Temarapport 2020 – informasjonssikkerhet og personvern
i høyere utdanning og forskning

KONTINUITET, BEREDSKAP OG ØVELSER

INNHOLD

SAMMENDRAG

I denne temarapporten presenteres utvalgte resultater fra Units kartlegginger av sektortilstanden på informasjonssikkerhets- og personvernområdet. Kartleggingene ble gjennomført i 2019 og 2020. Resultatene har ikke tidligere blitt publisert.

Spørsmålene som drøftes i temarapporten er

1) I hvilken grad hadde virksomhetene i UH-sektoren – 21 statlige universiteter og høgskoler, og åtte direktorater og selskaper – etablert kontinuitets- og beredskapsplaner for håndtering av ekstraordinære informasjonssikkerhetsbrudd og personvernhendelser?

2) Hadde disse virksomhetene øvd på hvordan slike hendelser kan mestres på hensiktsmessige og effektive måter?

Etablering av kontinuitets- og beredskapsplaner og øving på håndtering av alvorlige informasjonssikkerhets- og personvernhendelser, er krav som gjelder for alle virksomheter omfattet av Kunnskapsdepartementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».

Temarapporten gir følgende svar på spørsmålene ovenfor:

KONTINUITETS- OG BEREDSKAPSPLANER

- 3 av 29 virksomheter opplyste i 2019 om at de hadde etablert planer for håndtering av ekstraordinære informasjonssikkerhetsbrudd og personvernhendelser.
- 8 virksomheter opplyste i 2019 om at arbeidet med etablering av slike planer pågikk, men at planene ennå ikke var helt ferdigstilt.
- 18 virksomheter opplyste i 2019 om at kontinuitets- og beredskapsplaner på informasjonssikkerhets- og personvernområdet ikke var etablert, eller at arbeidet med planverket ikke hadde kommet veldig langt.
- 9 av 24 virksomheter som i 2019 mottok anbefaling fra Unit om etablering eller ferdigstilling av sin kontinuitets- og beredskapsplan, hadde fulgt opp denne anbefalingen i 2020.

ØVELSER

- 13 av 29 virksomheter opplyste om at de hadde gjennomført øvelser på håndtering av informasjonssikkerhetsbrudd og personvernhendelser i 2019.
- 16 virksomheter opplyste om at slike øvelser ikke hadde blitt avholdt i 2019.

Rapporten viser også at alle de 29 virksomhetene i kartleggingen hadde etablert tekniske og organisatoriske tiltak som styrker deres evne til å motstå og håndtere alvorlige informasjonssikkerhets- og personvernbrudd. Likevel savnes noe av den systematikken og planmessigheten i dette arbeidet som forutsettes i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

Samtidig viser rapporten at det er flere virksomheter som gjennomfører øvelser på hendelseshåndtering enn det er virksomheter som har planer for kontinuitet og beredskap på informasjonssikkerhets- og personvernområdet. Unit mener derfor at virksomhetene i sektoren bør sørge for at øvelsesaktiviteten skjer innenfor rammene av lokale kontinuitets- og beredskapsplaner.

Unit mener videre at det er viktig at læringspunkter fra øvelser benyttes som grunnlag for evaluering og (eventuelt) revisjon av det lokale planverket.

INNLEDNING

I Kunnskapsdepartementets «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning»[1] forventes det at virksomhetene i UH-sektoren etablerer kontinuitets- og beredskapsplan for håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser. Det kreves også at virksomhetene øver sin evne til å mestre slike hendelser.

I 2019 og 2020 kartla Unit om virksomhetene i UH-sektoren som omfattes av departementets policy hadde etablert planer og gjennomført øvelser.

I denne temarapporten presenteres resultatene fra kartleggingen.

POLICY FOR INFORMASJONSSIKKERHET OG PERSONVERN

Kunnskapsdepartementet har fastsatt krav til arbeidet med informasjonssikkerhet og personvern i «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning». Det er Unit som forvalter policyen. Policyen gjelder for 31 virksomheter – statlige universiteter og høgskoler, direktorater og selskaper – underlagt departementet.

Punkt 4 i policyen oppstiller krav til kontinuitet og beredskap. Her heter det blant annet at virksomhetene skal etablere løsninger for oppdagelse, varsling og håndtering av hendelser som medfører brudd på informasjonssikkerheten eller krenkelser av personvernet. Virksomhetene må også sørge for at viktige arbeidsoppgaver fortsatt kan utføres ved alvorlige hendelser, for eksempel langvarig bortfall av kritiske systemer, tjenester eller datanettverk. Videre at ledelsen stiller krav til og prioriterer arbeidet med kontinuitet og beredskap, og at det gjennomføres øvelser på håndtering av alvorlige brudd på informasjonssikkerheten eller personvernet.

I tillegg til policyen, er det vedtatt et eget rammeverk for håndtering av alvorlige IKT-sikkerhetshendelser i universitets- og høgskolesektoren.[2] Rammeverket beskriver rolle- og oppgavefordeling mellom virksomhetene, UH-sektorens responsmiljø (Uninett CERT), Unit, Kunnskapsdepartementet og andre nasjonale myndigheter.

OM UNITS TEMARAPPORTER

Units temarapporter retter søkelyset mot viktige områder i arbeidet med informasjonssikkerhet og personvern, og vil vanligvis bli publisert i forbindelse med nasjonal sikkerhetsmåned.

Rapportene retter seg mot alle i sektoren som jobber med, har lederansvar for eller er interessert i spørsmål om informasjonssikkerhet og personvern.

I tillegg til å gi informasjon om utvalgte temaområder, kan virksomhetene benytte rapportene til å vurdere eget ståsted opp mot den generelle tilstanden i sektoren.

1 Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning (https://www.unit.no/media/1981/download)

2 Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren (https://www.unit.no/rammeverk-handtering-av-ikt-sikkerhetshendelser-i-uh-sektoren)

BAKGRUNN

Kontinuitets- og beredskapsplaner for håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser inngår i ledelsessystemet for informasjonssikkerhet og internkontrollen for GDPR. Formålet med kontinuitet og beredskap er å styrke virksomhetenes motstandsdyktighet når de utsettes for store, negative påkjenninger som det ikke har vært mulig å forebygge, for eksempel som følge av dataangrep, tekniske sårbarheter, menneskelige feil eller uhell (brann, vannlekkasje, osv.). Dette oppnås ved at virksomhetene har planlagt og øvd på hvordan slike ekstraordinære påkjenninger best kan mestres.

Planer og øvelser skal sette virksomhetene i stand til raskt å oppdage, kontrollere, begrense skadene av og fjerne årsakene til informasjonssikkerhetsbrudd og personvern-hendelser. Det skal også bidra til at virksomhetene kan videreføre kritiske oppgaver samtidig som håndtering av hendelser og gjenoppretting av normal drift pågår. UH-sektorens håndtering av Covid 19-situasjonen er et eksempel på at evnen til å gjennomføre viktige deler av samfunnsoppdraget under vanskelige og unormale omstendigheter, for eksempel undervisning og eksamens-avvikling, kan ha stor verdi for studenter og ansatte.

I rapportene fra Units kartlegginger av arbeidet med informasjonssikkerhet og personvern i UH-sektoren,[3] drøftes ulike typer hendelser som det vil være naturlig å ta hensyn til også i arbeidet med kontinuitet og beredskap – og som det kan være hensiktsmessig å utvikle evnen til å håndtere.

Det gjelder blant annet følgende hendelser:

- Nettkriminell aktivitet, for eksempel økonomisk svindel og løsepengevirus.
- Uautorisert eksponering av særlige kategorier personopplysninger.
- Datatyveri utført av statlige hacker-grupper eller nettkriminelle aktører.
- Misbruk av lokale dataressurser for å gjennomføre dataangrep mot virksomheter i eller utenfor UH-sektoren.
- Utilgjengelige systemer eller tjenester på grunn av tekniske feil hos virksomhetene selv eller hos deres tjenesteleverandører.

3 Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2020 (https://www.unit.no/sites/default/files/media/filer/2020/06/5502%20Unit%20Rapport%20Info%20og%20Personvern%202020%20Enkeltsider%20Lav.pdf)

Tilstandsvurdering av informasjonssikkerhet og personvern blant de statlig eide universitetene og høgskolene: Rapport 2019 (https://www.unit.no/sites/default/files/media/filer/2019/06/Tilstandsvurdering-av-informasjonssikkerhet-personvern-blant-de-statlig-eide-universitetene-og-hogskolene.pdf)

Units kartleggingsrapporter i 2019 og 2020 viser at de aller fleste av disse typene hendelser ikke innebærer ekstraordinære påkjenninger for virksomhetene. Det er derfor når slike hendelser får et alvorlig omfang – og skadevirkningene kan tenkes å bli omfattende – at virksomhetene har særlig behov for kjente og øvde rutiner og prosesser for å oppdage hva som har skjedd, begrense skadevirkninger, iverksette alternative driftsløsninger og gjenopprette normal drift.

VEILEDNING OG RÅDGIVING OM KONTINUITET OG BEREDSKAP

Virksomheter som har behov for praktisk veiledning og rådgiving om etablering av sin kontinuitets- og beredskapsplan kan ta kontakt med rådgivingstjenesten hos Uninetts «Cybersikkerhetssenter for forskning og utdanning».[4]

I tillegg vil denne tjenesten kunne gi råd om tekniske og organisatoriske tiltak som kan styrke virksomhetenes evne til å motstå alvorlige informasjonssikkerhetsbrudd og personvernhendelser på en god måte. Dette inkluderer rådgiving og opplæring spesifikt rettet mot virksomhetenes hendelseshåndteringsteam (IRT – «Incident Response Team»).

Rådgivingstjenesten hos Uninett kan også bistå ved planlegging og gjennomføring av øvelser på mestring av alvorlige hendelser.

4 Cybersikkerhetssenter for forskning og utdanning (https://www.uninett.no/educsc)

KORT OM DATAGRUNNLAGET

Resultatene som presenteres i denne temarapporten er basert på data innhentet i forbindelse med Units årlige kartlegginger av sektortilstanden på informasjonssikkerhets- og personvernområdet. Kartleggingene omfattet 29 virksomheter (universiteter og høgskoler, direktorater og selskaper) som omfattes av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern. Kartleggingene ble gjennomført i januar-mars og mai-juni i 2019 og 2020.

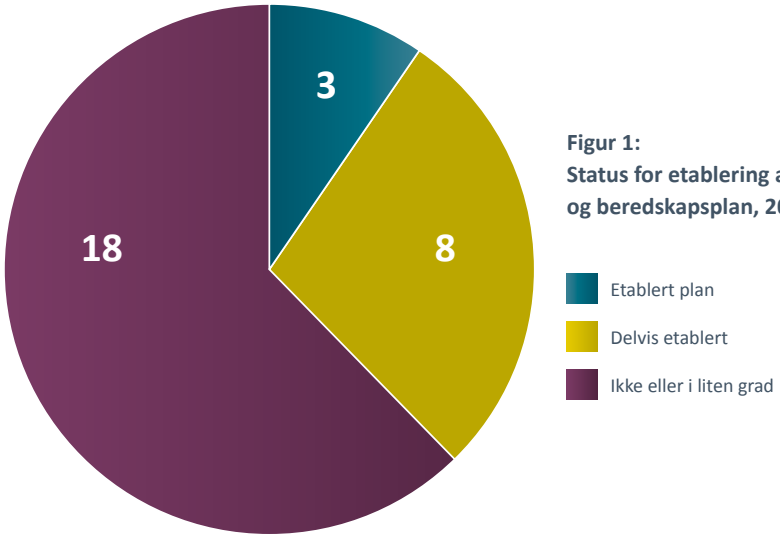
REDEGJØRELSE FOR DATAINNSAMLINGEN

Nærmere beskrivelser av hvordan Units kartlegginger blir gjennomført finnes i vedlegget til rapporten «Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2020» (se side 52-53).

KONTINUITETS- OG BEREDSKAPSPLAN

I Units kartlegging i 2019, rapporterte virksomhetene om status for arbeidet med etablering av kontinuitets- og beredskapsplan for håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser.

Figur 1 gir en oversikt over status for virksomhetenes arbeid med slike planer i 2019.



Figur 1:
Status for etablering av kontinuitets- og beredskapsplan, 2019

Figur 1 viser at tre virksomheter rapporterte om at de enten hadde ferdigstilt sin kontinuitets- og beredskapsplan eller at planen var svært nær ferdigstillelse. Samtidig rapporterte åtte virksomheter om at deler av planverket var på plass, det vil si at arbeidet var godt i gang, men at det fortsatt gjensto noe innsats for å ferdigstille det. Enkelte av disse virksomhetene mente at ferdigstillelse ville kunne skje i løpet av forholdsvis kort tid.

De resterende virksomhetene rapporterte om at de enten ikke hadde etablert planer for kontinuitet og beredskap på informasjonssikkerhets- og personvernområdet, eller at arbeidet med planverket var helt i startfasen og at det derfor gjensto mye arbeid før det var fullstendig.

VALG AV STRATEGI

Virksomhetene hadde valgt to hovedstrategier i arbeidet med etablering av kontinuitets- og beredskapsplan. Enkelte virksomheter hadde integrert rutiner og prosesser for håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser i sitt generelle beredskapsplanverk. Andre virksomheter hadde valgt å etablere egne planverk for dette, som kom i tillegg til den generelle beredskapsplanen.

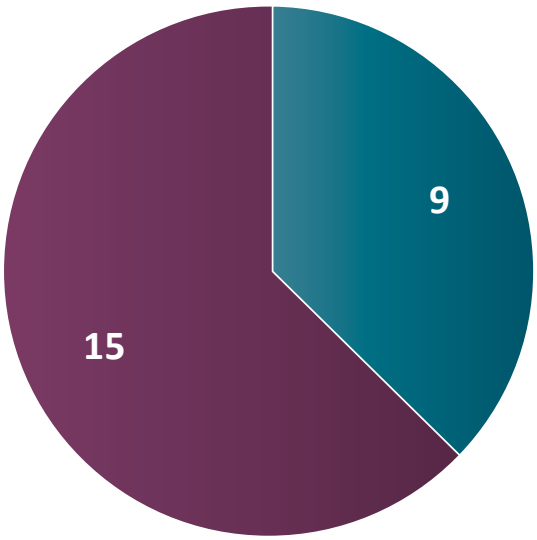
Valg av strategi virket dels å være styrt av hva den enkelte virksomhet mente var mest praktisk og hensiktsmessig. Men det virket også å bero på hvordan virksomhetene hadde valgt å ordne forholdet mellom arbeidet med informasjonssikkerhet, på den ene siden, og det øvrige sikkerhets- og beredskapsarbeidet, på den andre.

FORBEDRINGER I ARBEIDET MED KONTINUITET OG BEREDSKAP

På bakgrunn av oversikten i figur 1, mottok 24 virksomheter anbefalinger fra Unit om kontinuitet og beredskap i 2019. Anbefalingene gjaldt ferdigstillelse eller forbedring av virksomhetenes planer for håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser.

Fem virksomheter mottok ikke denne anbefalingen, enten fordi slike planer allerede fantes eller fordi arbeidet med planverket var kommet langt.

Figur 2 gir en oversikt over hvor mange av de 24 virksomhetene som i 2020 hadde fulgt opp anbefalingene fra 2019: Hadde virksomhetene forbedret eller ferdigstilt sine rutiner og prosesser for håndtering av ekstraordinære hendelser?



Figur 2:
Oppfølging av anbefalinger om kontinuitets- og beredskapsplan, 2020

Figur 2 viser at ni virksomheter hadde forbedret eller ferdigstilt sine rutiner og prosesser i 2020, slik som anbefalt av Unit i 2019.

15 virksomheter hadde ikke prioritert denne anbefalingen fra Unit. De hadde isteden fokusert på andre viktige områder og anbefalinger fra Unit. Dette handlet for eksempel om å styrke ressursinnsatsen, iverksette kompetansehevende tiltak, etablere behandlingsprotokoll, utvikle rutiner for ivaretakelse av de registrertes rettigheter eller gjennomføre risikovurderinger og innføre forebyggende tiltak.

Unit ba ikke virksomhetene om å gjøre nærmere rede for status for arbeidet med kontinuitets- og beredskapsplan ved kartleggingen i 2020. Dette vil bli fulgt opp i neste års kartlegging.

KONTINUITET, BEREDSKAP OG KORONA

Mesteparten (ca. 60 prosent) av Units kartlegging i 2020 ble gjennomført før Korona-nedstengingen 12. mars. Den siste delen av kartleggingen ble gjennomført i mai og tidlig i juni. Det er derfor usikkert hvordan nedstengingen har påvirket den videre fremdriften i arbeidet med planer for håndtering av alvorlige informasjonssikkerhetsbrudd og personvernhendelser.

Dette er, som allerede antydet, en problemstilling som Unit vil undersøke i 2021.

UFORMELLE PLANER

Selv om 15 virksomheter ikke hadde prioritert rutiner og prosesser for håndtering av alvorlige hendelser, innebar ikke det at kontinuitet og beredskap var fraværende på disse virksomhetenes dagsorden. Flere av virksomhetene rapporterte for eksempel om at de hadde uformelle planer for hvordan alvorlige informasjonssikkerhetsbrudd og personvernhendelser skulle håndteres. Planene omfattet blant annet bruk av hjemmekontor eller andre alternative lokasjoner i forbindelse med krisesituasjoner, og assistanse fra eksterne ekspertmiljøer eller leverandører ved større sikkerhetshendelser.

Det disse 15 virksomhetene likevel manglet var fullstendige og systematiske planer. Enkelte av virksomhetene kunne også ha visse andre mangler som har betydning for kontinuitets- og beredskapsarbeidet, for eksempel når det gjaldt oversikt over system- og tjenesteporteføljen, kartlegging av avhengigheter mellom og prioritering av IT-løsninger, eller krav til gjenopprettingstid, akseptabelt datatap og tjenestekvalitet.

DOKUMENTASJON

Alle virksomheter, også de som har uformelle planer for håndtering av alvorlige hendelser og som øver på håndtering av slike hendelser, skal dokumentere sitt planverk. Dette følger av punkt 12 i «Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning».

Hensikten med dokumentasjonen er blant annet å sikre at det finnes kjente og forutsigbare måter å håndtere alvorlige hendelser på. Dette kan effektivisere hendelseshåndteringen og redusere risikoen for interne misforståelser og uenigheter.

Å dokumentere planene kan i tillegg gjøre det lettere å inkorporere viktige læringspunkter fra reelle hendelser eller øvelser i det lokale planverket (læring og revisjon).

NYE INITIATIV

Figur 1 indikerer at mange virksomheter ikke eller i liten grad hadde etablert kontinuitets- og beredskapsplaner ved kartleggingen i 2019. Figur 2 viser at enkelte virksomheter rapporterte om at de hadde jobbet med slike planer ved kartleggingen i 2020. Det betyr at figurene ovenfor formidler et bilde av en sektor som har en vei å gå på kontinuitets- og beredskapsområdet. Dette bildet må imidlertid nyanseres noe:

Alle de 29 virksomhetene rapporterte i 2020 at de hadde gjennomført tekniske, organisatoriske eller pedagogiske initiativ for å styrke evnen til å motstå og håndtere alvorlige informasjonssikkerhetsbrudd og personvernhendelser. Det innebærer at selv om planer for håndtering av slike påkjenninger i mange tilfeller var mangelfulle eller fraværende, hadde virksomhetene iverksatt konkrete initiativ for å forebygge hendelser eller forberede virksomhetenes mestringsevne på sikkerhets- og personvernbrudd.

Eksempler på relevante initiativ er oppgradering av reservestrømløsninger, etablering av redundante førings-veier, nye strategier for sikkerhetskopiering, opprettelse av lokale hendelseshåndteringsteam (IRT) og segmentering av datanettverk. Hvilke andre initiativ som var iverksatt gjøres rede for i rapporten «Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2020» (se spesielt side 17-19).[5]

Det ble samtidig rapportert om medarbeidere som hadde deltatt på eksterne kurs eller samlinger – eller gjennomført egenstudier – for å bygge kompetanse på arbeidet med kontinuitet og beredskap. Flere av virksomhetene hadde i tillegg gjennomført øvelser på håndtering av informasjons-sikkerhetsbrudd eller personvernhendelser (se nedenfor).

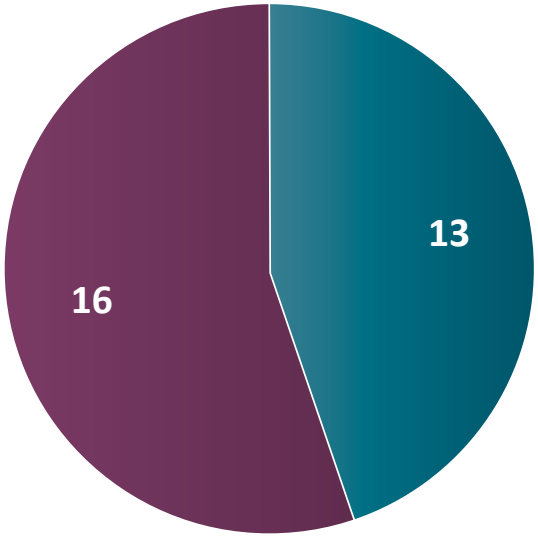
Initiativene nevnt ovenfor og i Units kartleggingsrapport for 2020 har, slik vi ser det, styrket sektorens evne til å motstå og håndtere hendelser. Samtidig har sektoren fortsatt en del ugjort når det gjelder planer for mestring av de påkjenninger som alvorlige informasjonssikkerhetsbrudd og personvern-hendelser kan innebære.

5 Informasjonssikkerhet og personvern i høyere utdanning og forskning. Risiko- og tilstandsvurdering 2020 (https://www.unit.no/sites/default/files/media/filer/2020/06/5502%20Unit%20Rapport%20Info%20og%20Personvern%202020%20Enkeltsider%20Lav.pdf)

ØVELSER

I Units kartlegging av sektortilstanden i 2020, rapporterte virksomhetene på om de hadde gjennomført øvelser på mestring av alvorlige informasjonssikkerhets- og personvernhendelser.

Figur 3 gir en oversikt over hvor mange virksomheter som rapporterte at de hadde gjennomført slike øvelser.



Figur 3:
Gjennomføring av øvelser

Figuren viser at 13 virksomheter hadde gjennomført øvelser på mestring av alvorlige hendelser i 2019. De fleste av disse virksomhetene hadde gjennomført én øvelse, men et par virksomheter opplyste om at to eller flere øvelser hadde blitt avholdt.

16 virksomheter rapporterte om at øvelser på mestring av hendelser ikke hadde vært gjennomført. Flere av disse virksomhetene opplyste imidlertid om at slike øvelser ble gjennomført i 2017 eller 2018.

Blant de 16 virksomhetene som ikke hadde gjennomført øvelser, var det enkelte som rapporterte om at øvelser ville bli gjennomført i 2020. Det var også noen virksomheter som opplyste om at planlagte øvelser våren 2020 hadde blitt avlyst/utsatt på grunn av Korona-nedstengingen. Om og eventuelt når disse øvelsene ville bli gjennomført, var ikke bestemt på kartleggingstidspunktet.

Som antydet ovenfor, viser oversikten i figur 3 at flere virksomheter hadde øvd på mestring av ekstraordinære informasjonssikkerhets- og personvernhendelser enn det var virksomheter som hadde etablert planer for håndtering av slike hendelser.

SCENARIOER

Scenarioene for øvelsene som hadde blitt gjennomført i 2019 spente over et relativt vidt spekter – alt fra digital sikkerhet, for eksempel løsepengevirus eller phishing, til intern-kommunikasjon, håndtering av media og gjenoppretting av data fra sikkerhetskopi.

Andre eksempler på øvelsesscenarier inkluderte testing av nye GDPR-rutiner, spesielt varsling av personvernhendelser til Datatilsynet eller til de registrerte. Flere virksomheter opplyste også om øvelser på andre GDPR-relaterte problem-stillinger, for eksempel uautorisert eksponering av særlige kategorier personopplysninger.

TYPE ØVELSER

Hvilke typer øvelser som ble gjennomført varierte noe mellom de 13 virksomhetene som hadde avholdt informasjonssikkerhets- og personvernøvelser.

Det vanligste var at virksomhetene hadde avholdt egne øvelser på håndtering av informasjonssikkerhetsbrudd eller personvernhendelser. Men det var også noen virksomheter hvor håndtering av slike hendelser inngikk som delelementer i større og mer tradisjonelle beredskapsøvelser.

De fleste virksomhetene hadde gjennomført mindre «skrivebordøvelser» (table-top-øvelser). Her ble relevante deltakere samlet for å drøfte hvordan de best kunne håndtere den tematikken som øvelsen handlet om. Noen færre virksomheter hadde gjennomført mer omfattende praktiske øvelser (spilløvelser).

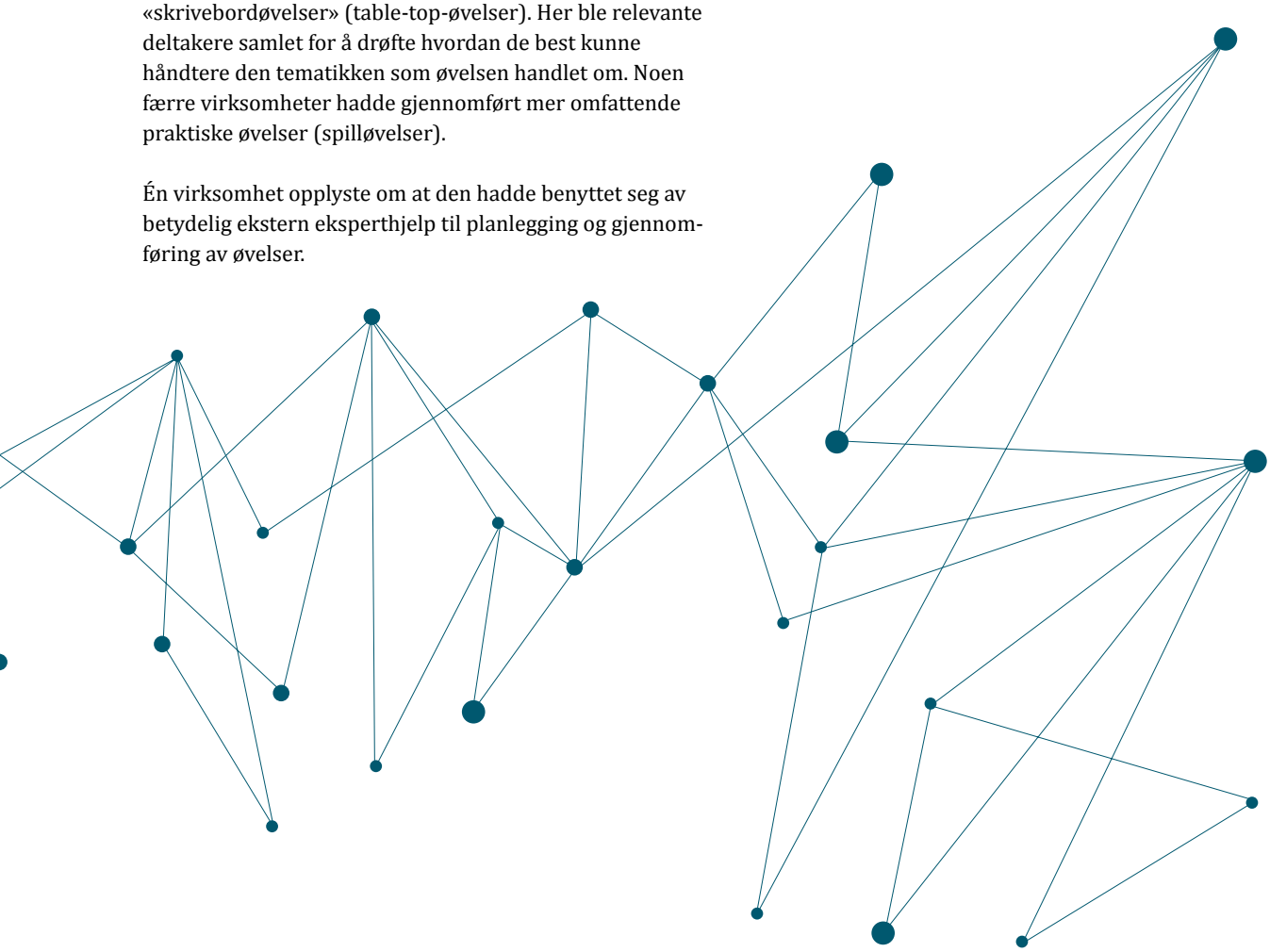
Én virksomhet opplyste om at den hadde benyttet seg av betydelig ekstern eksperthjelp til planlegging og gjennom-føring av øvelser.

LÆRING OG REVISJON

Virksomhetene opplyste i relativt liten grad om at konkrete tekniske eller organisatoriske forbedringstiltak, basert på erfaringer fra øvelsene, hadde blitt iverksatt etter at øvelsene var avholdt. Det virket derfor som at systematiske evalueringer av øvelsene med tanke på å forebygge fremtidige hendelser eller utbedre mangler i selve hendelseshåndteringen ikke var vanlig.

Selv om noen virksomheter opplyste om at erfaringer fra øvelser ble diskutert i ledelsens gjennomgang, virket det ikke å være vanlig at kontinuitets- og beredskapsplaner ble revidert i etterkant av øvelser. Dette skyldes naturlig nok at forholdsvis få virksomheter hadde etablert slike planer, og at evalueringer med sikte på revisjon og forbedring derfor ikke var aktuelt.

Det innebar likevel ikke at øvelsene ikke ga (eller kunne gi) viktige bidrag til virksomhetenes fremtidige arbeid med informasjonssikkerhet og personvern. Spesielt viktig her var at øvelsene bidro til å løfte frem betydningen av praksis-nær kompetanse om informasjonssikkerhet og personvern i en digitalisert hverdag.



OPPSUMMERING

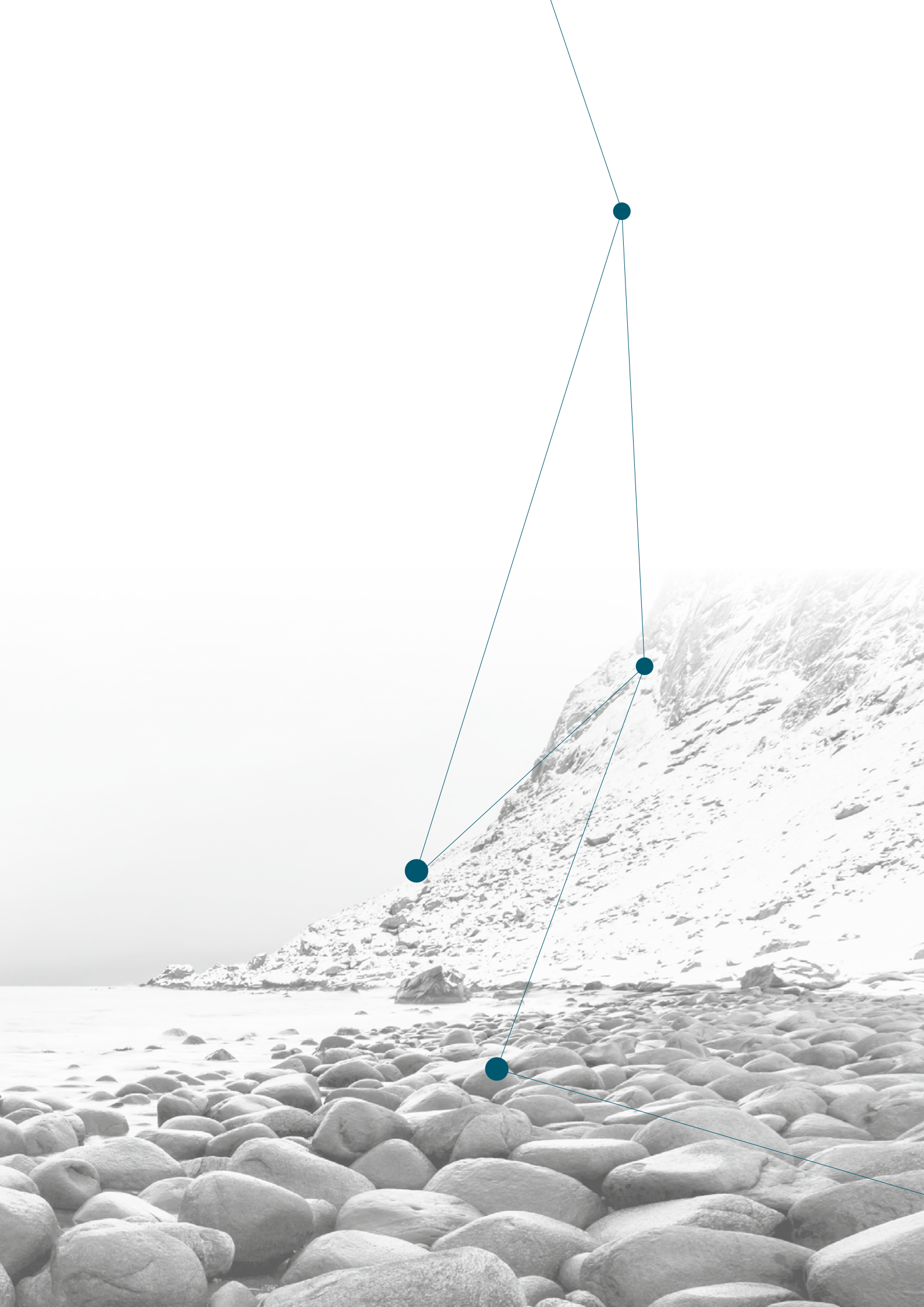
I Units rapport for 2020 om arbeidet med informasjonssikkerhet og personvern i høyere utdanning og forskning[6] konkluderes det med at det har skjedd forbedringer i dette arbeidet siden fjorårets kartlegging.

Denne temarapporten indikerer likevel at kontinuitet og beredskap er et område hvor sektoren har et tydelig forbedringspotensial. Det gjelder særlig etablering av planer for hvordan alvorlige hendelser skal håndteres. Samtidig er det flere virksomheter som gjennomfører øvelser på hendelseshåndtering enn som har planer for kontinuitet og beredskap på informasjonssikkerhets- og personvern-området. Slik vi ser det, bør det derfor være en prioritert oppgave for virksomhetene i sektoren å sikre at øvelsesaktiviteten skjer innenfor rammen av lokale kontinuitets- og beredskapsplaner.

Virksomhetene bør også sørge for at viktige læringspunkter fra øvelsene benyttes som grunnlag for evaluering og (eventuelt) revisjon av planverket.

Det er i tillegg verdt å merke seg at det ikke virket vanlig at øvelser ga grunnlag for iverksetting av nye tekniske, organisatoriske eller pedagogiske forbedringstiltak. Samtidig opplyste alle de 29 virksomhetene om at forbedringstiltak med betydning for kontinuitets- og beredskapsarbeidet hadde blitt gjennomført i 2019. Dette kan tyde på at sektoren har styrket sin evne til å motstå ekstraordinære påkjenninger på informasjonssikkerhets- og personvern-området, men at arbeidet fortsatt savner noe av den systematikken og planmessigheten som kreves i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern.

6 Informasjonssikkerhet og personvern i høyere utdanning og forskning: Risiko- og tilstandsvurdering 2020 (https://www.unit.no/sites/default/files/media/filer/2020/06/5502%20Unit%20Rapport%20Info%20og%20Personvern%202020%20Enkeltsider%20Lav.pdf)



Engasjert Byrå. Foto Shutterstock

UNIT

DIREKTORATET FOR IKT OG FELLESTJENESTER
I HØYERE UTDANNING OG FORSKNING