser (kontinuitet og beredskap)? Ble det øvd på håndtering av slike hendelser i 2020?

10. Hvilke hovedtema/-problemstillinger ble diskutert på ledelsens gjennomgang i 2020?
    - Viktige initiativ/tiltak på informasjonssikkerhets- og personvernområdet som planlegges gjennomført i 2021.

ÅRETS FOKUSOMRÅDE – KONSEKVENSENE AV COVID-19:

1. Hvordan har korona-nedstengningen påvirket virksomhetens generelle arbeid med informasjonssikkerhet (ledelsessystemet) og personvern (internkontrollen for GDPR)?

2. Hvilke nye IT-løsninger/-tjenester (om noen) har virksomheten tatt i bruk som følge av korona-nedstengningen?

3. Hvilke særskilte personvernutfordringer/-tiltak (om noen) har bruken av hjemmekontor og digital undervisning/eksamen ført til?

VEDLEGG 3: KARTLEGGINGSSKJEMA – DIREKTORATER OG SELSKAPER

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

2. Hvilke brudd på informasjonssikkerheten eller avvik fra egne sikkerhetsrutiner har virksomheten opplevd i 2019?
   - Anslagsvis antall og hovedtyper sikkerhetsbrudd eller rutineavvik.
   - Noen eksempler på mulige sikkerhetsbrudd og rutineavvik: nettfiske, løsepengevirus, direktørsvindel, tjenestenektangrep, brukerkontoer på avveie, informasjonstyveri, misbruk av dataressurser, brudd på rutiner/retningslinjer for tildeling eller avslutning av tilganger, misbruk av brukertilganger.

3. Hvilke uønskede personvernhendelser eller avvik fra egne rutiner for håndtering av personopplysninger har virksomheten opplevd i løpet av 2019?
   - Anslagsvis antall og hovedtyper personvernhendelser eller rutineavvik.
   - Noen eksempler på mulige personvernhendelser og rutineavvik: manglende vurdering av behandlingsgrunnlag, brudd på rutiner for sletting av person-opplysninger, oppbevaring av personopplysninger på usikre lagringsområder, vanskelig å ivareta de registrertes rettigheter (innsyn, retting, sletting, osv.), manglende behandlingsprotokoller eller tjenester som ikke har personvernerklæring.

4. Hvem oppdager eventuelle brudd på informasjonssikkerheten eller uønskede personvernhendelser, og hvordan meldes slike brudd/hendelser?
   - Noen eksempler på hvem som oppdager brudd/hendelser: studenter, faglig eller administrativt ansatte, IT-avdelingen, IRT eller tjenesteleverandører.
   - Noen eksempler på hvordan brudd/hendelser meldes: ad hoc (telefon, personlig oppmøte, epost, osv.) eller via formelle avviksmeldingskanaler.

5. Hva er de viktigste årsakene til eventuelle brudd på informasjonssikkerheten eller uønskede personvernhendelser?
   - Noen eksempler på mulige årsaker: uhell, tekniske svikt, mangelfull bruker-kompetanse/bevissthet, begrensede ressurser (tid, personell, økonomi), uklar fordeling av sikkerhetsoppgaver, vanskelig regelverk, feil hos leverandør, manglende sikkerhetsoppdatering eller tilsiktede handlinger fra eksterne aktører.

6. Hvordan vil virksomheten beskrive status for innføring og/eller drift av ledelsessystemet for informasjonssikkerhet?
   - Eventuelle endringer siden forrige kartlegging.

7. Hvordan vil virksomheten beskrive status for etterlevelse av GDPR og personopplysningsloven (etablering og innføring av internkontroll)?
   - Eventuelle endringer siden forrige kartlegging.

8. Hvilke viktige tiltak eller initiativ er gjennomført i 2019 for å styrke informasjonssikkerheten og/eller personvernet (GDPR)?
   - Noen eksempler på mulige tiltak/initiativ: gjennomføring av risikovurderinger i forskning, undervisning eller administrasjon, innføring av viktige tekniske sikringstiltak, etablering av kontinuitetsplan, formidlet informasjon om eller gjennomført opplæring i rutiner for bruk av personopplysninger.

9. Hvilke hovedtema/-problemstillinger ble diskutert på siste ledelsens gjennomgang?

10. Har det vært gjennomført øvelser på håndtering av uønskede hendelser som berører informasjonssikkerheten og/eller personvernet i løpet av 2019?

11. Hvor stor (anslagsvis) andel av virksomhetens system-/tjenesteportefølje driftes av eksterne leverandører (databehandlere)?

12. Hvilke rutiner/praksis gjelder når virksomheten vurderer å sette ut systemer/tjenester som behandler personopplysninger til eksterne leverandører (databehandlere)?

13. Hvordan forsikrer virksomheten seg om at eksterne leverandører (databehandlere) følger opp krav til informasjonssikkerhet og personvern underveis i tjenesteleveransen?

VEDLEGG 4: RAMMEVERK FOR VURDERING AV RISIKO

SANNSYNLIGHETSVERDIER (HENDELSESFREKVENS)

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

KONSEKVENSVERDIER (SKADEVIRKNINGER)

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

- **Personvernkrenkelser**: korte avbrudd i tilgangen til egne personopplysninger; enkelte opplysninger lagres noe lengre enn hva som er nødvendig; det registreres noen flere alminnelige opplysninger enn hva behandlingsformålet strengt tatt krever.
- **Tjenesteavbrudd:** korte perioder med ustabil tilgang til enkelte tjenester eller til mindre mengder data/opplysninger.
- **Økonomisk tap:** noe ekstraarbeid i forbindelse med hendelseshåndtering.
- **Tap av omdømme og tillit:** noe misnøye blant enkelte interne brukere.
- **Skader nasjonale interesser:** N/A.

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

- **Personvernkrenkelser:** uautorisert eksponering av mindre mengder alminnelige personopplysninger; enkelte opplysninger mangler eller er feil; opplysningene er utilgjengelige for den registrerte opp mot fem dager.
- **Tjenesteavbrudd:** stans i levering av ikke-kritiske tjenester, eventuelt manglende tilgang til lite tidskritiske data/opplysninger, i mindre enn 24 timer.
- **Økonomisk tap**: enkeltpersoner (ansatte eller studenter) utbetaler mindre beløp til nettkriminelle.
- **Tap av omdømme og tillit:** misnøye blant viktige interne brukergrupper.
- **Skader nasjonale interesser:** uautorisert tilgang til forskningsdata/-resultater innen områder som kan ha en viss betydning for ivaretakelse av nasjonale interesser.

Alvorlig: hendelser med merkbare skadevirkninger.
Eksempler på hendelser med merkbare skadevirkninger fordelt på utvalgte skadekategorier:

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

Meget alvorlig: hendelser med betydelige skadevirkninger.
Eksempler på hendelser med betydelige skadevirkninger fordelt på utvalgte skadekategorier:

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

VEDLEGG

RISIKONIVÅER OG OPPFØLGING

HØY RISIKO:

Hendelser som medfører behov for tiltak:

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

MIDDELS RISIKO:

Hendelser som medfører behov for vurdering av tiltak:

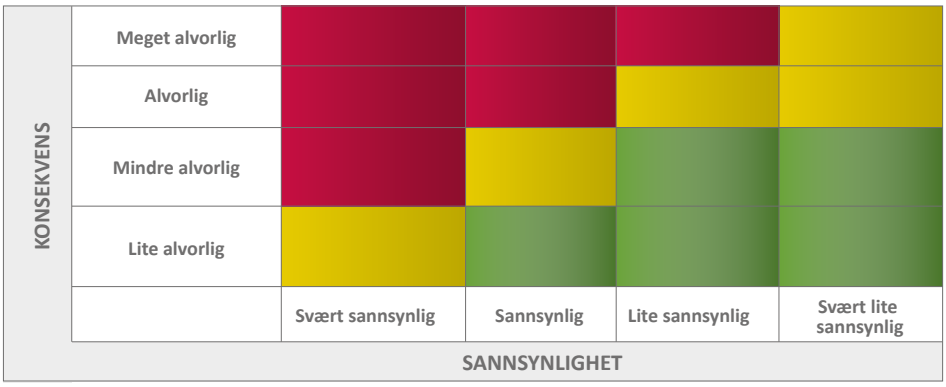
- Hendelser som er svært sannsynlige og som kan få lite alvorlige skadevirkninger.
- Hendelser som er sannsynlige og som kan få mindre alvorlige skadevirkninger.
- Hendelser som er lite sannsynlige og som kan få alvorlige skadevirkninger.
- Hendelser som er svært lite sannsynlige og som kan få alvorlige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

LAV RISIKO

Risikoen aksepteres:

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

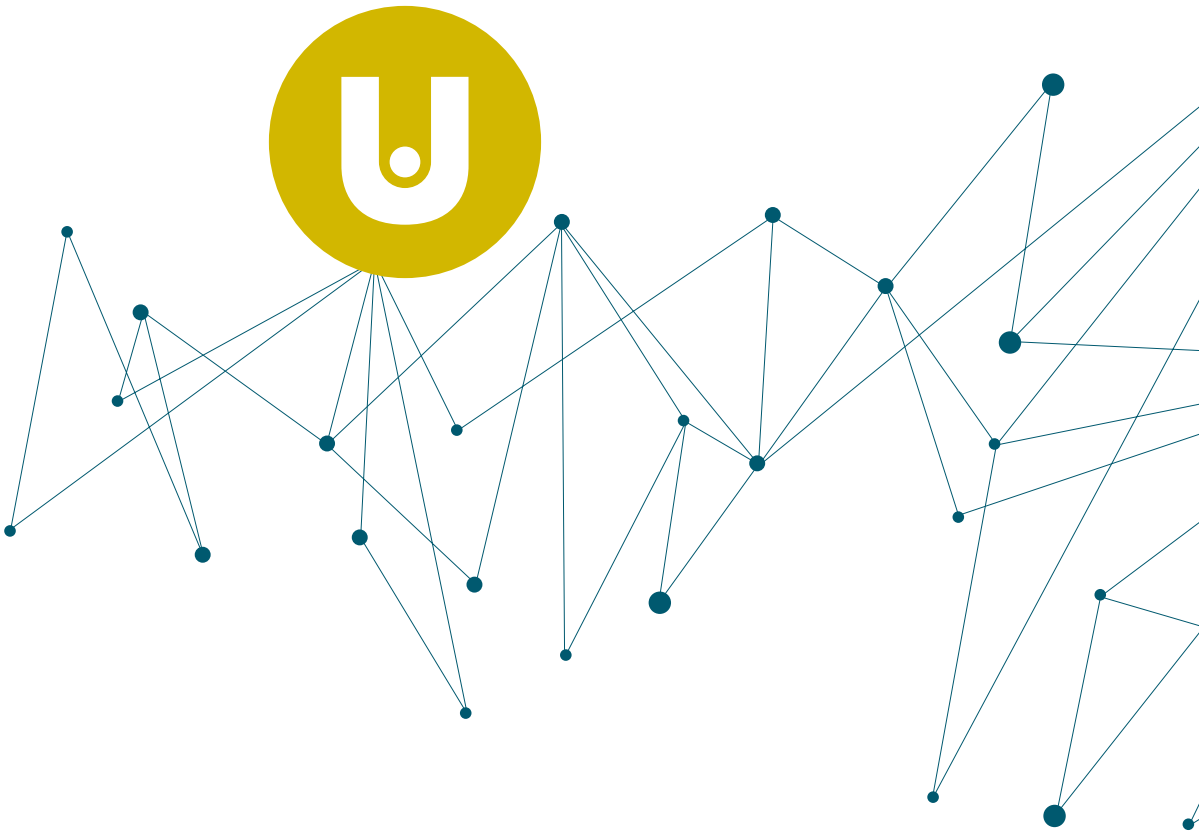
RISIKOMATRISE:



OM VURDERING AV KONSEKVENS

Når en uønsket hendelse har flere forskjellige skadevirkninger, kan alvorlighetsgraden variere: noen skadevirkninger kan være meget alvorlige; andre kan være mindre eller lite alvorlige.

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



unit.no

UNIT

DIREKTORATET FOR IKT OG FELLESTJENESTER
I HØYERE UTDANNING OG FORSKNING