INFORMASJONSSIKKERHET OG PERSONVERN I HØYERE UTDANNING OG FORSKNING

Risiko- og tilstandsvurdering 2020

INNHOLD

SAMMENDRAG

Dette er den andre årlige rapporten hvor Unit presenterer sin risiko- og tilstandsvurdering av arbeidet med informasjonssikkerhet og personvern hos statlige universiteter og høgskoler. I fjorårets rapport ble det gitt en oversikt over status for dette arbeidet i 2018. Risikoen for mangelfull oppnåelse av målene for informasjonssikkerhet og personvern i sektorens digitaliseringsstrategi ble også vurdert [1].

Årets rapport gir en tilsvarende statusoversikt for 2019, som også inkluderer åtte direktorater og selskaper, og vi gjør en ny vurdering av risikoen for manglende realisering av sektormålene. Til slutt vurderes risikoen for at sektoren utsettes for konkrete informasjonssikkerhets- og personvernhendelser.

Datagrunnlaget for årets rapport er svar på spørsmål om hvordan arbeidet med informasjonssikkerhet og personvern er prioritert, organisert og gjennomført hos 29 statlige universiteter, høgskoler, direktorater og selskaper. Spørsmålene ble besvart i kartleggingsmøter mellom den enkelte institusjon/virksomhet og Unit. I etterkant av møtene utarbeidet Unit et møtereferat som ble sendt til nstitusjonene og virksomhetene for skriftlige kommentarer. Det ble ikke bedt om tilgang til dokumentasjon for å verifisere institusjonenes og virksomhetenes svar.

TRENDER I 2019

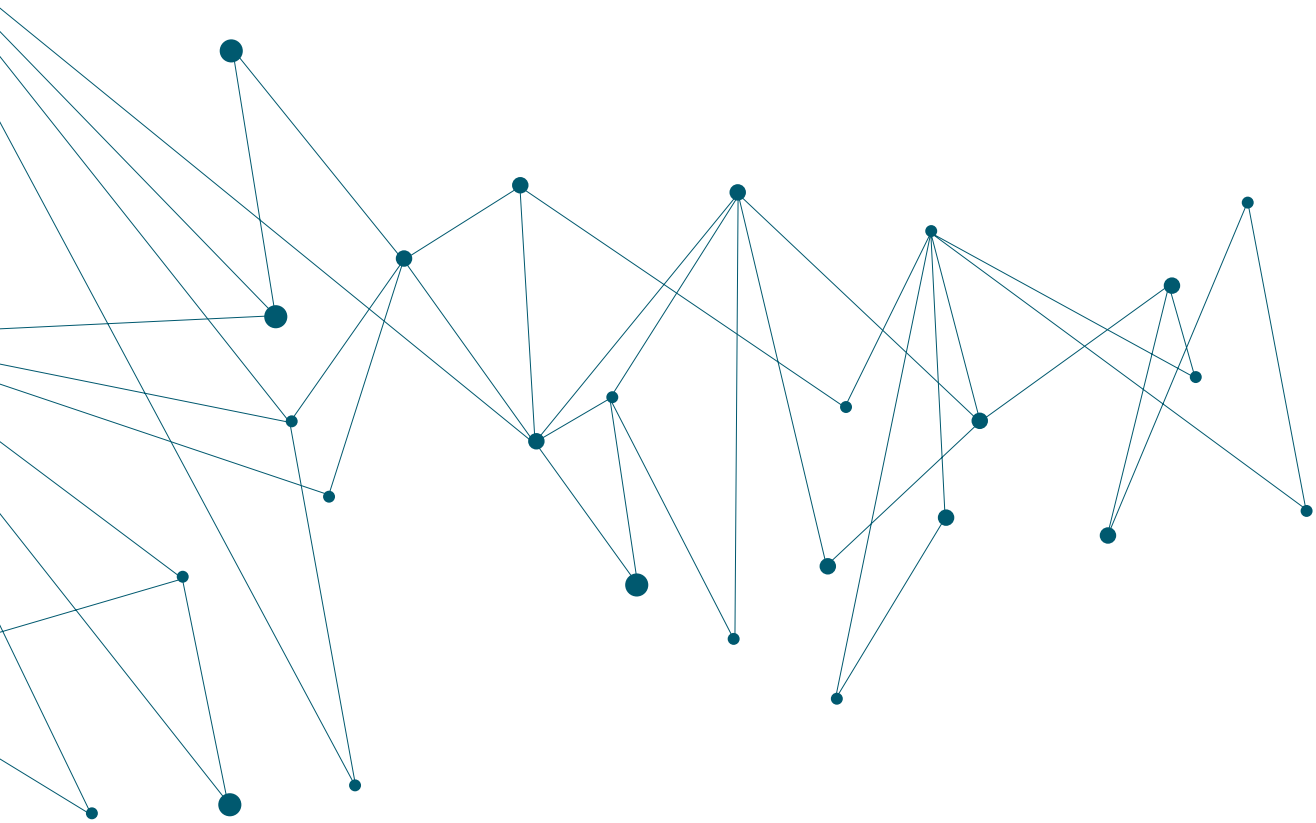
Trendene i sektorens arbeid med informasjonssikkerhet og personvern i 2019, kan oppsummeres i følgende hovedpunkter:

- Arbeidet med informasjonssikkerhet og personvern er styrket i 2019 sammenlignet med 2018. Styrkingen hadde skjedd på flere måter. Dette gjaldt særlig arbeidet med utarbeidelse og innføring av ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR.

- Antallet brudd på informasjonssikkerheten og uønskede personvernhendelser var omtrent på samme nivå i 2019 som i 2018. Samtidig ble det rapportert om at trusselbildet var blitt mer utfordrende, spesielt på grunn av mer avanserte forsøk på nettkriminalitet.

- Det ble rapportert om enkelte viktige sårbarheter/mangler i arbeidet med informasjonssikkerhet og personvern. Sårbarhetene gjaldt særlig manglende kompetanse om praktisk informasjonssikkerhetsarbeid og om reglene i GDPR. Det ble også meldt om behov for mer kapasitet til gjennomføring av planlagte tiltak og initiativ.

[1] Se https://www.unit.no/sites/default/files/media/filer/2019/06/Tilstandsvurdering-av-informasjonssikkerhet-personvern-blant-de-statlig-eide-universitetene-og-hogskolene.pdf.



HOVEDKONKLUSJONER

Selv om det har vært en positiv utvikling på området, mener Unit at risikoen fortsatt er høy for at flere av målene for arbeidet med informasjonssikkerhet og personvern i sektorens digitaliseringsstrategi ikke kan oppnås innen strategiperiodens utløp [2]. Arbeidet er styrket, tiltak er iverksatt og ledelsesforankringen er stort sett god, men tiden frem til strategiperiodens slutt blir trolig for knapp.

Videre er det Unit sin vurdering at nettkriminalitet utgjør den største risikoen for brudd på informasjonssikkerheten og uønskede personvernhendelser i UH-sektoren. Dette gjelder i særlig grad faktura- og direktørsvindel, og hendelser knyttet til uautoriserte anvendelser av kompromitterte brukerkontoer.

I tillegg mener Unit at risikoen for at innsideproblemer kan føre til informasjonssikkerhets- eller personvernhendelser er middels til høy. Dette handler om hendelser som skyldes interne forhold ved den enkelte institusjon eller virksomhet, for eksempel manglende kompetanse eller uklar arbeidsorganisering.

Når det gjelder statlig eller statsstøttet dataspionasje, mener Unit at dette er en risiko som deler av sektoren må være oppmerksom på.

OPPFØLGING

Unit mener at det ikke er behov for flere nye sektortiltak på informasjonssikkerhets- og personvernområdet nå. Det er allerede planlagt eller nylig iverksatt en rekke slike tiltak, blant annet innenfor rammen av «Program for informasjonssikkerhet i UH-sektoren» og som en del av sektorens handlingsplan for digitalisering. Det vil derfor, etter Units oppfatning, være hensiktsmessig å avvente effektene av disse tiltakene før det iverksettes nye.

Unit har også i år sendt brev til den enkelte institusjon og virksomhet med anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern.

[2] Dette gjelder følgende sektormål: (i) institusjonene skal etablere helhetlig styring og ledelse av arbeidet med informasjonssikkerhet og personvern, (ii) institusjonenes arbeid med styrking av informasjonssikkerheten og personvernet skal være systematisk, (iii) nivået på arbeidet med informasjonssikkerhet og personvern skal ligge høyere enn de nasjonale minstekravene.

INNLEDNING

Denne rapporten oppsummerer hovedfunnene i Unit sin kartlegging av arbeidet med informasjonssikkerhet og personvern i høyere utdanning og forskning for 2019 [3].

Rapporten inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i UH-sektoren [4].

Av styringsmodellen fremgår det at Unit skal utarbeide en årlig rapport som oppsummerer sektortilstanden når det gjelder arbeidet med informasjonssikkerhet og personvern [5]. Unit skal spesielt vurdere risikoen for at arbeidet med informasjonssikkerhet og personvern ikke oppfyller sektormålene slik de er beskrevet i «Digitaliseringsstrategi for universitets- og høyskolesektoren, 2017-2021».

I tillegg vil Unit i årets rapport vurdere risikoen for konkrete informasjonssikkerhets- og personvernhendelser i universitets- og høgskolesektoren. Dette er risikoer som vi mener at institusjonene og virksomhetene bør være ekstra oppmerksomme på og ta hensyn til fremover.

Det betyr at formålet med denne rapporten er tredelt.
For det første å gi en oversikt over tilstanden når det gjelder arbeidet med informasjonssikkerhet og personvern hos de statlige universitetene, høgskolene og øvrige virksomheter som omfattes av Kunnskapsdepartementets styringsmodell[6].
For det andre å vurdere
(i) risikoen for manglende måloppnåelse med bakgrunn i sektormålene som gjelder for arbeidet med informasjonssikkerhet og personvern, og
(ii) risikoen for at sektoren utsettes for konkrete informasjonssikkerhets- og personvernhendelser.

For det tredje å gi enkelte anbefalinger om tiltak på sektornivå som bør iverksettes for å styrke arbeidet med informasjonssikkerhet og personvern.

[3] En tilsvarende kartlegging ble gjennomført for 2018.

[4] 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.

[5] Oversikt over hvilke institusjoner og virksomheter som omfattes av KDs styringsmodell finnes her: https://www.unit.no/styringsmodell-informasjonssikkerhet-i-hoyere-utdanning-og-forskning.

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

KORT OM INFORMASJONSSIKKERHET OG PERSONVERN

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

Med personvern menes i denne sammenheng 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 [8].

SEKTORMÅL OG NASJONALE FØRINGER

Sektormålene for arbeidet med informasjonssikkerhet og personvern defineres i «Digitaliseringsstrategi for universitets- og høyskolesektoren, 2017-2021». I strategien understrekes det at informasjonssikkerhet og personvern skal være et fundament for digitalisering og strategiske satsninger i sektoren. Virksomhetsledelsen skal derfor sørge for at det etableres et systematisk arbeid for styrking av i nformasjonssikkerheten og personvernet. Dette arbeidet skal skje i tråd med nasjonale føringer [9], spesielt rettslige krav og andre nasjonale føringer, men det forventes at nivået på informasjonssikkerheten og personvernet skal ligge høyere enn hva som følger av de nasjonale minstekravene.

Til slutt skal studenter og forskere bevisstgjøres om problemstillinger knyttet til datasikkerhet og riktig håndtering av data.

RISIKOVURDERING – VERDIER, TRUSLER OG SÅRBARHETER

Vurderinger av risikoen for manglende måloppnåelse og uønskede informasjonssikkerhets- eller personvernhendelser baserer seg på tradisjonell risikovurderingsmetodikk [10]. Formålet med slike vurderinger er ikke primært å finne årsaker til det som allerede har skjedd, men å bedre oddsen for å oppnå det man ønsker. Dette er også formålet med denne rapporten: oversikten over tilstanden i sektoren (kapittel 1-3) danner grunnlaget for vurderinger av risikoen for mangelfull fremtidig måloppnåelse og uønskede hendelser (kapittel 4). Dersom vi mener at risikoen er høy, vil vi foreslå sektortiltak for å redusere den til et lavere og akseptabelt nivå.

Mer konkret innebærer dette at risiko avgjøres av forholdet mellom tre faktorer – verdier, trusselkilder og sårbarheter:

- **Verdier:** Det som sektoren skal beskytte mot uønskede informasjonssikkerhets- eller personvernhendelser, for eksempel informasjon eller data som benyttes i forskning, undervisning eller administrasjon.

[7] ISO/IEC 27001: 2013: Information Technology Security Techniques. Information Security Management Systems – Requirements. Torgeir Daler, Roar Gulbrandsen, Tore Audun Høie og Torbjørn Sjølstad (2010): Håndbok i datasikkerhet – informasjonsteknologi og risikostyring. Trondheim: Tapir akademiske forlag.

[8] Se Jon Wessel-Aas og Magnus Ødegaard (2018): Personvern. Publisering og behandling av personopplysninger. Oslo: Gyldendal; Peter Blume (2018): Databeskyttelsesret. København: Djøf Forlag.

[9] Se spesielt regjeringens nasjonale strategi for digital sikkerhet og delstrategien for digital sikkerhetskompetanse (https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/).

- **Trusselkilder:** Det som kan utsette verdiene i sektoren for uønskede informasjonssikkerhets- eller personvernhendelser, for eksempel nettkriminelle grupper eller statlig dataspionasje.

- **Sårbarheter:** Svakheter eller mangler som kan føre til uønskede informasjonssikkerhets- eller personvernhendelser, for eksempel manglende personvernkompetanse eller tekniske sikkerhetshull i programvare.

Det betyr for eksempel at risikoen for manglende måloppnåelse eller uønskede hendelser kan sies å være høy dersom sektorens verdier utsettes for betydelige trusler, samtidig som arbeidet med informasjonssikkerhet og personvern preges av vesentlige sårbarheter. Motsatt kan risikoen sies å være mindre dersom sektorens verdier utsettes for få trusler, og arbeidet med informasjonssikkerhet og personvern er robust og høyt prioritert.

KAPITTELOVERSIKT

I kapittel 1 gis et omriss av hvilke hovedtyper verdier som forvaltes i sektoren. Deretter drøftes hvilke informasjonssikkerhets- og personverninitiativ som de statlige universitetene og høgskolene hadde iverksatt i 2019. Til slutt gis en oversikt over sårbarheter som preget institusjonenes arbeid med informasjonssikkerhet og personvern.

I kapittel 2 gis en oversikt over hvilke trusselkilder og uønskede hendelser som universitetene og høgskolene rapporterte at de hadde vært utsatt for i løpet av 2019.

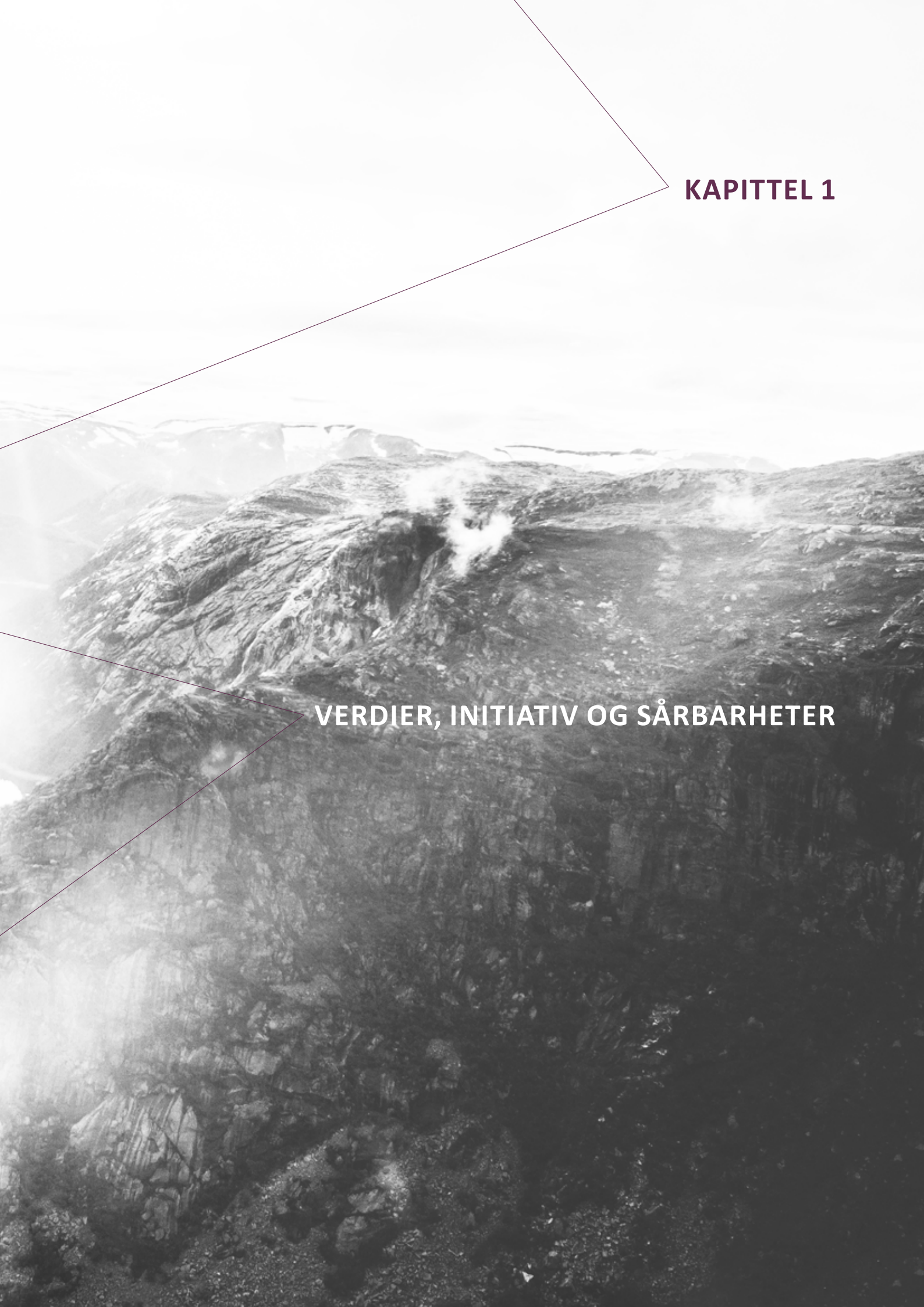
I kapittel 3 presenteres funnene fra fjorårets kartlegging av åtte selskaper og direktorater som inngår i Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern.

I kapittel 4 presenteres vurderingene av risiko for manglende måloppnåelse og uønskede informasjonssikkerhets- og personvernhendelser. Det gis også enkelte anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern i sektoren.

VEDLEGG

I vedlegget gjøres det rede for datagrunnlaget som denne rapporten baseres på.

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



KAPITTEL 1

VERDIER, INITIATIV OG SÅRBARHETER

VERDIER, INITIATIV OG SÅRBARHETER

INNLEDNING

I dette kapitlet drøftes fire spørsmål:

1 Hvilke verdier skal institusjonenes arbeid med informasjonssikkerhet og personvern ivareta?
2 Hvilke initiativ iverksatte institusjonene i 2019 for å unngå at verdiene ble utsatt for uønskede informasjonssikkerhets- og personvernhendelser?
3 Hva var status for sektorens arbeid på informasjonssikkerhets- og personvernområdet i 2019?
4 Hvilke sårbarheter påvirket (eller preget) institusjonenes arbeid med å styrke informasjonssikkerheten og personvernet?

Forholdet mellom verdier, initiativ og sårbarheter er avgjørende for å kunne vurdere hvilke risikoforhold som arbeidet med informasjonssikkerhet og personvern i universitets- og høgskolesektoren står overfor. Risiko vil bli drøftet i det siste kapitlet.

Nedenfor gir vi først en kort og skjematisk oversikt over hvilke hovedtyper verdier som institusjonene ivaretar.

Deretter følger en oversikt over status for og endringer i arbeidet med informasjonssikkerhet og personvern på sektornivå, og hvilke initiativ institusjonene iverksatte i 2019.

Avslutningsvis drøftes de viktigste sårbarhetene (manglene/svakhetene) i arbeidet med informasjonssikkerhet og personvern som institusjonene rapporterte om i 2019.

HVILKE VERDIER?

Mange av de verdiene som universiteter og høgskoler er helt avhengige av for å drive sin virksomhet og for å løse sitt samfunnsoppdrag, er nå digitalisert – eller er i ferd med å bli det. Arbeidet med informasjonssikkerhet og personvern har som formål å sørge for at disse verdiene forvaltes på en sikker og forsvarlig måte, både i forskning, undervisning, administrasjon og formidling. Dersom viktige verdier ikke beskyttes godt nok mot uønskede hendelser eller ikke forvaltes på forsvarlig vis, kan det ramme sektorens og den enkelte institusjons evne til måloppnåelse. Det kan også påføre enkeltpersoner eller aktører i og utenfor universitets- og høgskolesektoren skade, og svekke tilliten til enkeltinstitusjoner eller til sektoren som sådan. Som nevnt i fjorårets rapport, er det problematisk at kunnskapen om flere av de viktigste verdiene som skal ivaretas er til dels fragmentert, både på sektornivå og ved den enkelte institusjon.
Det vi likevel kan si er at det er tre hovedtyper verdier som institusjonene i særlig grad må beskytte og forvalte på forsvarlig vis.

Disse verdiene er:

1. Informasjonsverdier, spesielt:
   - Vitenskapelige data og faglig kunnskap, for eksempel forskningsdata/rådata, analyseresultater, vitenskapelige publikasjoner eller undervisningsmateriell.
   - Personopplysninger, for eksempel opplysninger om søkere, studenter, ansatte, gjester, alumni og deltakere i forskningsprosjekter.

2. Dataressurser, spesielt:
   - Digital infrastruktur, for eksempel datanettverk, tungregneanlegg, sensornettverk, forskningsdatabaser, laboratorieinstrumenter og audiovisuelt utstyr.
   - IT-systemer og -tjenester, for eksempel studentadministrative systemer, undervisningssystemer eller formidlingsløsninger.
   - Personlig IT-utstyr, for eksempel smarttelefoner eller stasjonære og bærbare datamaskiner.

3. Andre verdier, spesielt:
   - Økonomiske midler (penger).

Betydningen av informasjonsverdier, kanskje særlig i forskning, påvirkes av hvem informasjonen er viktig for. Variasjonsbredden i de informasjonsverdiene som forvaltes i sektoren generelt og forskning spesielt er stor, og kan derfor være betydningsfull for mange ulike aktører i og utenfor sektoren. Poenget er at verdien av informasjon øker med antallet aktører den er viktig for. Informasjon i forskning vil for eksempel ha verdi for den enkelte forsker og institusjon, men den kan også være viktig for personvernet til den enkelte forskningsdeltaker (der hvor det behandles personopplysninger). Enkelte forskningsdata/-kunnskap kan ha særskilt betydning for politikkutforming og forvaltning på viktige samfunnsområder (vær- og klimadata, maritime data, geologiske data, helsedata, osv.). Det vil også finnes

samarbeidspartnere og aktører i offentlig og privat sektor, for eksempel industriselskaper og aktører i helsesektoren, som har interesser knyttet til og ser betydningen av at informasjonsverdier i UH-sektoren forvaltes på en sikker og forsvarlig måte.

Videre kan andre eksterne aktører enn samarbeidspartnere og industriaktører vurdere enkelte av sektorens informasjonsverdier som verdifulle for egen del. Her kan det dreie seg om at andre staters myndigheter har særlig interesse for informasjon/kunnskap som produseres innenfor viktige forskningsområder, og som de derfor forsøker å tilegne seg på fordekte måter. Dette kan gjelde forskning som har kommersiell verdi eller forskning som har militære anvendelsesområder, for eksempel innenfor områder som nanoteknologi, maskinlæring, kryptologi eller undervannsteknologi [11].

I tillegg til informasjon, forvalter sektoren store verdier i form av dataressurser. Dette illustreres blant annet i omfanget av institusjonenes system- og tjenesteporteføljе. Her rapporterte enkelte institusjoner om at de forvaltet flere hundre systemer/tjenester. Selv de minste institusjonene forvaltet mellom 50 og ca. 170 IT-systemer eller -tjenester. Samtidig har bruken av eksterne IT-løsninger, enten levert av kommersielle selskaper eller av sektoraktører (Unit, Uninett, UiO, NSD, osv.), bidratt til at verdien av dataressursene i sektoren har økt de siste årene. I 2019 rapporterte 14 institusjoner at mer enn 50 prosent av den samlede databehandlingen nå skjer ved hjelp av eksternt leverte og driftede IT-løsninger. Avhengigheten av dataressurser – enten de forvaltes internt eller hos eksterne leverandører – er derfor stor og økende innenfor alle kjerneområdene i sektoren. Det betyr at uønskede informasjonssikkerhets- eller personvernhendelser som rammer disse verdiene kan få problematiske konsekvenser for institusjonene selv og sektoren i stort.

Sammen med informasjon og dataressurser, forvalter institusjonene en annen attraktiv verdi – økonomiske midler (penger). Flere av de største institusjonene er milliardvirksomheter, og resten forvalter store millionbeløp. I et senere kapittel skal vi se at disse verdiene utsettes for en viss risiko, og at økonomiske midler er den verdien som er årsak til de største informasjonssikkerhetsbekymringene i sektoren. Denne risikoen kommer også til uttrykk ved at «Økonomiregelverket i staten» inneholder tydelige krav til informasjonssikkerheten i økonomi- og regnskapssystemer [12].

OM LEDELSESSYSTEMER OG INTERNKONTROLL FOR GDPR

Hensikten med ledelsessystemer for informasjonssikkerhet er (i) å forebygge trusler mot sikkerheten til institusjonenes verdier (informasjon, dataressurser og økonomiske midler), (ii) avdekke og håndtere brudd på sikkerheten til verdiene som likevel oppstår, og (iii) gjenopprette normal drift etter større sikkerhetsbrudd. Det er toppledelsen som avgjør hvilke krav som skal stilles til informasjonssikkerheten i virksomheten, og som følger opp det praktiske arbeidet. Dette arbeidet skjer innenfor rammen av en sikkerhetsorganisasjon, hvor ansvar og oppgaver er definert og fordelt [13].

Internkontroll for GDPR skal sikre at behandling av personopplysninger skjer i samsvar med bestemmelsene i personopplysningsloven og GDPR. Alle som er ansvarlige for slik behandling har plikt til å opprette en internkontroll (jf. artikkel 24 i GDPR). Det er toppledelsen som har det endelige ansvaret for at en internkontroll er etablert, og for at den fungerer etter hensikten (sikrer at bestemmelsene i regelverket overholdes). Personvernombudet bistår virksomheten i arbeidet med internkontroll, blant annet ved å gi råd om hvordan reglene kan overholdes og ved å kontrollere regeletterlevelsen. Føringer og prosedyrer for arbeidet med personopplysningssikkerhet inngår i internkontrollen [14].

[11] Se for eksempel https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/.

[12] Se https://dfo.no/fagomrader/%C3%B8konomiregelverket.

[13] Se for eksempel Nasjonal sikkerhetsmyndighets «Grunnprinsipper for IKT-sikkerhet» (utkast).
https://www.nsm.stat.no/globalassets/dokumenter/grunnprinsipper-for-ikt-sikkerhet-2.0/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

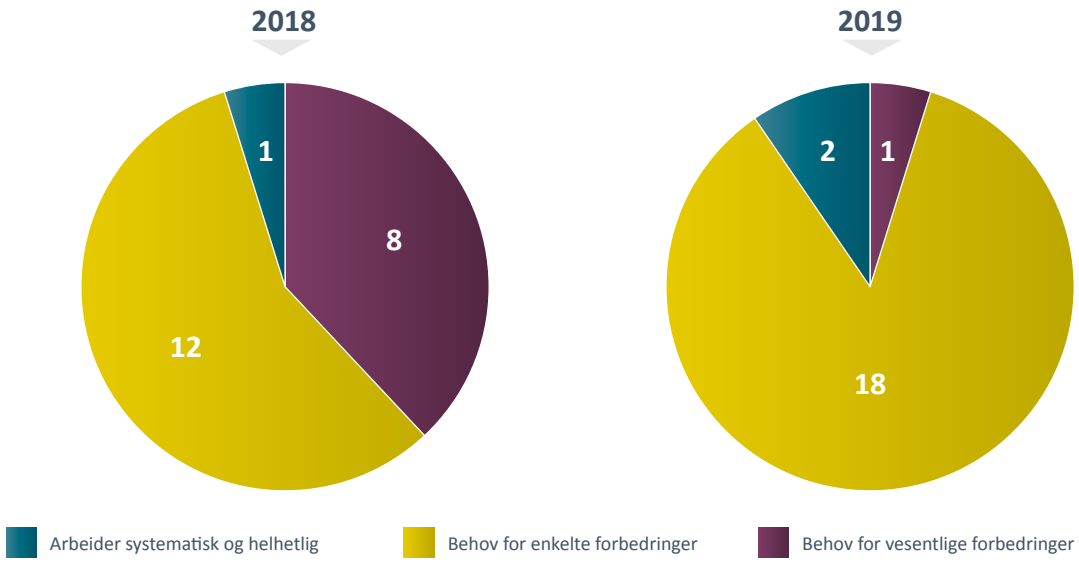
[14] Se Datatilsynets veiledningssider om internkontroll.
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/.

STATUS OG ENDRING

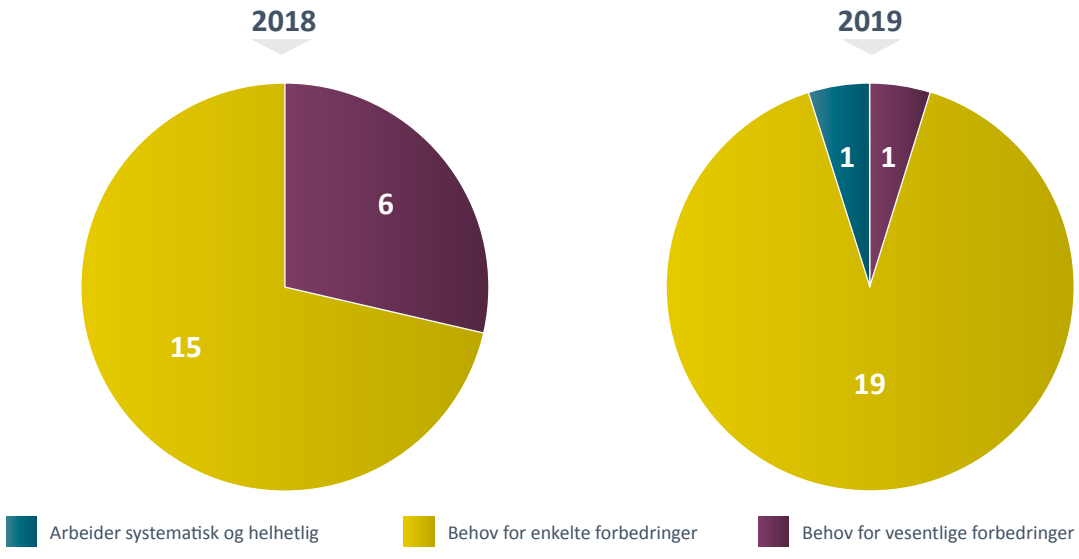
Universitetene og høgskolene iverksatte i 2019 en rekke initiativ for å beskytte og forvalte sine verdier (informasjon, dataressurser og økonomiske midler) på tilfredsstillende måter. Nedenfor skal vi se at initiativene i stor grad handlet om utarbeidelse, innføring eller praktisering av de arbeidsoppgaver som inngår i ledelsessystemer for informasjonssikkerhet eller internkontrollen for GDPR. Vi starter imidlertid med å gi en kort oversikt over endringer fra 2018 til 2019 i arbeidet med ledelsessystemer og internkontroll for GDPR.

Figur 1 og 2 oppsummerer status for arbeidet med ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR i 2019, og viser endringer fra 2018.

Figur 1: Status for arbeidet med ledelsessystem for informasjonssikkerhet, 2018 og 2019



Figur 2: Status for arbeidet med internkontroll (GDPR), 2018 og 2019



Figur 1 viser progresjonen i institusjonenes arbeid. I 2018 hadde åtte institusjoner behov for vesentlige forbedringer i arbeidet med ledelsessystemer (befant seg i oppstartsfasen), mens 12 institusjoner hadde behov for enkelte forbedringer (ledelsessystemet utarbeidet, men ikke fullt ut innført).

Én institusjon jobbet helhetlig og systematisk (ledelsessystemet innført i alle deler av organisasjonen). I 2019 var det langt færre institusjoner som fortsatt befant seg i oppstartsfasen (én), og flere som jobbet med innføring (18). To institusjoner rapporterte nå at de jobbet helhetlig og systematisk.

Også figur 2 viser forbedringer i arbeidet med internkontroll for GDPR fra 2018 til 2019. Det avspeiles særlig på to måter: reduksjon i antallet institusjoner som befant seg i oppstartsfasen med utarbeidelse og innføring av internkontroll for GDPR (seks i 2018 mot én i 2019), og økning i antallet institusjoner som hadde behov for enkelte forbedringer for å komme i mål (15 i 2018 mot 19 i 2019). I 2019 var det én institusjon som meldte at innføringen av internkontrollen i hele organisasjonen var sluttført (arbeidet helhetlig og systematisk). Ingen institusjoner rapporterte om det samme i 2018.

Figur 1 og 2 indikerer, som allerede antydet, to utviklingstrekk. For det første at få institusjoner (to) mente at innføringen av ledelsessystemer og internkontroll for GDPR i liten grad var påbegynt. Men det var også få institusjoner som rapporterte at de anså innføringen av et systematisk informasjonssikkerhets- eller personvernarbeid for sluttført.

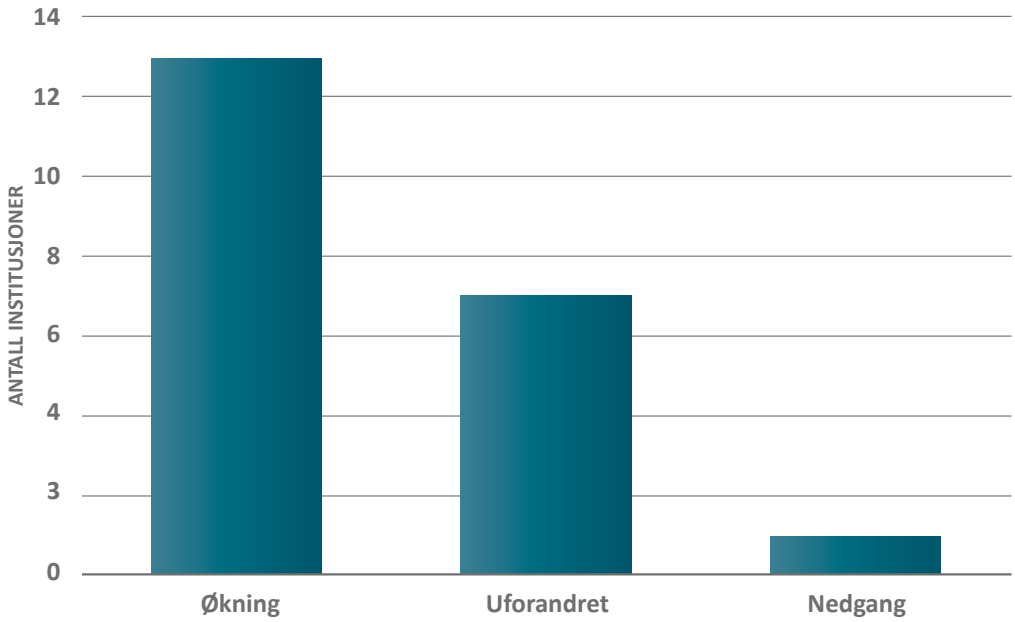
For det andre at det hadde vært fremgang i arbeidet med innføringen av både ledelses- og internkontrollsystemer sammenlignet med 2018. Det ble opplyst om økt støtte og oppmerksomhet fra toppledelsen og fra universitets- eller høgskolestyrene. Styrken i progresjonen varierte imidlertid noe mellom institusjonene: enkelte institusjoner rapporterte om raskere fremgang enn andre.

HVA BLE GJORT I 2019?

Et av de viktigste initiativene som institusjonene ble anbefalt av Unit å iverksette etter fjorårets kartlegging, var styrking av ressursinnsatsen. Flere årsverk i arbeid ble vurdert å være avgjørende for å bedre fremdriften i prosessen med utarbeidelse, innføring og praktisering av ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR.

Figur 3 viser antallet institusjoner som rapporterte at personalinnsatsen (målt som antall årsverk) hadde økt, var uforandret eller hadde blitt redusert i 2019.

Figur 3: Endringer i personalinnsatsen (årsverk) fra 2018 til 2019



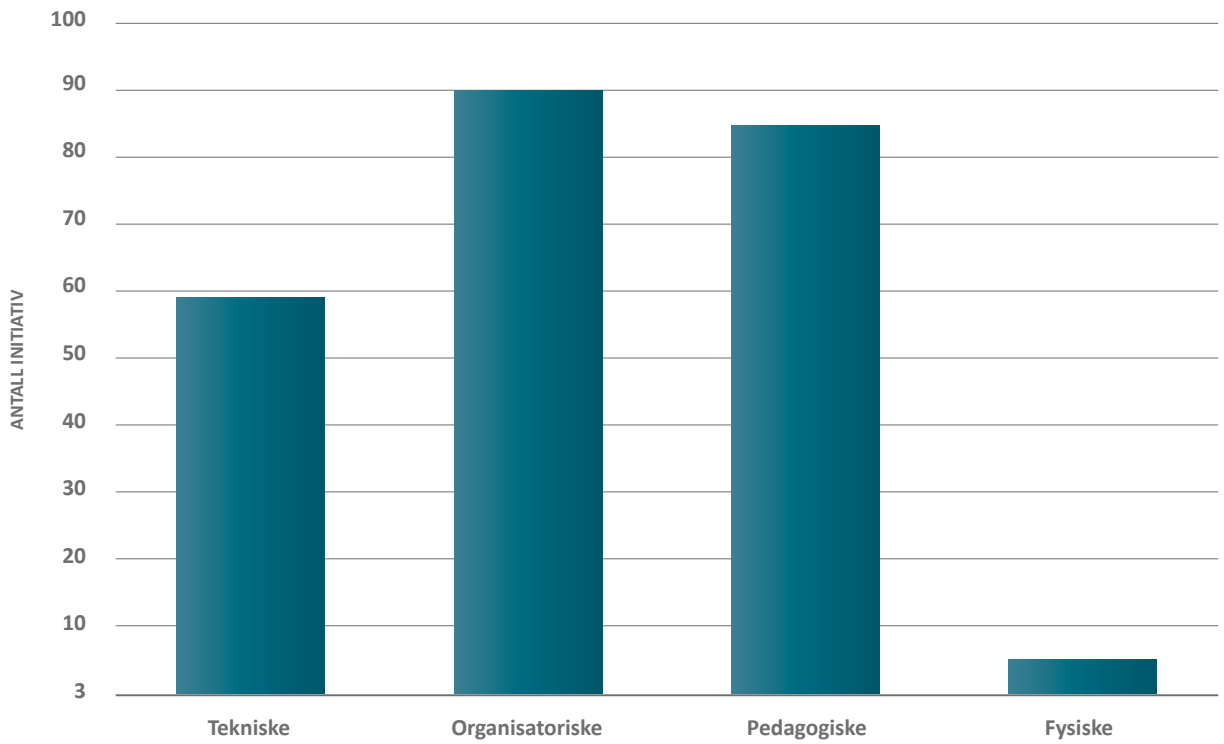
Som det fremgår av figuren, rapporterte 13 institusjoner at årsverksinnsatsen hadde økt i 2019 sammenlignet med 2018. Sju institusjoner rapporterte at årsverksinnsatsen var uforandret, mens én institusjon opplyste om nedgang. Den samlede økningen i antallet rapporterte årsverk var på omkring 13,5 årsverk. Det betyr at 0,22 prosent av samtlige årsverk i sektoren, det vil si hos de statlige universitetene og høgskolene, jobbet med informasjonssikkerhet og personvern i 2019 [15]. For 2018 var det tilsvarende tallet 0,19 prosent.

I årsverkstallene inngikk årsverkene til institusjonenes personvernombud og til de daglig ansvarlige for arbeidet med informasjonssikkerhet (CISO eller tilsvarende). Sju institusjoner oppga at de hadde ansatt personvernombud i 100 prosent stilling, mens like mange hadde ombud i deltidsstillinger. I de siste seks institusjonene var personvernombudet enten en rolle uten stillingsprosent eller det dreide som om innleie (fra konsulentselskap) på timebasis. Ved 12 institusjoner var CISO (eller tilsvarende) ansatt i fulle stillinger eller deltidsstillinger. Ved de resterende ni institusjonene var dette en rolle uten fast stillingsprosent.

I tillegg rapporterte institusjonene om at også andre personalressurser inngikk i årsverksanslagene. Det gjaldt blant annet personell som deltok i institusjonenes spesialgrupper for håndtering av IT-sikkerhetshendelser (IRT – Incident Response Teams). Dessuten ble det rapportert at IT-drifts- og utviklingsmiljøer jobbet en del med informasjonssikkerhet og personvern. Det samme gjaldt for enkelte medarbeidere i studie- og forskningsadministrasjon, HR og økonomiavdelingene. Spesielt i forskningsadministrasjon ble det rapportert om ansatte som jobbet med personvernrådgiving overfor vitenskapelige ansatte og studenter.

Det er verdt å merke seg at årsverksanslagene nesten ikke inkluderte vitenskapelig ansatte. Det er derfor grunn til å tro at årsverksanslagene ville blitt noe høyere dersom denne arbeidsinnsatsen hadde blitt inkludert i større grad enn hva som var tilfellet.

Figur 4: Hovedtyper informasjonssikkerhets- og personverninitiativ i 2019



[15] Det samlede årsverkstallet som disse prosentandelene er beregnet ut ifra er hentet fra statistikken til DBH (https://dbh.nsd.uib.no/).

ØVRIGE INITIATIV I 2019

Figur 3 gir en oversikt over hvilke hovedtyper informasjonssikkerhets- og personverninitiativ som institusjonene rapporterte om for 2019. Figuren oppsummerer og kategoriserer alle initiativene som de 21 institusjonene rapporterte om.

Antallet tiltak som oppsummeres i figuren kan gi et noe misvisende bilde av aktiviteten i 2019. Årsaken til dette er at enkelte initiativ omfatter flere enkeltstående aktiviteter. Eksempler på dette kan være «kurs for ansatte i GDPR» eller «opplæring i risikovurderinger». Begge disse initiativene kunne romme flere kurssamlinger eller mange enkeltkurs, men rapporteres likevel som kun to initiativ i figur 4. Det betyr at aktiviteten i 2019 var noe større enn det som fremgår av figuren.

Fremfor å legge for stor vekt på antallet initiativ (ca. 240), er profilen – hvordan initiativene fordeler seg mellom de fire kategoriene (tekniske, organisatoriske, pedagogiske og fysiske) – det mest anmerkningsverdige i figur 4. Dette fordi profilen indikerer hva institusjonene mente det var mest verdt å anvende ressursene på.

Av figuren ser vi at organisatoriske initiativ (90) og pedagogiske initiativ (85) var hyppigst forekommende blant de 21 institusjonene i 2019. Tekniske initiativ (59) fulgte som en god nummer tre, mens det ble rapportert om få fysiske initiativ (5).

De fleste organisatoriske initiativene var systemtiltak. Mange institusjoner rapporterte for eksempel om at de hadde videreutviklet sine ledelsessystemer for informasjonssikkerhet eller ferdigstilt internkontrollen for GDPR (eller begge deler). Tydeliggjøring av rollene i sikkerhetsorganisasjonen, revisjoner av sikkerhetsstrategier/-policyer og innlemmelse av ledelsessystemet i internkontrollen for GDPR (eller i institusjonenes generelle internkontrollsystemer) var eksempler på dette. Videre rapporterte institusjonene om konkrete aktiviteter som ble utført innenfor rammen av ledelsessystemene eller internkontrollen for GDPR. De hyppigst nevnte tiltakene var utarbeidelse av retningslinjer for behandling av personopplysninger, etablering av rutiner for sikker forvaltning av slike opplysninger og risikovurderinger av systemer eller tjenester.

DEFINISJONER

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

Fysiske initiativ:
Planlegging eller iverksetting av tiltak for å sikre verdier mot ulike typer fysiske miljøpåvirkning. Eksempler på dette kan være installasjon av nytt adgangskontrollsystem, kameraovervåking eller anskaffelse av alarmer eller sensorer for å motvirke tyveri, brann eller fuktskader.

Det var to hovedtyper pedagogiske initiativ som institusjonene rapporterte om. For det første skreddersydde opplærings- eller informasjonstiltak rettet mot ansatte med roller i informasjonssikkerhets- eller personvernarbeid, for eksempel systemeiere eller ledere i forskningsprosjekter. For det andre allmenne informasjonstiltak rettet mot alle studenter og ansatte. Deltakelse i nasjonal sikkerhetsmåned, og bruk av nanolæringskursene som inngår i denne årlige kampanjen, var et annet vanlig pedagogisk tiltak[16]. Også øvelser på håndtering av informasjonssikkerhets- eller personvernhendelser ble nevnt av en del institusjoner.

De tekniske initiativene dreide seg om tiltak som helt eller delvis hadde styrking av IT-sikkerheten som siktemål. Det initiativet som flest institusjoner rapporterte om, var innføring av tofaktorautentisering. Andre vanlige initiativ inkluderte bruk av tredjepartsverktøy for oppfølging av brukeratferd og re-konfigurering av datanettverk, for eksempel intern segmentering av campus-nettet og skjerming av viktige dataressurser fra internettet. Til slutt ble det rapportert om tiltak for å beskytte brukere og systemer mot nett-trusler (blant annet DNS brannmur).

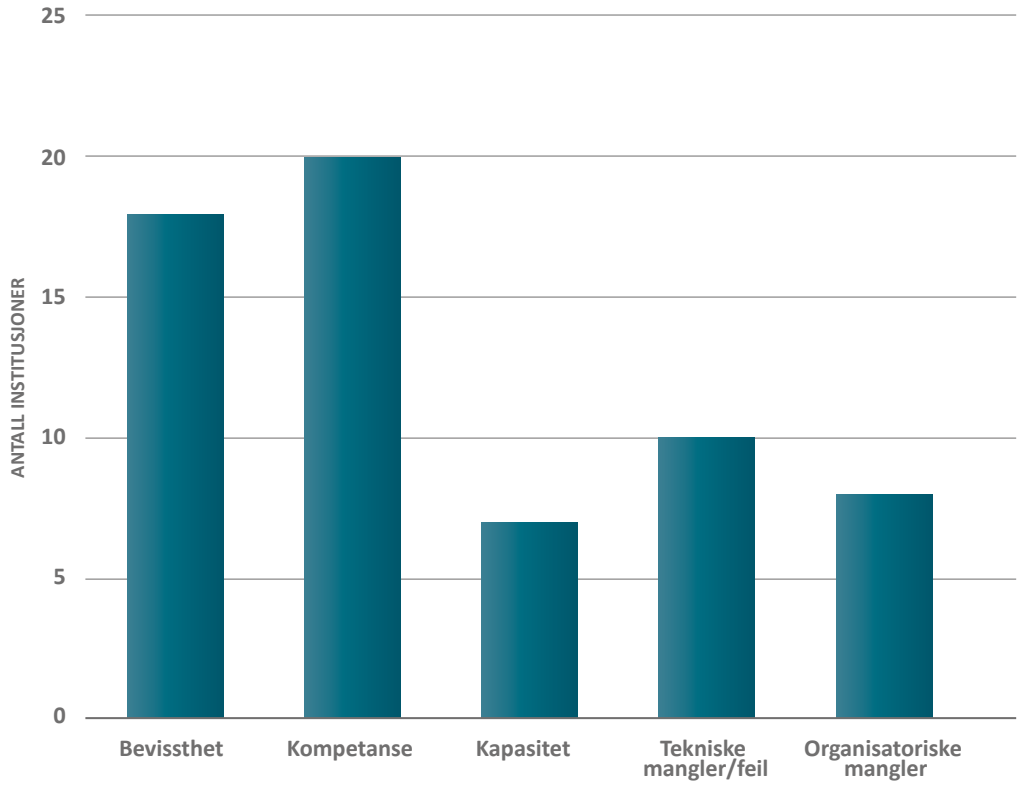
Det ble i liten grad rapportert om fysiske initiativ. De få initiativene som ble nevnt gjaldt adgangskontroll, kvalitetssikring av bruken av overvåkningskamera, etablering av redundante føringsveier og oppgradering av reservestrømløsning.

FORTSATT SÅRBARHETER

Institusjonene ble også bedt om å gjøre rede for hvilke sårbarheter de var bekymret for, det vil si forhold hos dem selv som de mente kunne utløse uønskede informasjonssikkerhets- eller personvernhendelser. Figur 5 viser hvor mange institusjoner som oppga at de var bekymret for de ulike sårbarhetene i figuren.

Figur 5 viser at 18 institusjoner mente at bevissthet om informasjonssikkerhets- og personvernutfordringer var en viktig sårbarhet, mens 20 institusjoner rapporterte at kompetanse om hvordan slike utfordringer best kunne håndteres var en viktig mangelvare [17]. Tekniske feil ble vurdert som den tredje viktigste sårbarheten (rapportert av 10 institusjoner). Organisatoriske mangler og begrenset kapasitet (personalressurser) ble nevnt av færrest institusjoner (henholdsvis sju og åtte institusjoner).

Figur 5: Rapporterte sårbarheter i 2019



[16] Se https://norsis.no/nsm/om-nasjonal-sikkerhetsmaned/.

[17] Det er ikke bare i universitets- og høgskolesektoren dette synes å være tilfelle. Se for eksempel «Mørketallsundersøkelsen 2018», side 20 (https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf).

Bevissthet og kompetanse sammenfaller med det som i figur 4 ble omtalt som pedagogiske initiativ. Formålet med pedagogiske initiativ er å styrke bevisstheten blant studenter og ansatte, og kompetansen hos medarbeidere med ansvar for å behandle og sikre personopplysninger og andre verdier. Ettersom institusjonene rapporterte om en rekke pedagogiske initiativ i 2019, kan det derfor virke paradoksalt at bevissthet og kompetanse likevel ble oppgitt som de viktigste sårbarhetene. Mente institusjonene at disse initiativene ikke hadde hatt den ønskede effekten?

For det første opplyste institusjonene – spesielt personvernombudene – om økende bevissthet blant administrativt og vitenskapelige ansatte. Dette kom til uttrykk ved at alle personvernombudene rapporterte om at de mottok flere spørsmål om lovlig og sikker behandling av personopplysninger enn tidligere. Dette indikerer at de pedagogiske initiativene kan ha hatt effekt (ved å føre til flere spørsmål). For det andre (og som vi skal se i neste kapittel) kan grunnen til at bevissthet og kompetanse ble oppgitt som viktige sårbarheter være endringer i trusselbildet. Poenget er at når trusselbildet blir mer utfordrende og komplisert, stilles det økende krav til bevissthet og kompetanse. Og i møtet med et mer komplekst trusselbilde i stadig endring, vil dette fort kunne bli noe du ikke får nok av – og som må styrkes og oppdateres jevnlig for å være relevant.

Det er verdt å merke seg at relativt få institusjoner oppfattet organisatoriske sårbarheter/mangler som viktige årsaker til at uønskede informasjonssikkerhets- og personvernhendelser kunne skje. Som vi så i figur 4, kan dette henge sammen med at institusjonene rapporterte at de i 2019 hadde planlagt eller iverksatt en del organisatoriske initiativ. Det kan derfor tenkes at denne innsatsen gjorde at institusjonene var mindre bekymret for at organisatoriske svakheter, for eksempel uklar oppgavefordeling eller mangelfulle rutiner, skulle føre til uønskede hendelser.

Samtidig ble institusjonene spurt særskilt om rutiner for ivaretakelse av sine GDPR-plikter i forbindelse med anskaffelse og oppfølging av databehandlere. Her rapporterte samtlige institusjoner at dette delvis var på plass. Det var imidlertid bare noen få institusjoner som hadde rutiner for oppfølging av databehandlere, det vil si periodisk kontroll med at vilkår i databehandleravtaler ble overholdt. Flere institusjoner opplyste om at denne organisatoriske sårbarheten ville bli rettet i forbindelse med planlagte revisjoner av internkontrollen for GDPR eller ledelsessystemet for informasjonssikkerhet.

Kapasitetsmangel (personalressurser) ble nevnt som særskilt bekymringsfullt av relativt få institusjoner. Selv om vi har sett at antallet årsverk dedikert til arbeidet med informasjonssikkerhet og personvern økte i 2019, er dette likevel noe overraskende [18].

Når det gjaldt de tekniske sårbarhetene som det ble rapportert om, handlet dette primært om feil (sikkerhetsbrudd) som hadde oppstått hos databehandlere. Det ble i liten grad rapportert om sårbarheter knyttet til internt driftede dataressurser (systemer, tjenester eller nettverk).

[18] Enkelte institusjoner rapporterte for eksempel om at oppfølging av tekniske sikringstiltak kunne lide under personellmangel. Dette gjaldt blant annet gjennomgang og kontroll av sikkerhetslogger.

KAPITTEL 2

TRUSLER OG HENDELSER

TRUSLER OG HENDELSER

INNLEDNING

I forrige kapittel ble det pekt på enkelte sårbarheter som fortsatt preger arbeidet med informasjonssikkerhet og personvern i sektoren. Spørsmålet som drøftes i dette kapitlet er i hvilken grad disse sårbarhetene har ført til uønskede informasjonssikkerhets- eller personvernhendelser i 2019.

Uønskede informasjonssikkerhets- og personvernhendelser utløses av trusselkilder, det vil si ulike typer «kilder til fare»[19]. Når det gjelder informasjonssikkerhet (inkludert personopplysningssikkerhet) kan det dreie seg om eksterne trusselkilder, for eksempel kriminelle grupper og APT/statsaktører. Men det kan i tillegg handle om interne trusselkilder, for eksempel at hendelser utløses av vitenskapelige ansatte med manglende sikkerhetskompetanse.

Også når det gjelder personvernhendelser handler det vanligvis om både interne og eksterne trusselkilder. Eksempler på interne trusselkilder er studenter som behandler personopplysninger i strid med interne retningslinjer eller at administrativt ansatte gjør feil i sin håndtering av personopplysninger. I tillegg kan det finnes en rekke andre «kilder til fare» (inkompetente tjenesteleverandører, gjesteforskere fra visse land, osv.).

Kjennskap til trusselkilder og uønskede hendelser – og hvordan dette endrer seg eller er stabilt over tid (trend-linjen) – er viktig for å vurdere risiko i sektoren. Risikobildet i sektoren drøftes særskilt i det siste kapitlet. Institusjonene og virksomhetene kan benytte oversikten over trusler og hendelser i dette kapitlet i sine egne risikovurderinger av informasjonssikkerhet og personvern.

I resten av kapitlet gis først en kort oversikt over hvordan nasjonale og utenlandske sikkerhetsmyndigheter og andre sikkerhetsaktører vurderer «kilder til fare» i forskning og høyere utdanning. Deretter følger en oversikt over informasjonssikkerhetshendelser som de 21 statlige universitetene og høgskolene rapporterte at de hadde vært utsatt for i 2019. Det gis samtidig en oversikt over de viktigste trusselaktørene.

Til slutt gis en oversikt over de personvernhendelser som institusjonene rapporterte om.

DET INTERNASJONALE TRUSSELBILDE

Internasjonalt – og spesielt i USA – har informasjonssikkerhet lenge vært rangert blant de aller viktigste fokusområdene i forbindelse med digitalisering i høyere utdanning og forskning[20]. I EDUCAUSE sin 2019-oversikt av de 10 mest betydningsfulle IT-områdene i amerikansk høyere utdanning og forskning, ble utarbeidelse og iverksetting av informasjonssikkerhetsstrategier rangert som viktigst. Personvern ble rangert som det tredje viktigste fokusområdet[21].

Informasjonssikkerhet og personvern i høyere utdanning og forskning har også fått større oppmerksomhet utenfor USA i løpet av 2019, blant annet på grunn av flere høyprofilerte sikkerhetsbrudd[22]. Blant annet publiserte søsterorganisasjonen til Nasjonal sikkerhetsmyndighet i Storbritannia – National Cyber Security Center (NCSC) – en egen vurdering av digitale sikkerhetstrusler i universitetssektoren[23]. Hovedkonklusjonen fra NCSC sin trusselvurdering var todelt, og har (som vi skal se i senere kapitler) også relevans for Norge:

1. Nettkriminelle grupper er den mest umiddelbare digitale sikkerhetstrusselen mot universiteter i Storbritannia.

2. Det er høy grad av sannsynlighet for at universitetssektoren vil være et prioritert mål for statsstøttet dataspionasje. Dette er vurdert som den største langsiktige digitale sikkerhetstrusselen i høyere utdanning og forskning i Storbritannia.

Sikkerhetsaktører i privat sektor samler og publiserer også data som viser utviklingen i det internasjonale trusselbildet i kunnskapssektoren. Det amerikanske selskapet Verizon utgir hvert år den kanskje mest omtalte sikkerhetsrapporten.

---

[19] Denne definisjonen av trusler er hentet fra Direktoratet for digitalisering sin begrepsliste (https://internkontroll-infosikkerhet.difi.no/begrepsliste#Trusler%20eller%20trusselkilder).

[20] Se for eksempel EDUCAUSE Review Special Report: Top 10 IT Issues 2011, side 28 (https://er.educause.edu/articles/2011/5/topten-it-issues-2011).

[21] Se EDUCAUSE Review Special Report: Top 10 IT Issues 2019 (https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2019), side 10.

I selskapets 2019-rapport legges det vekt på at kunnskapssektoren fortsatt er utsatt for trusler fra nettkriminelle grupper og statsstøttede aktører (APT-er[24])[25].

VURDERINGENE TIL NASJONALE SIKKERHETSTJENESTER

Disse trussel- og risikovurderingene deles i stor grad av norske sikkerhetstjenester: Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten.

I Nasjonal sikkerhetsmyndighet sin nasjonale risikovurdering for 2019 uttrykkes bekymring for at forskning er potensielle mål for fremmede staters etterretningsvirksomhet, og i Politiets sikkerhetstjeneste sin trusselvurdering for 2020 formidles en forventning om at utenlandsk etterretning vil rette spionasje mot norske forskningsmiljøer. Spionasjetrusselen som PST mener at norske forskningsmiljøer vil bli utsatt for utdypes på følgende måte:

> *«Utenlandske etterretningstjenester vil derfor kunne søke å infiltrere norske forskningsmiljøer innen kjernefysikk, fysikk, kjemi, biologi, toksikologi, farmasi, undervanns- og dypvannsteknologi, kontrollsystemer, styringssystemer, autonome fartøy, mønstergjenkjenning (kunstig intelligens), ingeniørdesign, nanoteknologi, satellitt- og missilteknologi, samt teknologi tilpasset arktiske forhold. Flere av disse fagområdene er også relevante for stater med programmer for utvikling av masseødeleggelsesvåpen (MØV).»*

I tillegg mener PST at internasjonalt forsknings- og utdanningssamarbeid kan bidra til «(...) andre staters sikkerhetstruende virksomhet mot Norge og andre land.»[28]

I Etterretningstjenestens årlige vurdering – Fokus 2020 – gjentas mye av det samme. Det hevdes for eksempel at norske universiteter og forskningsinstitusjoner systematisk benyttes av land som søker kunnskap om masseødeleggelsesvåpen. Tjenesten mener også at forskere og studenter fra enkelte land nyttiggjør seg norsk forskningsinfrastruktur (laboratorier, tungregneanlegg, osv.) til å skaffe seg kunnskap som reguleres av eksportkontrollregelverket[29].

---

[22] Australian National University var i flere måneder i 2018 utsatt for et større digitalt angrep fra ukjente trussel-aktører. Sikkerhetsbruddet fikk stor oppmerksomhet i australske og britiske massemedia. Se «Incident Report: On the Breach of the Australian National University's Administrative Systems» (https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach).

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

[24] APT-er definers av sikkerhetsselskapet Kaspersky som trusselaktører som "(...) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences". Dette er ofte (men ikke alltid) statlige eller statsstøttede grupper (https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats). Se også drøftelser i neste kapittel.

[25] Verizon: 2019 Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/dbir/).

[26] Nasjonal sikkerhetsmyndighet: Risiko 2019. Krafttak for et sikrere Norge, side 11 (https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf).

[27] Politiets sikkerhetstjeneste: Trusselvurdering 2020, avsnittet «Forskning og utvikling» (https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/).

[28] Ibid.: avsnittet «Forskning og utvikling».

[29] Etterretningstjenesten: Fokus 2020. Etterretningstjenestens vurdering av aktuelle sikkerhetstrusler, side 34-35 (https://forsvaret.no/presse_/ForsvaretDocuments/Fokus2020-web.pdf).

INFORMASJONSSIKKERHETSHENDELSER I 2019

I hvilken grad har trusselkildene som nasjonale og internasjonale sikkerhetstjenester er opptatt av – og andre «kilder til trusler» mot sektorens verdier – ført til uønskede informasjonssikkerhets- og personvernhendelser i 2019?

Totalt rapporterte de statlige universitetene og høgskolene om i overkant av 2500 informasjonssikkerhetshendelser i løpet av 2019, inkludert brudd på eller forsøk på brudd på personopplysningssikkerheten [30]. Tallene fra Uninett CERT – 792 registrerte IT-sikkerhetshendelser – inngår ikke i totaltallet [31].

Alle institusjoner rapporterte om at de hadde vært utsatt for hendelser på informasjonssikkerhetsområdet i 2019, og det totale antallet hendelser som ble rapportert var høyere enn i 2018. Det er også verdt å merke seg at det store flertallet av rapporterte hendelser og avvik handler om IT-sikkerhet (eller digital sikkerhet), spesielt nettbaserte hendelser. De resterende hendelsene handlet om andre typer hendelser, spesielt menneskelige feil og brudd på rutiner (innside-hendelser, se nedenfor).

ENDRINGER SIDEN 2018

Det totale antallet rapporterte informasjonssikkerhets-hendelser for 2019, er altså noe høyere enn hva som ble rapportert for 2018. NTNU rapporterte for eksempel om en økning i antallet IT-sikkerhetshendelser fra 2018 til 2019. UiO CERT rapporterte imidlertid om en liten nedgang i registrerte IT-sikkerhetshendelser sammenliknet med 2018. Samtidig oppga UiO CERT at andelen hendelser med stort skadepotensial hadde økt (flere farlige hendelser). De øvrige institusjonene rapporterte om at hendelsesomfanget var omtrent det samme i 2019 som i 2018.

En viktig endring var likevel at mange institusjoner mente at forsøkene på nettsvindel, for eksempel faktura- eller direktørsvindel, hadde økt noe, og at forsøkene hadde blitt mer profesjonelle og troverdige enn før. Det ble særlig påpekt at språket i nettfiske-epostene var forbedret, og at de inneholdt informasjon (blant annet om ledere eller ansatte) som viste at det var gjort et grundigere forarbeid enn hva man hadde sett tidligere.

Institusjonene rapporterte også om visse endringer i typer hendelser. Særlig påfallende var nedgangen i antallet hendelser med løsepengevirus. Dette er hendelser hvor nettkriminelle tar kontroll over digitale verdier (informasjon og dataressurser), blokkerer institusjonens tilgang til verdiene (krypterer data) og krever penger for å gi kontrollen tilbake til institusjonen. Relativt mange institusjoner rapporterte at de hadde vært utsatt for løsepengevirus i 2018. I 2019 var det få institusjoner som rapporterte om det samme.

OM HENDELSES- OG AVVIKSRAPPORTERINGEN

I kartleggingen for 2019 ble ikke institusjonene bedt om å rapportere på forhåndsdefinerte hendelser/avvik. Det eneste Unit ba om var at institusjonene ga en oversikt over hvilke hendelser de hadde vært utsatt for, og som de selv mente det var verdt å nevne. Det ble derfor rapportert på noe ulik måte fra de forskjellige institusjonene. Likevel mener vi at presentasjonen nedenfor gir et rimelig dekkende bilde av sektortilstanden, slik den ble rapportert til Unit.

[30] Totaltallet på omkring 2500 hendelser inkluderer ikke rapporteringer hvor antall hendelser ble oppgitt på en svært omtrentlig måte, for eksempel «gjentatte forsøk på nettfiske», og som derfor ikke lot seg tallfeste.

[31] Uninett CERT rapporterte om at uønskede hendelser i forskningsnettet stort sett var de samme i 2019 som i 2018. Trusselbildet hadde derfor ikke forandret seg i vesentlig grad. De uønskede hendelsene som var representert i størst grad i Uninett CERT sin statistikk for 2019, var (i) sårbarheter (tekniske sikkerhetshull i for eksempel applikasjoner eller operativsystem som kan føre til datainnbrudd – 400 hendelser), og (ii) kompromitterte datamaskiner (datamaskiner som hadde blitt utsatt for vellykkede dataangrep – 210 hendelser).

Nedgangen i antallet hendelser med løsepengevirus står i motsetning til utviklingen internasjonalt. Både i kunnskapssektoren [32] og i andre deler av offentlig (og privat) sektor var løsepengevirus et voksende problem i 2019[33]. Statistikk fra Microsoft antyder imidlertid at Norge var blant de landene i Europa som var minst utsatt for løsepengevirus i 2019 [34]. Det kan tenkes at norske universiteter og høgskoler har nytt godt av dette.

Til slutt kan to andre utviklingstrekk nevnes. For det første at nedgangen i antallet tjenestenektangrep fortsatte i 2019[35]. For det andre at det ikke ble meldt om misbruk av institusjonenes dataressurser til utvinning av kryptovaluta (Bitcoin, Monero, osv.) i 2019. I 2018 ble det meldt om flere tilfeller av denne formen for misbruk av dataressurser.

KATEGORISERING AV HENDELSER

De omkring 2500 informasjonssikkerhetshendelsene som institusjonene rapporterte om kan deles inn i disse hovedkategoriene:

- **Nettkriminalitet** **ca. 2360 hendelser.**
- **Innsidehendelser:** **ca. 100 hendelser.**
- **Tekniske hendelser:** **ca. 60 hendelser[36].**
- **APT/statsaktører:** **1-2 hendelser.**
- **Andre typer hendelser:** **11 hendelser.**

NETTKRIMINALITET

Ca. 2360 hendelser kan (mest sannsynlig) kategoriseres som ulike former for nettkriminalitet[37]. Med nettkriminalitet menes sikkerhetstruende aktivitet som gjennomføres via internett og hvor motivet er økonomisk vinning. Trusselaktørene er enten organiserte kriminelle grupper eller enkeltpersoner.

Nettkriminell aktivitet som flest institusjoner rapporterte om:

1. Nettfiske, målrettet nettfiske («spydfiske», sosial manipulasjon) var den typen hendelser som flest institusjoner rapporterte om. Hendelsene innebar vanligvis at brukere mottok e-poster med lenker til nettsider kontrollert av kriminelle aktører. Her ble brukerne bedt om å oppgi brukernavn og passord.

2. Kompromitterte brukerkontoer ble rapportert av nest flest institusjoner. Hendelsene dreide seg vanligvis om at brukere oppga brukernavn og passord på nettsider kontrollert av nettkriminelle aktører. Deretter ble de kompromitterte brukerkontoene misbrukt på ulike måter. Vanligvis handlet dette om utsendelse av søppel-epost eller utsendelse av nye nettfiske-eposter til andre studenter eller ansatte.

3. Direktørsvindel ble rapportert av tredje flest institusjoner. Det innebar at ansatte (spesielt på økonomiavdelingene) mottok e-poster fra nettkriminelle aktører. I e-postene utga aktørene seg for å være ledere ved institusjonene. «Lederne» ba om at de ansatte foretok hasteutbetalinger til bankkontoer kontrollert av de nettkriminelle aktørene.

4. Fakturasvindel ble rapportert av noen færre institusjoner enn direktørsvindel. Dette er en form for nettsvindel som likner på direktørsvindel: ansatte (spesielt i økonomiavdelinger) mottok falske og troverdige fakturaer fra nettkriminelle aktører. Dersom betalingene ble gjennomført ble pengene overført til en bankkonto kontrollert av de nettkriminelle aktørene. Det ble rapportert om ett tilfelle hvor et større beløp hadde blitt utbetalt (se nedenfor).

---

[32] Se for eksempel CrowdStrike: 2020 Global Threat Report, side 15-24 https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/
For eksempler på løsepengevirus-angrep i kunnskapssektoren, se Reuters, 5. februar 2020: University of Maastricht Says it Paid Hackers 200 000-euro Ransom (https://www.reuters.com/article/us-cybercrime-netherlands-university/university-of-maastricht-says-it-paid-hackers-200000-euro-ransom-idUSKBN1ZZ2HH), eller BBC, 10. desember 2019: Thousands of Students in Germany Queue for Email Access (https://www.bbc.com/news/technology-50838673).

[33] Se også Europol: Internet Organized Crime Threat Assessment 2019, avsnitt 4.2 (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019).

[34] Specops (2020): The European Countries Most at Risk of Cyber-Crime (https://specopssoft.com/blog/european-countries-cyber-crime/).

[35] Slike angrep innebærer at tilgangen til nettressurser blokkeres eller forsinkes ved at ressursene utsettes for store mengder «falsk» datatrafikk.

[36] Dette tallet er noe usikkert. Årsaken er at én institusjon oppga at den i 2019 hadde håndtert «en del saker som gjelder gamle og sårbare systemer og nettsider», men uten at dette ble nærmere konkretisert.

[37] For analyser av nettkriminalitet, se for eksempel E. R. Leukfeldt og Thomas J. Holdt (2019): «Examining the Social Organization of Cyber-Criminals in the Netherlands Online and Offline». International Journal of Offender Therapy and Comparative Criminology. Vol. 64, Issue 5, side 522-538. Se også Jonathan Lusthaus (2018): Industry of Anonymity: Inside the Business of Cybercrime. Cambridge, Mass.: Harvard University Press, eller Brian Krebs (2014): Spam Nation. The Inside Story of Organized Cybercrime – From Global Epidemic to Your Front Door. Naperville, Ill.: Sourcebooks.

ANNEN NETTKRIMINALITET I 2019:

Det ble i tillegg rapportert om enkelte andre typer hendelser som mest sannsynlig kan kategoriseres som nettkriminalitet:

- kompromitterte informasjonsverdier:
  trussel-aktører hadde fått tilgang til institusjonenes data eller informasjon,
- IoT-hacking:
  kompromittering av videokameraer som senere ble brukt i dataangrep (tjenestenekt) mot andre virksomheter,
- utpressingsepost:
  ansatte som mottok eposter med trussel om offentliggjøring av belastende personlig informasjon dersom penger ikke ble utbetalt,
- angrepsforberedelser:
  skanning av datanettverk for å finne sikkerhetshull, og
- innbrudd i telefonløsning.

5. Skadevare. Det var relativt få institusjoner som rapporterte om at de hadde vært utsatt for skadevare. Disse hendelsene innebar at datamaskiner ble tilført uønsket funksjonalitet (eller «ondsinnet programvare»: datavirus, trojanere, osv.). Løsepengevirus er eksempel på skadevare som ble nevnt, men det ble også rapportert om trojanere. Trojanere benyttes ofte til innhøsting av brukeropplysninger uten at brukeren selv er klar over det, for eksempel passord eller kredittkortopplysninger (men har også en rekke andre bruksområder).

6. Kredittkorthendelser. Et par institusjoner rapporterte om kompromittering av kredittkortopplysninger. Kompromitteringen skjedde vanligvis ved at studenter eller ansatte oppga slike opplysninger på nettsider kontrollert av nettkriminelle aktører. Det ble ikke meldt om at disse hendelsene hadde ført til større økonomisk tap.

INNSIDEHENDELSER

Ca. 100 rapporterte hendelser eller avvik kan kategoriseres som innsidehendelser. Med dette menes faktiske sikkerhetsbrudd eller nesten-brudd forårsaket av ikke-tekniske forhold hos institusjonene selv. Ikke-tekniske forhold omfatter ulike typer menneskelige feil eller avvik fra egne sikkerhetsrutiner. Det inkluderer ikke feil fremprovosert av eksterne trusselaktører, for eksempel nettkriminelle grupper. Typiske årsaker til innsidehendelser er begrenset brukerkompetanse, manglende bevissthet/sikkerhetskultur, bekvemmelighet, tidspress, eller uklare ansvarsforhold [38].

Innsidehendelser som flest institusjoner rapporterte om:

1. Rutinebrudd var den typen innsidehendelser som flest institusjoner opplyste om at de hadde vært utsatt for. Slike avvik handlet blant annet om at ansatte eller studenter lånte ut (eller delte) sine ID-kort eller påloggingsinformasjon (brukernavn/passord) til andre ansatte eller studenter. Dette kunne (i enkelte tilfeller) føre til uautorisert tilgang til skjermverdig eller sensitiv informasjon eller dataressurser.

2. Feil publisering av dokumenter/personopplysninger ble rapportert av nest flest institusjoner. Disse hendelsene kjennetegnes av at skjermverdig eller sensitiv informasjon (som oftest personopplysninger) ble gjort tilgjengelige for uvedkommende via hjemmesider eller gjennom andre publiseringskanaler, for eksempel læringsplattformer.

3. Feilsending av e-post/SMS. Slike hendelser ble rapportert av færrest institusjoner. Det omfattet tilfeller hvor e-poster (med vedlegg) eller SMS med beskyttelsesverdig eller sensitivt innhold (som oftest personopplysninger) ble sendt til feil mottakere.

[38] Innsidehendelser omfatter også hendelser som skyldes uærlighet eller illojalitet. Institusjonene rapporterte ikke om tilfeller hvor dette var årsakene til innsidehendelser.

TEKNISKE HENDELSER

Ca. 60 hendelser kan kategoriseres som tekniske hendelser. Dette handlet primært om tekniske feil eller mangler i programvare. Slike feil/mangler kunne for eksempel føre til kompromittering av informasjon eller at systemer ble utilgjengelige for brukerne.

Tekniske hendelser som flest institusjoner rapporterte om:

1. Sårbarheter/sikkerhetshull. Enkelte institusjoner rapporterte om at de hadde oppdaget eller mottatt varsler om svakheter/mangler i programvare som kunne føre til brudd på sikkerheten. Det ble ikke meldt om at svakhetene/manglene faktisk hadde ført til slike brudd.

2. Utilgjengelighet og uautorisert eksponering. Dette gjaldt hendelser hvor elektroniske meldinger ikke hadde kommet frem til mottakerne, og at meldinger ble (potensielt) eksponert for uvedkommende.

APT/STATSAKTØRER

Det ble meldt om én eller to hendelser som involverte APT/statsaktører. Dette er brudd eller forsøk på brudd på informasjonssikkerheten som vanligvis skjer via internett og hvor motivet primært er dataspionasje/tyveri[39].

Trusselaktørene er vanligvis ressurssterke grupper med tilknytning til ulike lands statsapparat (enten statsansatte hackere eller private hackergrupper – nettkriminelle – som utfører oppdrag på bestilling fra eller i samforstand med sine respektive myndigheter). Gruppene jobber ofte målrettet og langsiktig – de er vanskelig å oppdage, vanskelig å identifisere og vanskelige å fjerne dersom de har lyktes med å få fotfeste i datanettverket.

Følgende hendelser som involverte (eller kunne involvere) APT/statsaktører ble rapportert:

- Mistanke om brudd på eksportkontrollrestriksjoner hos én institusjon. Mistanken gjaldt datatyveri fra nanoteknologilaboratorium utført på oppdrag fra iranske myndigheter.

- Mistanke om forsøk på dataspionasje hos én institusjon. Dette gjaldt medlemmer i en delegasjon fra Kina som delte ut minnepinner til forskere.

I tillegg ble det rapportert om enkelte mistanker om APT/statsaktøraktivitet.

I fjorårets kartlegging opplyste flere institusjoner at de hadde vært utsatt for datatyveri fra vitenskapelige tidsskriftdatabaser, trolig utført av en iransk APT (kjent som «the Mabna Institute» eller «Silent Librarian»[40]). Det ble ikke meldt om slik APT-aktivitet i 2019.

ANDRE TYPER HENDELSER

Dette er en restkategori. Den inkluderer rapporter om hendelser som ikke naturlig hører til i kategoriene ovenfor. Det ble rapportert om 11 slike hendelser for 2019. Dette gjaldt for eksempel tyveri av IT-utstyr (bærbar pc), sosial manipulasjon via telefon og manglende tilgang til ekstern tjeneste. I tillegg ble det nevnt ett tilfelle med mulig datatap på grunn av en løsepengevirus-hendelse hos et samarbeidende universitet i utlandet (Universitetet i Maastricht)[41].

[39] Enkelte APT/statsaktører har også andre mål med sin virksomhet, for eksempel dataødeleggelse, sabotasje (fysisk skade) eller tjenesteforringelse. For analyser av APT/statsaktører, 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 FireEye: M-Trends 2019 (https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html).

[40] «The Mabna Institute» («Silent Librarian» eller «Cobalt Dickens») er en privat nettkriminell gruppe i Teheran som koordinerer deler av sin virksomhet med iranske myndigheter. 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 NRK (2018): Avsløret av FBI: 44 norske top-forskere utsatt for hackerangrep fra Iran (https://www.nrk.no/norge/pst_-_-iran-bak-hacking-av-norske-universiteter-1.14044442).

[41] Se Sergui Gatlan (2020): "TA505 Behind Behind Maastricht University Ransomware Attack". Bleeping Computer (https://www.bleepingcomputer.com/news/security/ta505-hackers-behind-maastricht-university-ransomware-attack/).

ALVORLIGHETSGRAD OG VANLIGE SKADEVIRKNINGER

Som vi har sett, rapporterte institusjonene om forholdsvis mange informasjonssikkerhetshendelser og avvik i 2019. Institusjonene mente imidlertid at de aller fleste hendelsene hadde relativt små skadevirkninger. Dette mønsteret med forholdsvis mange hendelser og få alvorlige skadevirkninger, så vi også i kartleggingen for 2018.

Ovenfor har vi nevnt at det ble rapportert om flere hendelser med stort skadepotensial i 2019 enn i 2018. Eksempler på dette var målrettede forsøk på direktørsvindel, spamkampanjer av et visst omfang og viktige sårbarheter i systemer eller nettsider.

Følgende skadevirkninger ble rapportert å være de mest vanlige i 2019:

- Krenkelser av personvernet. I denne sammenheng vil dette si uautorisert tilgang til eller eksponering av opplysninger om enkeltpersoner, ofte som følge av innsidehendelser (for eksempel offentliggjøring av personopplysninger på hjemmesider eller feilsending av e-poster).

- Uautorisert bruk av dataressurser. Bruk av kompromitterte brukerkontoer til masseutsendelse av søppel-epost eller at kompromittert IT-utstyr (internett -tilkoblede videokamera) ble brukt i dataangrep mot andre virksomheter.

- Omdømmetap. Enkelte negative medieoppslag som følge av informasjonssikkerhetesbrudd eller avvik, eller i forbindelse med at dataressurser ble misbrukt til masseutsendelse av søppel-epost (svartelisting hos leverandører).

- Tapt arbeidstid. Kortere perioder med produksjonstap på grunn av manglende eller ustabil tilgang til digitale systemer eller tjenester.

- Erstatningskostnader. Mindre økonomiske tap i forbindelse med gjenkjøp av stjålet IT-utstyr (vanligvis bærbare datamaskiner).

- Direkte økonomisk tap. Mindre økonomiske tap i forbindelse med nettsvindel, spesielt direktørsvindel. Tapene beløp seg til mellom 5000 og 10 000 kroner, men i ett tilfelle var det snakk om et større beløp (se nedenfor).

- Oppryddingskostnader. Kostnader knyttet til institusjonenes håndtering av informasjonssikkerhets-hendelser og avvik (ekstraarbeid).

Av hendelser som ble rapportert å ha medført større/ alvorlige skadevirkninger, er følgende tilfeller verdt å nevne spesielt:

- Fakturasvindel. Utbetaling av ca. 12 millioner kr. (1,2 millioner euro) til en nettkriminell aktør etter mottak av et forfalsket innbetalingskrav på bestilt medisinsk utstyr [42].

- Mistanke om statsstøttet dataspionasje. Iranske gjesteforskere ga besøkende forskere fra hjemlandet uautorisert tilgang til laboratorium hvor det ble forsket på flerbruksteknologi (teknologi som både har sivile og militære anvendelsesområder). I tillegg var det mistanke om at forskerne hadde eksponert laboratorieutstyr mot internettet.[43]

- Innbrudd i telefoniløsning. Innbruddet medførte at institusjonen ble påført et «betydelig økonomisk tap» (tapet ble ikke tallfestet nærmere).

Det er i tillegg verdt å nevne et par hendelser hvor det var tvil om det faktisk hadde skjedd et sikkerhetsbrudd og hvor eventuelle skadevirkninger derfor var ukjent. Dette gjaldt en hendelse med kompromittering av server, hvor en ukjent trusselaktør hadde hatt tilgang til serveren over en lengre periode (minst 100 dager [44]). Institusjonen hadde likevel ikke registrert konkrete skadevirkninger som følge av kompromitteringen.

En annen institusjon rapporterte om indikasjoner på IT-sikkerhetsbrudd. Hva indikasjonene kunne bety var institusjonen usikker på: det kunne bety at «noen» hadde hatt tilgang til institusjonens datanettverk.

Den siste hendelsen indikerer at sektoren kan være utsatt for «tause» hendelser: uønsket nettaktivitet rettet mot digitale verdier som institusjonene mangler verktøy og kapasitet til å oppdage. Flere andre institusjoner hadde mistanker om «tause» hendelser [45].

[42] Saken fikk en viss medieoppmerksomhet i desember 2019. Se for eksempel nyhetsoppslag hos NRK (https://www.nrk.no/tromsogfinnmark/et-av-norges-storste-universitet-svindlet-for-12-millioner-1.14830758). I etterkant av hendelsen sendte Kunnskapsdepartementet ut et brev til sine underliggende virksomheter hvor det ble oppfordret til ekstra overvåkenhet ved håndtering av innkommende betalingskrav.

[43] Saken fikk medieoppmerksomhet i januar 2020. Se for eksempel VG (https://www.vg.no/nyheter/innenriks/i/jd73bb/to-ntnu-forskere-siktet-av-pst) eller NRK (https://www.nrk.no/trondelag/ntnu-begynte-a-mistenke-de-to-siktede-forskerne-allerede-for-ett-ar-siden-1.14869687).

[44] Dette omtales som «dwell time» (oppdagelsestid): antallet dager fra første indikasjon på sikkerhetsbrudd til bruddet blir oppdaget. Ifølge datasikkerhetsselskapet FireEye, var gjennomsnittlig oppdagelsestid i vår del av verden 175 dager i 2018 (FireEye: M-Trends 2019, side 7. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html). I 2019 hadde oppdagelsestiden sunket til 54 dager, dels på grunn av flere løsepengevirus-angrep (FireEye: M-Trends 2020, side 15. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html).

Til slutt ble det rapportert om at fire informasjons-sikkerhetshendelser hadde blitt politianmeldt i 2019.

Personvernhendelser – omfang og alvorlighetsgrad – diskuteres nedenfor.

PERSONVERNHENDELSER I 2019

Institusjonene rapporterte om 142 personvernhendelser i 2019. Dette tallet inkluderer også en del brudd på informasjonssikkerheten til personopplysninger.

19 institusjoner opplyste at de hadde registrert minst én (men vanligvis flere) personvernhendelser. To institusjoner hadde ikke registrert noen slike hendelser i 2019.

Vi har ikke tilsvarende tall fra fjorårets kartlegging (institusjonene ble ikke spurt spesielt om personvernhendelser). Det er derfor ikke mulig å si noe om endringer fra 2018.

Av de til sammen 142 personvernhendelsene ble 14 meldt til Datatilsynet. Institusjonene oppga at flertallet av meldte hendelser ikke var så alvorlige at det var nødvendig å varsle de berørte (eller «de registrerte»). I et par tilfeller ble dette imidlertid gjort. Her handlet det om at opplysninger om personer med hemmelig adresse var tilgjengelig via søketjenester på internettet, og et tilfelle hvor saks-dokumenter i en varslingssak hadde forsvunnet.

Det er videre verdt å merke seg at majoriteten av rapporterte personvernhendelser gjaldt forskningsområdet, spesielt studentforskning. Hendelsene handlet i hoved-sak om manglende overholdelse av interne rutiner, særlig krav om melding til NSD ved oppstart eller avslutning av forsknings- eller studentprosjekter. De ser derfor ikke ut til å ha medført alvorlige krenkelser av personvernet til deltakerne i forsknings- eller studentprosjekter.

I enkelte tilfeller førte avvikene fra rutiner for håndtering av personopplysninger i forskning til at opplysningene ble oppbevart lengre enn nødvendig. De mest alvorlige forskningshendelsene gjaldt imidlertid manglende informasjon til eller samtykke fra forskningsdeltakerne, og tilfeller hvor sensitive forskningsdata ble lagret på områder hvor dataene kunne ha vært tilgjengelige for uvedkommende (andre ansatte eller studenter). Det ble også rapportert om noen tilfeller hvor opplysninger om forskningsdeltakere ikke var tilfredsstillende anonymisert.

Personvernhendelser i den administrative virksomheten handlet særlig om feil ved bruk av e-post eller annen elektronisk kommunikasjon, for eksempel SMS, eller feil i forbindelse med publisering av informasjon i lærings-plattformer. Det ble i tillegg rapportert om et begrenset antall hendelser hvor det manglet behandlingsgrunnlag, eller hvor grunnlaget ikke var formelt fastsatt før behandlinger av personopplysninger tok til.

Personvernhendelser og avvik som flest institusjoner rapporterte om i 2019:

- Manglende melding til NSD ved oppstart av forskningsprosjekter og studentprosjekter.
- Manglende sluttmelding til NSD ved avslutning av forskningsprosjekter og studentprosjekter.
- Feil lagring av personopplysninger, spesielt i forskningsprosjekter og studentprosjekter.
- Uautorisert eksponering av (eller tilgang til) personopplysninger, for eksempel manglende skjerming av opplysninger ved elektronisk kommunikasjon.
- Manglende sletting av personopplysninger etter avslutning av forsknings- og studentprosjekter.

MINDRE VANLIGE PERSONVERNHENDELSER I 2019:

- Mangelfull anonymisering av deltakere i forskningsprosjekter.
- Mangelfull informasjon til forskningsdeltakere om behandlinger av personopplysninger i forskningsprosjekter.
- Manglende samtykke fra forskningsdeltakere til behandlinger av personopplysninger i forskningsprosjekter.
- Manglende behandlingsgrunnlag ved innsamling og videre behandling av personopplysninger.

[45] Sikkerhetsselskapet FireEye konkluderte med følgende etter en kartlegging av «tause» hendelser hos amerikanske universiteter: "The typical campus network has been compromised by a half dozen or more named APT groups at any given time (…) They have lingered on university networks for months, even years, and are only now being discovered". FireEye (2015): Storming the Ivory Tower. Why Cyber Attackers are Targeting Higher Education, and What Universities Can Do About It, side 3 (https://www.fireeye.com/current-threats/threat-intelligence-reports/wp-storming-the-ivory-tower.html).

IVARETAKELSE AV PERSONVERNRETTIGHETER

Noen institusjoner rapporterte om at de manglet tilfredsstillende rutiner for ivaretakelse av de registrertes rettigheter (retten til informasjon, innsyn, retting, sletting, begrenset behandling, osv.). Det er likevel vårt inntrykk at alle rettighetshenvendelser fra de registrerte (vanligvis studenter), for eksempel innsynskrav eller krav om sletting av egne opplysninger, ble behandlet på en seriøs måte. Dette til tross for at spesielt innsynskrav kunne være krevende å imøtekomme.

Innsynskrav, det vil si forespørsler om innsyn i egne personopplysninger, innebar vanligvis at institusjonene måtte fremskaffe og sammenstille opplysninger fra en rekke undervisningstjenester og administrative systemer. Institusjonene mente at flere av disse systemene og tjenestene ikke er tilfredsstillende tilrettelagt for effektiv ivaretakelse av personvernrettigheter, særlig innsynskrav. Behandling av innsynskravene var derfor arbeid som ofte tok tid og som krevde koordinering mellom mange ulike system- eller tjenesteeiere.

BRUK AV PERSONVERNRETTIGHETER

Samtidig rapporterte de 21 institusjonene om få rettighetshenvendelser i 2019. Til sammen handlet det om omkring 20 slike henvendelser. 12 institusjoner rapporterte at de ikke kjente til å ha mottatt rettighetshenvendelser.

Det ble ikke utelukket at rettighetsbruken kunne være noe større enn hva institusjonene opplyste om. Henvendelser kunne for eksempel gå direkte til systemeiere eller tjenesteansvarlige uten at dette ble kjent for andre ved institusjonen. Det ble også påpekt at deltakere i forskningsprosjekter av og til trakk tilbake samtykker som var gitt til behandling av personopplysninger. Disse henvendelsene er ikke inkludert i de omkring 20 rettighetshenvendelsene.

Det begrensede antallet rettighetshenvendelser kan tolkes som uttrykk for tillit til institusjonenes måte å behandle personopplysninger på, eller som liten interesse for personvern. Alternativt, kan det forstås som manglende kjennskap til regelverk og rettigheter, for eksempel fordi institusjonene ikke hadde informert tydelig nok om hva de registrerte (spesielt studenter) kan kreve.

KAPITTEL 3

DIREKTORATER OG SELSKAPER

DIREKTORATER OG SELSKAPER

INNLEDNING

I tillegg til universitetene og høgskolene, omfattes også direktorater og selskaper som er direkte underlagt Kunnskapsdepartementet av Units kartlegging av arbeidet med informasjonssikkerhet og personvern. Disse direktoratene og selskapene ble kartlagt av Unit[46] våren og høsten 2019. Neste kartlegging gjennomføres etter at denne rapporten er publisert. Funnene derfra vil bli publisert i neste års rapport.

Følgende virksomheter ble kartlagt av Unit i 2019:

- 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.
- Uninett AS.
- Norsk utenrikspolitisk institutt (NUPI).
- De nasjonale forskningsetiske komiteene (FEK).

I dette kapitlet følger først en kort gjennomgang av hvilke verdier/oppgaver som denne delen av UH-sektoren forvalter. Deretter gis en gjennomgang av trusler og uønskede hendelser. Så følger en oversikt over personalressurser dedikert til arbeidet og status for utarbeidelse og innføring av ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR.

Avslutningsvis følger en oversikt over hvilke sårbarheter som virksomhetene mente preget arbeidet med informasjonssikkerhet og personvern.

VIRKSOMHETENE OG VERDIENE

De virksomhetene som ble kartlagt i 2019 hadde til sammen omkring 1290 ansatte (heltid og deltid).

Størrelsen på disse virksomhetene gjør at de fleste av dem forvalter færre verdier – informasjonsverdier, dataressurser og økonomiske midler – enn/sammenlignet med universitetene og høgskolene. Likevel forvalter flere av virksomhetene, for eksempel NSD og Uninett, informasjonsverdier og dataressurser som er viktige for sektoren, og leverer tjenester på informasjonssikkerhets- og personverområdet. NFR spiller en avgjørende rolle for norsk forskning og innovasjon, for eksempel gjennom forskningsfinansiering (inkludert bevilgninger til utvikling av digitale forskningsinfrastrukturer) og utvikling av forskningspolitikk og strategiske satsninger.

De resterende virksomhetene ivaretar ulike forvaltningsoppgaver i høyere utdanning og forskning (Diku, NOKUT og FEK), eller utfører forskning innenfor til dels sensitive kunnskapsområder (Simula og NUPI).

TRUSLER OG HENDELSER

De åtte virksomhetene rapporterte om til sammen 42 hendelser. De fleste hendelsene hadde inntruffet i 2018. Alle virksomhetene hadde vært utsatt for hendelser som de fant det verdt å opplyse om. Som for universitetene og høgskolene, inkluderer ikke totaltallet hendelser som var for lite spesifikke til at et konkret antall kunne bestemmes, for eksempel «mange tilfeller med nettfiske».

De 42 rapporterte informasjonssikkerhets- og personvernhendelsene fordelte seg på hendelseskategoriene (diskutert i forrige kapittel) på følgende måte:

- Nettkriminalitet: 27 hendelser.
- Innsidehendelser: 7 hendelser.
- Tekniske hendelser: 5 hendelser.
- APT/statsaktører: 2 mistenkte hendelser.
- Andre typer hendelser: 1 hendelse.

Vi ser at hendelsesprofilen – hvordan enkelthendelser fordelte seg på de ulike kategoriene – i stor grad speiler det vi så hos de statlige universitetene og høgskolene: nettkriminalitet (nettfiske, faktura- og direktørsvindel, kompromitterte brukerkontoer, løsepengevirus og annen

[46] Unit omfattes av styringsmodellen for informasjonssikkerhet og personvern i UH-sektoren. Kartleggingen av Units eget arbeid med informasjonssikkerhet og personvern utføres av departementet.

skadevare) var den klart største hendelseskategorien. Deretter fulgte innsidehendelser (menneskelige feil – feilkonfigurering av tjenester, feil publisering, feilsending av e-post, osv.) og tekniske hendelser (vanligvis hos leverandører av tjenester og nettleverandører).

Når det gjaldt de to hendelsene som er kategorisert som APT/statsaktører, handlet dette om mistanker om data-spionasje/-tyveri, eller forsøk på dette. Her dreide det seg om mulig spionvare i minnepinner funnet etter et kinesisk delegasjonsbesøk.

Den andre mistenkte hendelsen dreide seg om servere som hadde vært kompromittert over en lengre periode, men hvor angriperen trolig ikke hadde tatt seg videre inn i virksomhetens datanettverk. Virksomheten rapporterte at NSM hadde bistått i håndtering av hendelsen, men det hadde ikke vært mulig å avgjøre om det var APT/statsaktør eller andre aktører (nettkriminelle) som stod bak[47].

Som hos universitetene og høgskolene, ble det også hos disse virksomhetene rapportert om få hendelser som gjaldt løsepengevirus, tjenestenektangrep og misbruk av dataressurser til utvinning av kryptovaluta.

Det ble ikke rapportert om at hendelsene hadde ført til alvorlige skadevirkninger. Det innebar for eksempel at faktura- og direktørsvindel ikke hadde ført til urettmessige utbetalinger (men i ett tilfelle ble utbetaling stoppet av banken). Det innebar også at løsepengevirus-angrepene var såpass små og avgrensede at de ikke hadde medført skadevirkninger av betydning (og hadde heller ikke ledet til utbetaling av løsepenger).

Det ble imidlertid rapportert om enkelte tilfeller med urettmessig eksponering av personopplysninger, det vil si krenkelser av personvernet. Dette gjaldt opplysninger om virksomhetenes egne ansatte, det var snakk om relativt små mengder opplysninger og det handlet ikke om sensitive personopplysninger.

I tillegg ble det rapportert om innbrudd i og misbruk av telefonløsning.

PERSONALRESSURSER

Personvernombudene utgjorde 30 prosent av årsverkene som var øremerket for arbeidet med informasjonssikkerhet og personvern. De resterende årsverkene var i hovedsak knyttet til IT-avdelingene og arbeidet med IT-sikkerhet. Hos enkelte av virksomhetene ble det i tillegg opplyst om ansatte med juridisk bakgrunn som jobbet med etterlevelse av GDPR. Det vanlige var likevel at GDPR-arbeidet foregikk i regi at virksomhetenes personvernombud.

Hos seks av de åtte kartlagte virksomhetene var det ikke knyttet en fast stillingsprosent til ombudsrollen. Ombuds-oppgavene var derfor noe som kom i tillegg til disse medarbeidernes ordinære arbeidsoppgaver. De to siste virksomhetene hadde ansatt personvernombud i 100 prosent stilling.

[47] Virksomheten hadde iverksatt en rekke IT-sikkerhetstiltak etter hendelsen, blant annet anskaffelse av NSM sitt varslingssystem for digital infrastruktur (VDI).

LEDELSESSYSTEMER OG INTERNKONTROLL

Virksomhetene ble spurt om status for arbeidet med utarbeidelse og innføring av ledelsessystemer for informasjonssikkerhet og internkontrollen for GDPR.

Når det gjaldt ledelsessystemer for informasjonssikkerhet, rapporterte én virksomhet at systemet var utarbeidet og innført, det vil si at det både var dokumentert og ble praktisert i virksomheten. Dette innebar at alle de sentrale aktivitetene i ledelsessystemet ble utført slik som planlagt, for eksempel at risikovurderinger ble gjennomført, nødvendige sikringstiltak ble iverksatt og ledelsens gjennomgang ble foretatt.

Seks virksomheter rapporterte at ledelsessystemet var utarbeidet og i noen grad innført (delvis praktisert). Graden av innføring varierte mellom disse virksomhetene. Det berodde særlig på at for enkelte av virksomhetene var dette et nybrottsarbeid. Innføringen var derfor en pågående aktivitet. For andre virksomheter kunne det handle om at praktiseringen av aktivitetene i ledelsessystemet hadde forvitret noe over tid, og at de nå «tok sats» på nytt.

Én virksomhet rapporterte om at ledelsessystemet verken var utarbeidet eller innført.

Når det gjaldt arbeidet med internkontrollen for GDPR, handlet det om et pågående, men ikke ferdigstilt arbeid hos de fleste virksomhetene. Tre virksomheter rapporterte om at arbeidet hadde tilfredsstillende progresjon, men at det ikke var ferdigstilt. Fire andre virksomheter uttrykte at arbeidet var kommet i gang, men at det fortsatt var en vei å gå før man var i mål. Hos én virksomhet ble det opplyst om at det ikke var avsatt ressurser til arbeidet med GDPR.

SÅRBARHETER

De åtte virksomhetene ble bedt om å opplyse om hva de mente var de viktigste sårbarheter i deres arbeid med informasjonssikkerhet og personvern. Sårbarhetene som ble nevnt var i hovedsak de samme som ble rapportert hos universitetene og høgskolene.

Følgende typer sårbarheter ble hyppigst nevnt:

- Organisatoriske mangler: oppgitt av fem virksomheter.
- Kompetanse: oppgitt av fire virksomheter.
- Tekniske mangler: oppgitt av fire virksomheter.

Organisatoriske sårbarheter handlet særlig om mangelfulle rutiner for behandling av personopplysninger og sikring av andre informasjonsverdier, og svakheter med hensyn til IT-drift. Det ble i tillegg rapportert om mangel på grunnleggende kompetanse om GDPR og informasjonssikkerhet, men her hadde flere virksomheter iverksatt pedagogiske tiltak (spesielt ved at nøkkelpersonell hadde deltatt på eksterne kurs). Tekniske sårbarheter dreide seg blant annet om teknisk gjeld (gamle IT-løsninger) og manglende verktøy for kontroll med lokal datatrafikk.

Bare to virksomheter opplyste om at kapasitet (personalressurser) var en viktig sårbarhet. Ingen virksomheter rapporterte om utfordringer knyttet til manglende bevissthet/kultur blant de ansatte (med hensyn til informasjonssikkerhet og personvern).

Det ble til slutt rapportert om sårbarheter som ikke naturlig hører hjemme i kategoriene ovenfor. Eksempler på dette var utfordringer knyttet til forskning i utlandet (konfliktområder) og jobbreiser (risiko for at IT-utstyr med sensitive data mistes eller stjeles).

Det ble også opplyst om bekymringer i forbindelse med at utenlandske ansatte eller gjester/besøkende fra enkelte land kunne utgjøre en informasjonssikkerhetsrisiko.

KAPITTEL 4

VURDERING AV RISIKO OG ANBEFALINGER

VURDERING AV RISIKO OG ANBEFALINGER

INNLEDNING

I dette kapitlet gis en samlet vurdering av risiko, det vil si summen av og sammenhengen mellom verdier, trusler og sårbarheter diskutert i kapittel 1-4.

Risiko vurderes på to nivåer. For det første risikoen for at sektormålene for arbeidet med informasjonssikkerhet og personvern (jf. drøftelsen av disse målene i innledningen til denne rapporten). For det andre en vurdering av risiko for viktige informasjonssikkerhets- og personvernhendelser som ble rapportert til Unit i 2018 og 2019.

Avslutningsvis gis enkelte anbefalinger om hvilke tiltak som kan iverksettes for å håndtere risikoen.

RISIKO FOR MANGLENDE MÅLOPPNÅELSE

I «Digitaliseringsstrategi for universitets- og høyskole-sektoren, 2017-2021» defineres følgende hovedmålsettinger for sektorens arbeid med informasjonssikkerhet og personvern:

1. Helhetlig styring og ledelse av arbeidet med informasjonssikkerhet og personvern som fundament for digitalisering og strategiske satsninger.

2. Systematisk arbeid for styrket informasjonssikkerhet og personvern basert på nasjonale føringer, for eksempel rettslige krav og krav i tildelingsbrev til institusjonene.

3. Bevisstgjøring av studenter og forskere med hensyn til datasikkerhet og riktig håndtering av data.

4. Et nivå på oppnådd informasjonssikkerhet og personvern som ligger høyere enn de nasjonale minstekravene.

I fjorårets rapport konkluderte Unit med at det var høy risiko for at universitetene og høgskolene ikke ville være i stand til å realisere målsettingene ved utgangen av strategiperioden. Videre konkluderte Unit med at det var mest realistisk at målsetting 3 – bevisstgjøring av studenter og forskere – kunne nås. For sektormål 1, 2 og 4, ble risikoen vurdert å være størst.

Disse konklusjonene ble begrunnet med bakgrunn i tre hovedpunkter:

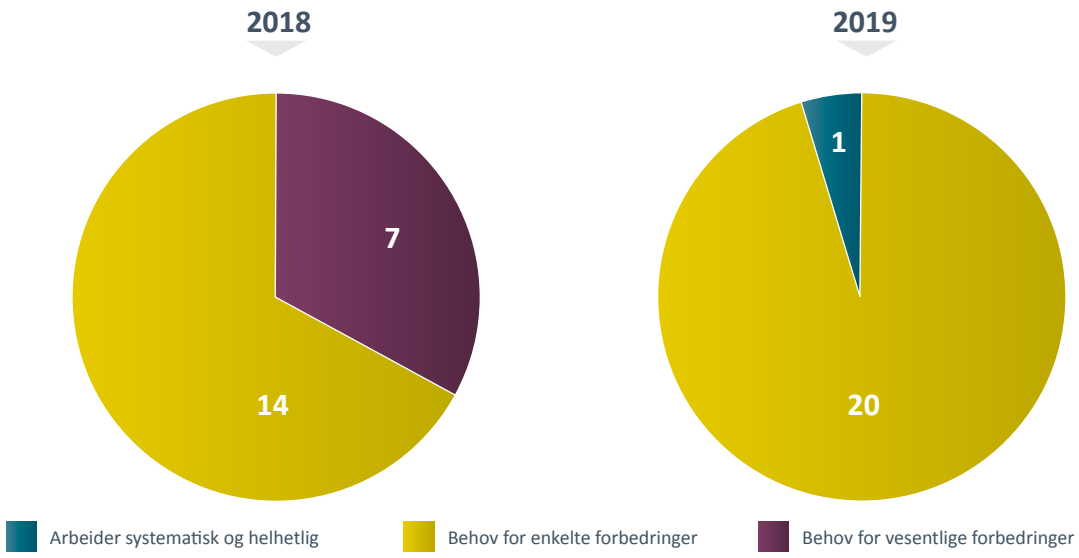
1. Sektoren forvaltet store, sammensatte og til dels uoversiktlige verdier (informasjon, dataressurser og økonomiske midler).

2. Sektoren rapporterte om at viktige tiltak på informasjonssikkerhets- og personvernområdet var iverksatt, men tiltakene kunne ikke fullt ut kompensere for sårbarhetene/manglene.

3. Sektoren rapporterte om relativt mange sikkerhetsbrudd, personvernavvik og sikkerhetstruende hendelser med skadepotensial, men antallet alvorlige hendelser var likevel begrenset.

I årets rapport, som også omfatter åtte øvrige virksomheter (direktorater og selskaper), har vi sett at flere av sårbarhetene det ble rapportert om i fjor, er utbedret, men ikke fullt og helt. Følgende forhold hadde blitt forbedret fra 2018 til 2019:

- Flere personalressurser har blitt dedikert til arbeidet med informasjonssikkerhet og personvern i 2019 enn i 2018. Enkelte institusjoner som ikke hadde styrket ressurs-innsatsen i 2019 rapporterte om at de hadde konkrete planer om dette.



Figur 6: Samlet status for arbeidet med informasjonssikkerhet og personvern hos universitetene og høgskolene i 2018 og 2019

- Institusjonene rapporterte om at det var iverksatt en rekke organisatoriske, pedagogiske og tekniske initiativ i løpet av 2019. Dette innebar ikke at arbeidet med å lukke avvik, spesielt å sørge for innføring av ledelsessystemer for informasjonssikkerhet og internkontroll for GDPR i alle deler av virksomheten, var sluttført, men at avvikslukkingen var i gang.

- Tendensen vi så i fjorårets kartlegging – toppledelsen (direktør/rektor) og universitets- eller høgskolestyrene er mer involvert i og stiller tydeligere krav til arbeidet med informasjonssikkerhet og personvern – har fortsatt. Innsatsen synes derfor å bli møtt med økende støtte fra de som formelt sett har ansvaret.

- Personvernombudene og ledere for arbeidet med informasjonssikkerhet (CISO/rådgivere) mottok flere henvendelser fra studenter og ansatte om lovlig og sikker behandling av personopplysninger i 2019 enn tidligere. Dette indikerer at bevisstheten er styrket, i alle fall med hensyn til innsamling og videre bruk av personopplysninger. Bevissthet ble likevel fremhevet som et område hvor det fortsatt var sårbarheter.

- Omfanget av informasjonssikkerhets- og personvern-hendelser for 2019 var på (omtrent) det samme nivået som for 2018. Det samme gjaldt hvilke typer hendelser det var snakk om og antallet alvorlige hendelser. Det ble rapportert om et noe mer utfordrende trusselbilde (se nedenfor).

Figur 6 gir en samlet statusoversikt over arbeidet med informasjonssikkerhet og personvern hos de 21 universitetene og høgskolene i 2018 og 2019. For 2018 viser figuren at sju institusjoner hadde behov for å styrke dette arbeidet vesentlig. De øvrige 14 institusjonene hadde behov for enkelte forbedringer, mens ingen institusjoner hadde etablert et systematisk og helhetlig arbeid. I 2019 hadde dette bildet endret seg noe. Ingen institusjoner hadde nå behov for vesentlige forbedringer i arbeidet med informa-sjonssikkerhet og personvern, mens 20 institusjoner hadde behov for enkelte forbedringer. Én institusjon hadde etablert et systematisk og helhetlig informasjonssikkerhets- og personvernarbeid.

Vi kan ikke si noe om endringer fra 2018 til 2019 hos de øvrige virksomhetene (direktoratene og selskapene)[48].

[48] Som tidligere nevnt, er kartleggingen av de øvrige virksomhetene – direktorater og aksjeselskaper – planlagt i mai/juni i år.

Figur 6 indikerer likevel at utviklingen i store deler av UH-sektoren har vært positiv – viktige forbedringstiltak var gjennomført og flere var planlagt. Samtidig viser figuren at informasjonssikkerhets- og personvernarbeidet fortsatt var preget av en del sårbarheter og mangler. Det handlet primært om at få institusjoner rapporterer om at ledelsessystemet for informasjonssikkerhet og internkontrollen for GDPR var innført og ble praktisert i alle deler av virksomheten. Det ble også rapportert om sårbarheter med hensyn til kompetanse og bevissthet/holdninger blant studenter og ansatte. Det ble i tillegg meldt om visse kapasitetsutfordringer, spesielt knyttet til opplæring og kompetanseheving.

Vår vurdering er derfor at hovedkonklusjonen fra fjorårets kartlegging står fast: sektormål 3 (bevisstgjøring av studenter og forskere) vil sannsynligvis kunne realiseres, men risikoen for at sektormål 1, 2 og 4 ikke realiseres er høy. Vi har sett at disse målene dreier seg om helhetlig ledelse/styring og systematisk innsats, og at nivået på informasjonssikkerheten og personvernet i sektoren skal ligge over de nasjonale minstekravene. Vi mener at tiden frem til utgangen av gjeldende strategiperiode (2021) blir for knapp til at disse målene vil kunne oppnås. Sektoren har nærmet seg, men timeglasset renner for fort ut.

RISIKO FOR INFORMASJONSSIKKERHETS- OG PERSONVERNHENDELSER

Styrkingen av arbeidet med informasjonssikkerhet og personvern i 2019, hadde ikke (som vi har sett) ført til nevneverdig nedgang i antallet registrerte uønskede hendelser. Det kan bero på at styrkingen har ført til færre «tause» hendelser, det vil si at hendelser som tidligere ikke ble oppdaget nå (i 2019) blir det. En annen mulighet er at trusselbilde i sektoren har blitt mer utfordrende (flere potensielt farlige trusler mot informasjonssikkerheten og personvernet).

Nedenfor følger en vurdering av risiko for de viktigste informasjonssikkerhets- og personvernhendelsene som ble nevnt under årets og fjorårets kartlegging (jf. kapittel 2).

NETTKRIMINALITET

I kapittel 2 så vi at rapporterte hendelser for 2019 i særlig grad handlet om nettkriminalitet. Risikoen for alvorlige hendelser som følge av nettkriminalitet vurderes derfor som høy.

- Moderat til alvorlig konsekvens: Vi har sett at skadevirkningene av nettkriminelle hendelser ofte ikke er veldig alvorlige. I enkelte tilfeller kan det likevel være tilfelle. Det kan for eksempel handle om feilaktige utbetalinger av betydelige millionbeløp, eller tyveri av personopplysninger og brukerkontoer for salg på det mørke nettet. I tillegg kan slike hendelser ha andre konsekvenser. Spørsmålene som kan stilles i den forbindelse er (i) i hvem sine lommer havner pengene og (ii) hva kan det tenkes at pengene blir brukt til? [49]

- Høy sannsynlighet (frekvens): Omfanget av nettkriminelle hendelser er omfattende i sektoren. Selv om suksessraten så langt har vært begrenset, ble det rapportert at forsøkene har blitt mer profesjonelle og troverdige enn tidligere. Vi mener derfor at sannsynligheten for alvorlige skadevirkninger er noe høyere enn før.

I tillegg til den generelle trusselen som nettkriminell aktivitet representerer for sektoren, ønsker vi å peke på risiko knyttet til enkelte konkrete nettkriminelle trusler:

FAKTURA- OG DIREKTØRSVINDEL

Risikoen for faktura- og direktørsvindel vurderes som høy.

- Moderat til alvorlig konsekvens: Som for nettkriminalitet generelt, trenger ikke skadevirkningene av faktura- og direktørsvindel å være veldig alvorlige. Men de økonomiske skadevirkningene kan i enkelte tilfeller være betydelige. Det samme gjelder for virksomhetenes omdømme. Psykologiske virkninger for den enkelte ansatte som har latt seg lure til å foreta urettmessige utbetalinger må også regnes med.

- Høy sannsynlighet (frekvens): Institusjonene og virksomhetene rapporterte om stadig flere slike hendelser. I tillegg ble det rapportert at forsøkene var mer målrettede og troverdige enn tidligere. Dermed blir det trolig vanskeligere å unngå feil og lettere å la seg lure [50].

[49] For reportasjer om og analyser av nettkriminelle nettverk og deres koblinger til andre former for organisert kriminalitet, se for eksempel https://krebsonsecurity.com/.

[50] Unit har også registrert tilfeller av fakturasvindel i sektoren etter at kartleggingen ble avsluttet.

KOMPROMITTERTE BRUKERKONTOER

Risikoen for at kompromitterte brukerkontoer benyttes til nettkriminelle handlinger vurderes som høy.

- Moderat til alvorlig konsekvens: Heller ikke skadevirkningene av kompromitterte brukerkontoer trenger å være alvorlige. Institusjonene og virksomhetene rapporterte for eksempel at kompromitterte kontoer hovedsakelig ble benyttet til utsendelse av søppel-epost. Kompromitterte kontoer kan likevel bli anvendt til langt alvorligere handlinger enn dette, for eksempel planting av skadevare eller datatyveri (inntrengning i deler av datanettverket hvor sensitiv informasjon behandles).

- Høy sannsynlighet (frekvens): Kompromitterte brukerkontoer ble rapportert av mange institusjoner i 2019. Det var derfor ikke uvanlig at brukere oppga brukernavn og passord på nettsider kontrollert av trusselaktører (vanligvis nettkriminelle grupper). Planlagt og til dels iverksatt innføring av to-faktorautentisering hos flere av institusjonene vil trolig bidra til at denne risikoen reduseres i deler av sektoren.

LØSEPENGEVIRUS

Risikoen for større hendelser som følge av løsepengevirus-angrep vurderes som middels.

- Moderat til alvorlig konsekvens: Skadevirkningene av større løsepengevirus-angrep kan være alvorlige. Samtidig er skadevirkningene økende. Det skyldes at mange av løsepengevirus-angrepene som er gjennomført de siste månedene, er blitt mer aggressive enn tidligere. I tillegg til at tilgangen til informasjon og dataressurser blokkeres, stjeles informasjon fra virksomhetenes datasystemer og trusselaktørene truer med at den vil bli publisert dersom løsepenger ikke betales [51]. Dermed kan skadevirkningene bli større og mer sammensatte enn før (for eksempel tapt produktivitet, ekstrautgifter til gjenoppretting, omdømmekostnader, krenkelser av personvernet og sanksjoner fra tilsynsmyndigheter).

- Liten sannsynlighet (frekvens): Ingen norske universiteter, høgskoler, direktorater eller selskaper hadde blitt utsatt for større løsepengevirus-angrep (bare angrep rettet mot enkeltbrukere, men ikke mot organisasjonen som sådan). For 2019 ble det dessuten rapportert om en nedgang i denne typen hendelser. Dette står i motsetning til trenden internasjonalt i 2019, hvor løsepengevirus-angrep ble mer vanlige også i høyere utdanning og forskning. Vi mener derfor at sannsynligheten for slike angrep kan være noe mindre i norsk UH-sektor enn i enkelte andre land. Etter at kartleggingen ble avsluttet, har vi registrert forsøk på spredning av det som trolig er løsepengevirus.

ANNEN SKADEVARE ENN LØSEPENGEVIRUS

Dette er en samlekategori som inkluderer mange ulike typer ødeleggende programvare, blant annet programvare som stjeler informasjon (forsknings-, ansatte- eller studentdata osv.) eller misbruker lokale dataressurser (for eksempel krypto-mining). Det er derfor utfordrende å gi en felles vurdering av såpass forskjelligartede trusler.

På bakgrunn av hendelsesrapportering i 2018 og 2019, mener vi likevel at risikoen for større hendelser som følge av annen skadevare enn løsepengevirus, er middels.

- Moderat til alvorlig konsekvens: Som nevnt ovenfor, kan konsekvensene av annen skadevare være alvorlige, blant annet kompromittering av sensitive forskningsdata, inkludert personopplysninger, eller tyveri av kredittkortopplysninger. Men verken i kartleggingene for 2019 eller 2018 ble det rapportert om alvorlige konsekvenser som følge av slik skadevare.

---

[51] Se for eksempel https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/?&web_view=true eller https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-may-tip-nasdaq-on-attacks-to-hurt-stock-prices/?&web_view=true.

[52] CERT/SOC-miljøene i sektoren rapporterte om at de hadde registrert en del skadevarehendelser i 2019. Det ble ikke rapportert om like mange hendelser eller mistenkte hendelser fra institusjonene og de øvrige virksomhetene.

[53] I 2019 registrerte Uninett CERT 12 tilfeller hvor dataressursene til deres kunder hadde blitt misbrukt til å gjennomføre tjenestenektangrep mot andre virksomheter.

• Liten sannsynlighet (frekvens): Det ble i relativt liten grad rapportert om uønskede hendelser som følge av annen skadevare. Vi mottok heller ikke rapporter i fjorårets kartlegging som tydet på at slik skadevare var hyppig forekommende i sektoren. Vi ser imidlertid ikke bort ifra at det kan finnes «tause» skadevarehendelser – hendelser som ikke oppdages. I så fall vil risikoen være noe høyere enn hva vi legger til grunn [52].

TJENESTENEKTANGREP

Risikoen for større tjenestenektangrep (DDoS) vurderes som lav.

• Moderat konsekvens: Skadevirkningene av tjenestenektangrep vil typisk være tapt produktivitet som følge av at systemer og datanettverk ikke er tilgjengelige for autoriserte brukere. Institusjonene og virksomhetene rapporterte om små skadevirkninger av slike angrep.

• Liten sannsynlighet (frekvens): Institusjonene og virksomhetene rapporterte om få tjenestenektangrep i løpet av de siste årene. Samtidig er trenden (hyppigheten) nedadgående (færre hendelser i 2019 enn i 2018). Sektoren bør likevel være oppmerksom på risikoen for at egne dataressurser (for eksempel IoT-utstyr) misbrukes i tjenestenektangrep mot virksomheter i andre sektorer eller land [53].

INNSIDEHENDELSER

Risikoen for brudd på informasjonssikkerheten og krenkelser av personvernet som følge av innsidehendelser – menneskelige feil som ikke er fremprovosert av nettkriminelle grupper eller andre eksterne trusselaktører – vurderes som middels til høy.

• Moderat til alvorlig konsekvens: Også når det gjelder innsidehendelser, er skadevirkningene i mange tilfeller ikke alvorlige. Men i enkelte tilfeller ble det rapportert om (potensielt) alvorlige skadevirkninger, for eksempel at kontaktinformasjon til personer med hemmelig adresse var søkbar på internettet og at uvedkommende hadde hatt tilgang til sensitive personopplysninger.

• Høy sannsynlighet (frekvens): Institusjonene og virksomhetene rapporterte om at innsidehendelser var relativt vanlig. Samtidig hadde det blitt iverksatt tiltak for å redusere hyppigheten av slike hendelser (bevisstgjøring og opplæring). Slike initiativ ble også rapportert i kartleggingen for 2018, men det virker ikke som dette har medført at frekvensen av innsidehendelser er vesentlig redusert. Institusjonene pekte på behovet for ytterligere tiltak for å redusere sannsynligheten for (og skadevirkningene av) innsidehendelser.

SÆRSKILT OM APT/STATSAKTØRER

Risikoen for datatyveri/-spionasje utført av APT/statsaktører er vanskelig å vurdere. Vi mener likevel at deler av sektoren må være oppmerksomme på risikoen for denne typen hendelser. Sannsynligheten for (hyppigheten av) slike hendelser er trolig relativt begrenset i sektoren som sådan, men skadevirkningene av enkelthendelser kan være alvorlige (for eksempel ulovlig overføring av kunnskap som kan ha militære anvendelsesområder). Her støtter vi oss dels på risiko- og trusselvurderingene til nasjonale etterretnings- og sikkerhetstjenester (E-tjenesten, PST og NSM), og dels til rapporteringene fra institusjonene og virksomhetene i sektoren.

Det virker for oss som at nasjonale sikkerhetstjenester vurderer trusselen fra APT/statsaktører mot forskningsmiljøer i UH-sektoren som noe større enn tidligere (se kapittel 2). Samtidig rapporterte enkelte institusjoner at de hadde vært utsatt for APT/statsaktører i løpet av de siste årene. I tillegg ble det opplyst om ubekreftede mistanker om slik aktivitet.

Det synes rimelig å anta at risikoen for APT/statsaktører er ujevnt fordelt i sektoren – visse institusjoner og virksomheter er trolig mer utsatte enn andre. Variasjoner i risiko vil, ifølge nasjonale sikkerhetstjenester, kunne bero på faglig profil – hvilke typer forskning som bedrives[54]. Det er derfor vår vurdering av risikoen for slike hendelser gjør det ekstra viktig at institusjonene kartlegger (og etablerer sterkere kontroll med) forskningsdata som kan være av interesse for APT/statsaktører.

Enkelte av direktoratene og selskapene rapporterte om hendelser hvor det var mistanke om at APT/statsaktører sto bak. Det kan derfor ikke utelukkes at noen av disse virksomhetene kan være gjenstand for interesse fra slike aktører.

ANBEFALINGER PÅ SEKTORNIVÅ

Etter fjorårets kartlegging utarbeidet Unit en rekke anbefalinger for å styrke arbeidet med informasjonssikkerhet og personvern. Vår vurdering er at det ikke er hensiktsmessig å presentere helt nye tiltak på dette tidspunktet, før vi vet mer om effektene av allerede planlagte eller nylig iverksatte tiltak. Dette gjelder følgende hovedtiltak:

1. Handlingsplan for digitalisering i høyere utdanning og forskning, 2019 til 2021[55]. Planen oppstiller ulike initiativ for å realisere målene i sektorens digitaliseringsstrategi. Spesielt viktige er tiltakene som gjelder etableringen av en rådgivnings- og veiledningstjeneste for informasjonssikkerhet og personvern og initiativ for å heve informasjonssikkerhets- og personvernkompetansen.

2. Program for informasjonssikkerhet og personvern i universitets- og høgskolesektoren. I tillegg til tiltakene nevnt ovenfor, inkluderer programmet viktige initiativ for å styrke sektorens evne til å oppdage og håndtere digitale sikkerhetstrusler. Det gjennomføres også et initiativ gjeldende bruk av NSMs system for varsling av dataangrep fra APT/statsaktører.

3. Risikohåndteringsplan. Unit utarbeidet en risikohåndteringsplan i etterkant av fjorårets kartlegging. I risikohåndteringsplanen presenteres tiltak for å styrke arbeidet med informasjonssikkerhet og personvern på sektornivå. Tiltakene er langsiktige, og dekker de risikoforholdene som ble identifisert under årets kartlegging.

Unit har utarbeidet en policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. Policyen oppsummerer de kravene som følger av lovregulering og andre nasjonale føringer på informasjonssikkerhets- og personvernområdet. Policyen bidrar derfor til å klargjøre hvilke krav som stilles til institusjonene og de øvrige virksomhetene.

Policyen har vært på høring i sektoren og vil bli lansert før sommeren 2020.

ANBEFALINGER PÅ VIRKSOMHETSNIVÅ

Alle institusjoner og øvrige virksomheter mottok egne brev fra Unit etter fjorårets kartlegging. I brevene ble det blant annet gitt anbefalinger for det videre arbeidet med informasjonssikkerhet og personvern. De fleste institusjonene hadde fulgt opp anbefalingene på en god måte. Unit har også i år sendt anbefalingsbrev til den enkelte virksomhet med anbefalinger om hva de bør prioritere i 2020.

Vi anbefaler at departementet også i år følger opp funnene og konklusjonene i denne rapporten i styringsdialogen med den enkelte institusjon og virksomhet.

[54] PST peker spesielt på forskningsmiljøer som arbeider med kjernefysikk, fysikk, kjemi, biologi, toksikologi, farmasi, undervanns- og dypvannsteknologi, kontrollsystemer, styringssystemer, autonome fartøy, mønstergjenkjenning (kunstig intelligens), ingeniørdesign, nanoteknologi, satellitt- og missilteknologi og teknologi tilpasset arktiske forhold.

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

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 åtte direktorater og selskaper som omfattes av styringsmodellen for informasjonssikkerhet og personvern i UH-sektoren.

Kartleggingsmøtene med universitetene og høgskolene ble gjennomført i perioden januar til mars 2020. Kartleggingsmøtene med direktoratene og selskapene ble gjennomført i perioden mai til oktober 2019.

FORBEREDELSER

I forkant av kartleggingsmøtene fikk institusjonene og virksomhetene tilsendt spørsmålene som ble besvart i løpet av møtene.

I forberedelsene til kartleggingen ble det gjennomført samtaler med Unit sine representanter i fagutvalgene for (a) utdanning, (b) forskning, (c) infrastruktur, mellomvare og data, og (d) administrasjon, ledelse og kontorstøtte. Hensikten med samtalene var å få oversikt over viktige digitaliseringsinitiativ i sektoren som har betydning for arbeidet med informasjonssikkerhet og personvern.

DELTAKERE

Institusjonenes og virksomhetenes deltakelse på kartleggingsmøtene varierte noe – fra tre til åtte ledere og medarbeidere. Deltakerne var primært sikkerhets- og beredskapsledere, informasjonssikkerhetsledere eller -rådgivere, rådgivere i forskningsadministrasjonen og personvernombud. Unit stilte vanligvis med tre deltakere, men på enkelte møter med to.

GJENNOMFØRING

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.

15 møter ble avholdt som videokonferanser. De øvrige (14) ble avholdt som fysiske møter.

Fra én institusjon mottok Unit skriftlige besvarelser på de tilsendte spørsmålene. Ved de øvrige institusjonene og virksomhetene ble svarene gitt muntlig i møtet. Svarene ble fortløpende notert av deltakerne fra Unit.

I etterkant av møtene utarbeidet Unit et kartleggingsreferat som oppsummerte institusjonenes og virksomhetenes svar. Referatene ble sendt til den enkelte institusjon og virksomhet for kvalitetssikring.

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 institusjoner og virksomheter i UH-sektoren; risiko- eller trusselvurderinger eller fra nasjonale myndigheter; risiko- eller trusselvurderinger fra internasjonale aktører og forskningslitteratur innenfor relevante fagområder.

I tillegg ble det gjennomført et møte med Uninett CERT.

ENKELTE BEGRENSNINGER

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

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

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

unit.no

unit.no

UNIT

DIREKTORATET FOR IKT OG FELLESTJENESTER
I HØYERE UTDANNING OG FORSKNING