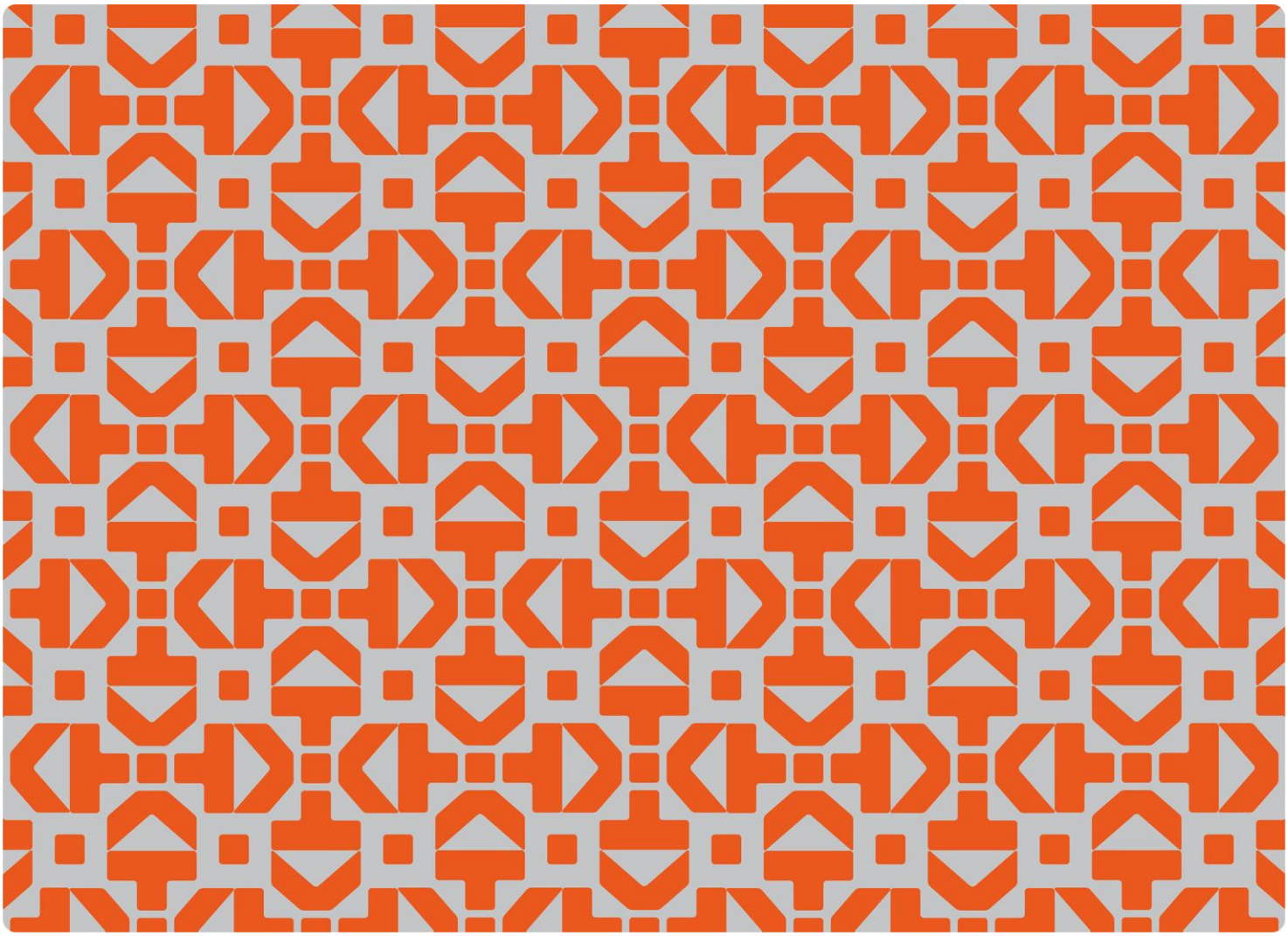
Rapport nr. 2/2024

Informasjonssikkerhet og personvern i et femårsperspektiv

Utvikling i UH-sektoren 2018-2022



Informasjonssikkerhet og personvern i et femårsperspektiv
Utvikling i UH-sektoren 2018-2022

Redaktør:
Kristin Selvaag

Forfattere:
Mathias Gullbrekken Sandnes
Tommy Tranvik

ISSN 2703-9102
Utgitt: 02/2024

Innhold

Sammendrag

I denne rapporten oppsummeres utviklingen i arbeidet med informasjonssikkerhet og personvern hos 21 statlige universiteter og høgskoler for perioden 2018 til 2022. Grunnlaget for beskrivelsene av utviklingen er HK-dir sine årlige kartlegginger av arbeidet med informasjonssikkerhet og personvern i UH-sektoren. Kartleggingene er en del av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning.

Utvikling vurderes etter grad av etterlevelse av de lovpålagte kravene i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning. Vi ser spesielt på kravene som handler om institusjonenes evne til å forebygge, oppdage, og håndtere informasjonssikkerhets- og personvernhendelser. Avslutningsvis drøftes risikonivå for ulike typer brudd på informasjons- og personopplysningssikkerheten sett opp mot gjennomførte tiltak i perioden.

Hovedfunnene fra rapporten er:

- Det har vært en moderat økning i etterlevelse av kravene i departementets policy til arbeidet med informasjonssikkerhet og personvern hos de 21 statlige universitetene og høgskolene i perioden 2018-2022. I 2022 etterlevde to universiteter kravene i Kunnskapsdepartementets policy. De resterende institusjonene etterlevde enkelte eller deler av kravene.

- Alle universitetene og høgskolene har etablert de viktigste rutinene i internkontrollen for personvern, og den styrende delen av ledelsessystemet for informasjonssikkerhet. De fleste institusjonene manglet imidlertid fortsatt tilfredsstillende systematikk i arbeidet i 2022.

- Fra og med 2022 ble det registrert en nedgang i antall hendelser og brudd på informasjons- og personopplysningssikkerheten hos institusjonene. Det ble også registrert en nedgang i antall meldte avvik til Datatilsynet.

- Risikoen for brudd forårsaket av løsepengevirus og statlig hacking (kunnskapsspionasje) har økt siden 2019, og ble vurdert som høy i 2022. Brudd forårsaket av utilsiktede feil og uhell blant ansatte, tjenestenektangrep (DDoS) og misbruk av lokale dataressurser av nettkriminelle trusselaktører, er redusert noe i perioden. Risikoen for tilfeller av vellykkede forsøk på direktør- og fakturasvindel ble redusert fra et høyt risikonivå i 2019 til et lavt nivå i 2022.

Utviklingen de siste fem årene viser at det har vært forbedringer i arbeidet med informasjonssikkerhet og personvern hos de 21 universitetene og høgskolene, men at det fortsatt er behov for forbedringer. Samtidig ser vi at utviklingen i etterlevelse av kravene i departementets policy er ujevnt fordelt mellom institusjonene – enkelte institusjoner har styrket seg mer enn andre i perioden.

Vi mener at det er behov for mer kunnskap om effekten av iverksatte sikkerhetstiltak hos universitetene og høgskolene. Et slikt tiltak kan være periodiske revisjoner av arbeidet med informasjonssikkerhet og personvern i UH-sektoren. Kunnskapen fra revisjonene kan bidra til å

styrke institusjonenes arbeid med å forbedre sin etterlevelse av kravene i policyen, og gi Kunnskapsdepartementet et bedre grunnlag for å beslutte fellestiltak i sektoren.

Innledning

Økt grad av digitalisering gir muligheter for innovasjon og utvikling innen undervisning, forskning, og formidling i universitets- og høyskolesektoren (UH-sektoren). Samtidig innebærer digitaliseringen betydelige utfordringer knyttet til sikring av digitale verdier og ivaretakelse av personvernet.

Forsvarlig sikring av virksomhetskritiske prosesser og tjenester som digital eksamen, informasjonsverdier som forskningsdata, og personopplysninger om studenter og ansatte, er derfor viktig for at sektoren skal kunne løse sitt samfunnsoppdrag. Ansvaret for tilstrekkelig informasjonssikkerhet og ivaretakelse av personvernet i henhold til lovpålagte krav ligger hos den enkelte virksomhets ledelse.

Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å beskytte informasjonsverdier – opplysninger, datamaskiner og programvare – mot at de eksponeres for uvedkommende, endres eller slettes på uautoriserte måter, skades eller ødelegges eller er utilgjengelige for rettmessige brukere. Dersom bruddene gjelder personopplysninger, for eksempel at de kommer på avveie eller endres uten at det var meningen, kan det innebære krenkelser av personvernet til de registrerte (de enkeltpersoner som opplysningene gjelder).

Personvern handler om mer enn å beskytte opplysninger om de registrerte mot brudd på sikkerheten til opplysningene. Grunntanken er at personvernet ivaretas ved at de registrerte har medinnflytelse over og kan utøve en viss kontroll med bruken av egne opplysninger.

Krenkelser av personvernet kan blant annet skje ved at de registrerte ikke får kjennskap til at det samles inn opplysninger om dem, hvem som samler inn opplysningene, hvilke opplysninger det dreier seg om og hva opplysningene skal brukes til. Andre eksempler på krenkelser kan være at det samles inn flere opplysninger enn nødvendig, opplysningene brukes til andre formål enn de registrerte er kjent med og at opplysningene ikke slettes som avtalt.

Det er Kunnskapsdepartementet som har det overordnede ansvaret for informasjonssikkerheten og forsvarlig behandling av personopplysninger i UH-sektoren. For å ivareta dette ansvaret lanserte departementet styringsmodell for informasjonssikkerhet og personvern i 2019.

Det praktiske arbeidet med å gjennomføre styring og oppfølging av virksomhetene som omfattes av styringsmodellen, ble delegert til HK-dir, tidligere Unit.[1] Styringen og oppfølgningen fra HK-dir skjer med grunnlag i departementets krav og forventinger til arbeidet med informasjonssikkerhet og personvern. Kravene er samlet i Kunnskapsdepartementets policy for informasjonssikkerhet og personvern i UH-sektoren.[2]

Styringsmodell for informasjonssikkerhet og personvern i høyere utdanning og forskning

[1] Styringsmodellen er tilgjengelig på https://hkdir.no/hoyere-utdanning-og-forskning/sikkerhet/styring-av-informasjonssikkerhet-og-personvern. Sist besøkt 02.01.2024.
[2] Departementets policy er tilgjengelig på https://www.regjeringen.no/no/dokumenter/f04-20-policy-for-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-ogforskning/id2769629/. Sist besøkt 7.06.2023.

Departementets styringsmodell for informasjonssikkerhet og personvern har fire hovedelementer:

1. **Krav fra Kunnskapsdepartementet**: Departementet stiller krav til virksomhetenes arbeid med informasjonssikkerhet og personvern. Kravene oppsummeres i departementets policy for informasjonssikkerhet og personvern.
2. **Årlig kartlegging av HK-dir**: HK-dir kartlegger årlig hvordan virksomhetene etterlever kravene i departementets policy, og rapporterer resultatene til departementet og offentligheten.
3. **Anbefalinger fra HK-dir**: Basert på kartleggingene, gir HK-dir skriftlige anbefalinger til hver enkelt virksomhet om det videre arbeidet med informasjonssikkerhet og personvern.
4. **Tiltaksplan fra HK-dir**: HK-dir utarbeider hvert år en risikohåndteringsplan med anbefalinger til fellestiltak på sektornivå for å styrke virksomhetenes arbeid med informasjonssikkerhet og personvern. Departementet godkjenner planen, og HK-dir følger opp godkjente tiltak.

Kravene i policyen kan deles inn i tre deler: punkt 1-5 gjelder informasjons- og personopplysningssikkerheten, for eksempel at virksomhetene underlagt departementet skal gjennomføre risikovurderinger og etablere sikringstiltak. Punkt 6-10 gjelder øvrige krav til behandling av personopplysninger, for eksempel plikter virksomhetene å ivareta rettighetene til personer som de behandler personopplysninger om. Punkt 11-12 gjelder begge deler, og stiller krav til opplæring og kompetanseheving, og dokumentering av arbeidet innen disse forvaltningsområdene.

For å bidra til at virksomhetene i UH-sektoren etterlever kravene i policyen på en tilfredsstillende måte, gjennomfører HK-dir årlige kartlegginger av arbeidet med informasjonssikkerhet og personvern hos alle virksomheter som omfattes av styringsmodellen. På bakgrunn av kartleggingene vurderer HK-dir tilstanden for arbeidet med informasjonssikkerhet og personvern hos disse virksomhetene, og vurderer risiko for brudd på informasjons- og personopplysningssikkerheten. HK-dir har publisert funnene fra kartleggingene i risiko- og tilstandsrapporter hvert år siden 2019.[3]

Om begrensninger og datagrunnlaget[4]

Denne rapporten er hovedsakelig basert på informasjon samlet inn av HK-dir gjennom møter med hver enkelt virksomhet i perioden 2019-2023. Vi har ikke bedt om eller fått tilgang til interne dokumenter som beskriver virksomhetenes arbeid med informasjonssikkerhet og personvern. Videre har vi ikke utført kontroller av personverntiltak eller tester av informasjonssikkerheten.

Etter fem år med kartlegging av etterlevelse av rettslige krav og vurdering av risiko, er tiden inne for å undersøke hvilken effekt dette arbeidet har hatt på virksomhetene som er underlagt styringsmodellen. Et godt mål på dette er i hvilken grad styringsmodellen har ført til forbedret

[3] Viktige funn og resultater fra kartleggingene har blitt oppsummert i årlige risiko- og tilstandsrapporter. Risiko- og tilstandsrapportene er tilgjengelige på https://hkdir.no/vaare-tenester/styring-av-informasjonssikkerhet-og-personvern-i-hoeyere-utdanning-og-forskning. Sist besøkt 02.01.2024.

[4] For nærmere beskrivelse av begrensinger og metode i kartleggingene, se Risiko- og tilstandsvurdering 2023, s. 12-13, og s. 90-97. Rapporten er tilgjengelig på Informasjonssikkerhet og personvern i høyere utdanning og forskning | HK-dir (hkdir.no). Sist besøkt 24.01.2024.

etterlevelse av kravene i policyen, og om risikoen for uønskede hendelser og brudd på informasjons- og personopplysningssikkerheten er redusert. I denne temarapporten tar vi utgangspunkt i de 21 statlige universitetene og høgskolene som omfattes av styringsmodellen.[5]

I det følgende oppsummerer vi først utviklingen i universitetene og høgskolenes etterlevelse av kravene i policyen mellom 2018 og 2022. Deretter ser vi nærmere på utviklingen i hendelser, brudd, og skadevirkninger som er blitt rapportert fra universitetene og høgskolene i denne perioden. I neste del viser vi utviklingen i HK-dir sine årlige vurderinger av risiko for brudd og hendelser.

Avslutningsvis gir vi en vurdering av hvilke tiltak som har bidratt til å forbedre arbeidet med informasjonssikkerhet og personvern hos institusjonene disse fem årene, og hvilke behov for forbedringer vi ser i det videre arbeidet.

[5] Disse 21 er: Arkitektur- og designhøgskolen i Oslo, Høgskolen i Innlandet, Høgskolen i Molde - Vitenskapelig høgskole i logistikk, Høgskolen i Østfold, Høgskolen i Volda, Høgskulen på Vestlandet, Kunsthøgskolen i Oslo, Nord universitet, Norges Handelshøyskole, Norges idrettshøgskole/Noregs idrettshøgskole, Norges miljø- og biovitenskapelige universitet (NMBU), Norges musikkhøgskole, Norges teknisk-naturvitenskapelige universitet (NTNU), OsloMet – storbyuniversitetet, Samisk høgskole, Universitetet i Agder, Universitetet i Bergen, Universitetet i Oslo, Universitetet i Sørøst-Norge, Universitetet i Stavanger, og Universitetet i Tromsø – Norges arktiske universitet.

Direktoratet for høyere utdanning og kompetanse

Etterlevelse av kravene i policyen

I denne delen gjør vi rede for endringer i institusjonenes etterlevelse av kravene i departementets policy for informasjonssikkerhet og personvern i perioden 2018 til 2022.[6] HK-dir måler utvikling i etterlevelse av kravene ved bruk av en modenhetstrapp med tre nivåer:

Modenhet 1 – Lav grad av etterlevelse: Det er behov for vesentlige forbedringer i arbeidet med kravet.

Modenhet 2 – Moderat grad av etterlevelse: Det er behov for enkelte forbedringer i arbeidet med kravet.

Modenhet 3 – Tilfredsstillende grad av etterlevelse: Etterlevelsen av kravet vurderes som tilfredsstillende.

Med utgangspunkt i modenhetsnivåene gir vi først en kort beskrivelse av to faser i arbeidet med informasjonssikkerhet og personvern: Først nullpunktmålingen for 2018, og den påfølgende utviklingen i 2019 hvor etableringen av ledelsessystem og internkontroll for personvern står i fokus.[7]

Deretter beskrives høgskolenes og universitetenes gjennomføring og kontroll av arbeidet på disse områdene for perioden 2020-2022. Her skiller vi mellom de kravene i policyen som rettes mot ivaretakelse av personvernet, og de kravene som rettes mot informasjonssikkerhet. Til slutt beskriver vi den samlede utviklingen i etterlevelse av alle kravene i policyen.

Etableringen av ledelsessystem og internkontroll: 2018-2019

Tilstands- og risikovurderingen for 2018 viste at 15 av universitetene og høgskolene hadde moderat etterlevelse av kravene til personvern i policyen, mens 6 hadde lav etterlevelse. Det vil si at universitetene og høyskolene samlet sett kun hadde delvis oversikt over egen behandling av personopplysninger, manglende systematikk i gjennomføring av rutiner og prosedyrer, og mangelfull rapportering om behov og gjennomførte tiltak på dette området.

Samtidig rapporterte alle institusjonene at de var i startfasen med personvern- eller GDPR-prosjekter for å etablere internkontrollregimer på personvernområdet. Prosjektene handlet om å kartlegge IT-systemer som ble benyttet til behandling av personopplysninger, protokollføring av

[6] Kartleggingene og de årlige risiko- og tilstandsvurderingene tar utgangspunkt i foregående år, kartleggingen i 2019 måler dermed tilstand for 2018.

[7] Fremstillingen av to faser er en forenkling ment for å få frem hovedtrekkene i institusjonenes utvikling av arbeidet med informasjonssikkerhet og personvern i perioden. Det var variasjon i hvor langt høgskolene og universitetene hadde kommet med etablering, innføring, og gjennomføring av aktiviteter og tiltak knyttet til internkontroll for personvern og ledelsessystem for informasjonssikkerhet i 2018. Det var det fortsatt i 2022.

slike behandlinger, og utarbeiding av rutiner for å håndtere forespørsler fra studenter og ansatte om retting og sletting av personopplysninger.[8]

Drift av GDPR-prosjektene pågikk frem til utgangen av 2019. Mellom 2018 og 2019 styrket 5 av de 6 institusjonene med lavt modenhetsnivå seg betydelig i etterlevelse av kravene til forsvarlig behandling av personopplysninger.

Internkontroll for personvern[9]

Virksomheten må sikre en forsvarlig *behandling av personopplysninger* ved at man ivaretar den registrertes rettigheter og friheter, samtidig som man ivaretar virksomhetens mål ved behandlingen. Etter personvernforordningen (artikkel 24) innebærer det en forholdsmessighet hvor man ser på behandlingens art, omfang, formål og sammenheng, samt risikoene for fysiske personers rettigheter og friheter, og ut fra det gjennomfører egnede tekniske og organisatoriske tiltak.

Internkontroll skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte. Tiltakene skal dokumenteres og oppdateres ved behov.

Når det gjaldt informasjonssikkerheten var det kun 2 institusjoner som hadde tilfredsstillende etterlevelse av kravene i policyen, 9 hadde moderat etterlevelse, og 10 hadde lav etterlevelse av kravene i 2018. Med unntak av én institusjon, hadde alle høgskolene og universitetene etablert den styrende delen av sitt ledelsessystem for informasjonssikkerhet i 2019. Den gjennomførende og kontrollerende delen av ledelsessystemet gjensto imidlertid for alle unntatt to høgskoler. I 2019 hadde situasjonen bedret seg betydelig ved 9 av institusjonene: kun én høgskole gjensto med lav etterlevelse av kravene til ledelsessystemet.

Ledelsessystem for informasjonssikkerhet[10]

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

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

Det var varierende etterlevelse av kravene i policyen blant universitetene og høgskolene i både 2018 og 2019. Alle institusjonene hadde imidlertid et klart behov for å styrke arbeidet med å gjennomføre og kontrollere tiltak og aktiviteter innen både personvern og informasjonssikkerhet.

[8] Se Risiko- og tilstandsvurdering 2019 s. 24-39, rapporten er tilgjengelig på: Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 03.01.2024

[9] Vi har benyttet Datatilsynets beskrivelse fra deres veileder om internkontroll for personvern. Veilederen er tilgjengelig på Etablere internkontroll | Datatilsynet. Sist besøkt 04.01.2024.

[10] Definisjoner er hentet fra Risiko- og tilstandsvurdering 2019 s. 25, rapporten er tilgjengelig på: Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 03.01.2024

Implementering av ledelsessystem og internkontroll: 2020-2022

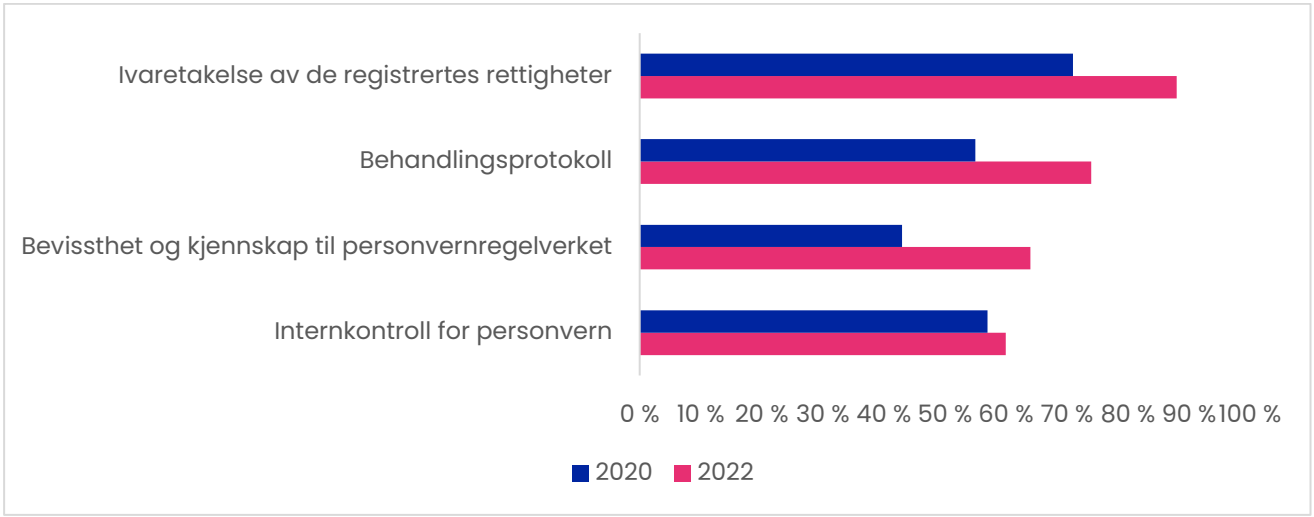
I 2020 kom universitetene og høgskolene over i en ny fase i arbeidet med informasjonssikkerhet og personvern. Fra og med 2020 dreide fokuset til institusjonene seg over fra etableringen av internkontroll og ledelsessystem til å iverksette, kontrollere, og revidere tiltakene og aktivitetene for å nå sine personvern- og sikkerhetsmål. Dette innebærer at universitetene og høgskolene i denne perioden fikk testet hvorvidt de hadde fullstendige og gode nok rutiner, systemer og planverk. På bakgrunn av erfaringene med testing og implementeringen av aktivitetene og tiltakene i ledelsessystem og internkontroll, har alle universitetene og høgskolene forbedret sin etterlevelse av enkelte krav i policyen i denne perioden.

Samtidig har universitetene og høgskolene i løpet av perioden forbedret etterlevelsen av de kravene i policyen som retter seg mot forsvarlig behandling av personopplysninger mer enn kravene som retter seg mot informasjonssikkerhet. Det er også enkelte krav i policyen som er etterlevd på et høyere modenhetsnivå av flere institusjoner enn enkelte andre krav.

For å vise utviklingen og hvilken betydning dette har for risiko for brudd på informasjonssikkerheten og krenkelser av personvernet, er det gitt en mer detaljert beskrivelse av etterlevelsen av kravene i policyen for 2020-2022 enn årene før. Beskrivelsen er todelt mellom kravene som retter seg mot forsvarlig behandling av personopplysninger og informasjonssikkerhet. Til slutt beskriver vi den samlede etterlevelsen av policyen.

Arbeidet med personvern 2020-2022

HK-dir gir en modenhetsvurdering av hver enkelt høgskoles og universitets etterlevelse av kravene i policyen som er rettet mot forsvarlig behandling av personopplysninger i forbindelse med de årlige risiko- og tilstandsvurderingene. Figur 1 sammenligner institusjonenes etterlevelse av kravene rettet mot personvern i policyen i 2018 med 2022 ved å summere modenhetsnivåene for begge årene. Ved 100 prosentpoeng etterlever alle høgskolene og universitetene de aktuelle kravene på et tilfredsstillende nivå.



Figur 1: Etterlevelse av krav til personvern 2020 og 2022

Figur 1 viser at høgskolene og universitetene har i gjennomsnitt et høyere modenhetsnivå i etterlevelse av kravene på dette området i 2022 enn i 2020. Samtidig er utviklingen ujevn mellom kravene i policyen. I det følgende beskriver vi hva kravene i figuren innebærer for det enkelte

universitet og høgskole, og hvor mange institusjoner som har forbedret sitt modenhetsnivå i denne perioden.

Ivaretakelse av de registrertes rettigheter

Kravene til ivaretakelse av de registrertes rettigheter innebærer at universitetene og høgskolene tilbyr adekvat informasjon til, og kan håndtere forespørsler fra, personer som er registrert i deres systemer om innsyn, retting, og sletting av personopplysninger. Institusjonene skal også ha innført rutiner for varsling av de registrerte personene og Datatilsynet dersom det oppdages brudd på personvernet.[11]

I 2020 hadde 12 av institusjonene tilfredsstillende etterlevelse på dette området, tilsvarende tall for 2022 var 16. De øvrige høgskolene og universitetene etterlevde kravene på et moderat nivå i både 2020 og 2022. Dette er et av områdene med størst grad av etterlevelse i sektoren målt i antall institusjoner som etterlever kravene med tilfredsstillende modenhet.

Behandlingsprotokoll

Universitetene og høgskolene skal føre en komplett og oppdatert protokoll over hvilke personopplysninger de behandler i egen virksomhet. Hensikten med dette kravet er at universitetene og høgskolene skal ha oversikt over sin behandling av personopplysninger.

I 2022 hadde 10 av universitetene og høgskolene tilfredsstillende etterlevelse av kravene på dette området, mot 3 institusjoner i 2020. De minste høgskolene og universitetene sto for tilveksten. De øvrige institusjonene var på et moderat nivå i 2022. Styrkningen på dette området gjør at universitetene og høgskolene i gjennomsnitt har bedre oversikt over behandling av personopplysninger enn tidligere.

Bevissthet og kjennskap til personvernregelverket

Universitetene og høgskolene skal sørge for relevant opplæring og kompetanseheving for ledere, medarbeidere og studenter knyttet til pålagte oppgaver i henhold til kravene i personvernforordningen. De skal også sørge for bevissthet om vanlige trusler mot personvernet og informasjonssikkerheten hos disse gruppene, for eksempel epostsvindel.

Den største utviklingen innenfor kravene som retter seg mot personvernområdet er arbeidet med bevissthet og kjennskap til personvernregelverket for ledere, medarbeidere, og studenter. I 2020 hadde kun ett universitet tilfredsstillende etterlevelse på dette området, men i 2022 hadde totalt 3 universiteter og 4 høgskoler samme status. Samtidig hadde andelen universiteter og høgskoler med lav etterlevelse falt fra 4 institusjoner til 1 institusjon i 2022.

Økt bevissthet og kjennskap til personvernregelverket øker sannsynligheten for at arbeidsoppgaver knyttet til behandling av personopplysninger i større grad utføres rettidig og etterrettelig. Dette kan også bidra til å redusere risiko for at ansatte og studenter begår feil eller faller for vanlige typer forsøk på svindel.

Internkontroll for behandling av personopplysninger

Et av de mest krevende kravene i policyen er å etablere en fullstendig internkontroll for personopplysninger, som også er implementert i alle deler av virksomheten. Dette innebærer å etablere, utføre, og rapportere på fullstendige rutiner og prosesser som konkretiserer hvordan

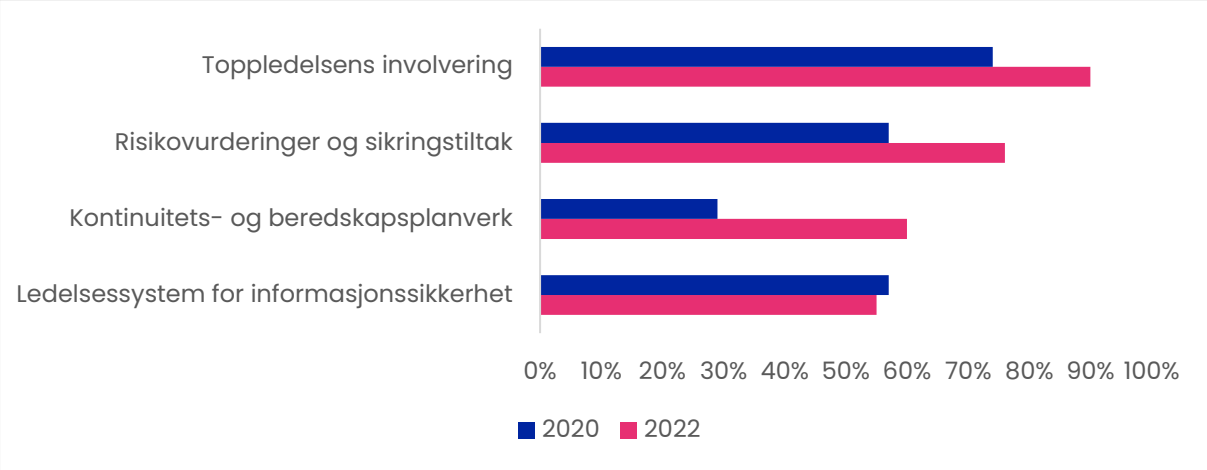
[11] Opplistingen av de registrertes rettigheter og behandlingsansvarliges plikter er ikke uttømmende.

rettslige krav til behandling av personopplysninger skal etterleves i det daglige arbeidet. For å oppnå tilfredsstillende etterlevelse av dette kravet, må universitetene og høgskolene etterleve de fleste kravene innenfor de overnevnte områdene på en tilfredsstillende måte.

I 2020 hadde 3 av institusjonene tilfredsstillende etterlevelse av kravet til internkontroll for personopplysninger. De resterende 18 holdt et moderat nivå. I 2022 hadde antallet institusjoner med tilfredsstillende etterlevelse økt til 4, mens de øvrige fortsatt hadde moderat etterlevelse av kravene. Til tross for god utvikling i de overnevnte kravene de siste årene, gjenstår det fortsatt en del arbeid før sektoren som helhet oppnår en tilfredsstillende etterlevelse av kravene til forsvarlig behandling av personopplysninger.

Arbeidet med informasjonssikkerhet 2020-2022

I likhet med kravene til personvern, gir HK-dir en modenhetsvurdering av hver enkelt høgskoles og universitets etterlevelse av kravene i policyen om sikring av informasjonsverdier i forbindelse med de årlige risiko- og tilstandsvurderingene. Figur 2 sammenligner institusjonenes etterlevelse av disse kravene i 2018 med 2022 ved å summere modenhetsnivåene for begge årene. Ved 100 prosentpoeng etterlever alle høgskolene og universitetene de aktuelle kravene på et tilfredsstillende nivå.



Figur 2: Etterlevelse av krav til personvern og informasjonssikkerhet 2020 og 2022

Utviklingen i etterlevelse av kravene til sikring av informasjonsverdier har forbedret seg i perioden fra 2020 til 2022, men samlet sett i mindre grad enn utviklingen i etterlevelse av de kravene som gjelder personvern. Nedenfor beskriver vi hva kravene i figur 2 innebærer, og utviklingen i etterlevelse av kravene blant universitetene og høgskolene i perioden.

Kontinuitets -og beredskapsplanverk

Institusjonene skal ha etablert beredskaps – og kontinuitetsplaner for hvordan informasjonssikkerhetshendelser skal oppdages og håndteres, og kritiske arbeidsoppgaver kan utføres ved bortfall av viktige systemer, tjenester eller datanettverk. Dette innebærer at ledelsen ved universitetene og høgskolene utpeker medarbeidere med særlig ansvar på dette området (IRT), fastsetter egne krav til kontinuitet, og avsette tilstrekkelig ressurser til arbeidet.

Kravene som er rettet mot institusjonenes evne til å håndtere informasjonssikkerhetshendelser, spesielt kontinuitets -og beredskapsplanverket, har hatt god utvikling i perioden. I 2020 hadde 10

institusjoner lav etterlevelse av kravene på dette området, like mange hadde moderat etterlevelse, og kun ett universitet hadde tilfredsstillende etterlevelse.

I 2022 hadde 4 institusjoner tilfredsstillende, og resterende institusjoner moderat etterlevelse av kravene om beredskaps -og kontinuitetsplaner for håndtering av informasjonssikkerhetshendelser. Universitetene og høgskolene har derfor sannsynligvis styrket sin evne til å håndtere informasjonssikkerhetshendelser i perioden. Samtidig viser utviklingen også at det fortsatt er mangler på dette området hos 17 av institusjonene.

Risikovurderinger og etablering av sikringstiltak

Universitetene og høgskolene skal forebygge hendelser som kan føre til brudd på personopplysnings -og informasjonssikkerheten. Dette skal gjøres ved å vurdere risikoen for forekomst av uønskede sikkerhetshendelser, og kartlegge mulige konsekvenser av slike hendelser. Det er ledelsen ved universitetene og høgskolene som skal definere akseptabelt risikonivå[12] for sin virksomhet, og har ansvaret for at tiltak iverksettes i de tilfellene risikoen ikke kan aksepteres.

I 2020 hadde 5 institusjoner tilfredsstillende etterlevelse av kravene til gjennomføring av risikovurderinger og etablering av nødvendige sikringstiltak, 14 holdt et moderat nivå, og 2 institusjoner hadde lav etterlevelse av kravene. I 2022 hadde 11 institusjoner tilfredsstillende etterlevelse av kravene på dette området, de 10 øvrige holdt et moderat nivå.

Arbeidet med kravene til gjennomføring av risikovurderinger og påfølgende sikringstiltak har satt universitetene og høgskolene i bedre stand til å identifisere og vurdere risiko for, og iverksette tiltak for å forhindre, brudd på informasjonssikkerheten og krenkelser av personvernet.

Involvering og oppmerksomhet fra toppledelsen

Det er universitetenes og høgskolenes styre og øverste ledelse som har ansvaret for etterlevelse av kravene i policyen. Dette innebærer at ledelsen skal stille tydelige krav, sette mål, avsette tilstrekkelige ressurser, og delegere myndighet til medarbeidere som trenger det for å sikre gjennomføring av det lovpålagte arbeidet med informasjonssikkerhet og personvern ved egen institusjon.

Kravene til toppledelsen og styrenes involvering og oppmerksomhet til arbeidet med informasjonssikkerhet og personvern er blant de best etterlevde kravene blant høgskolene og universitetene. I 2022 hadde 17 institusjoner tilfredsstillende etterlevelse av kravene på dette området, og 5 institusjoner holdt et moderat nivå. Dette er en forbedring fra 2020, da holdt 13 institusjoner et tilfredsstillende nivå, 8 institusjoner et moderat nivå, og 1 institusjon et lavt nivå i etterlevelse av kravene på dette området.

[12] Datatilsynet beskriver akseptabelt risikonivå/toleransenivå for sikkerhet som: «Risikovurdering handler om å identifisere konsekvenser ved ulike hendelser eller scenarier, og å vurdere hvor sannsynlig eller lett en uønsket hendelse kan inntreffe. Det er virksomhetens ledelse som avgjør hvor stor risiko (risikoappetitt) virksomheten skal ta ved ulike scenarier. Dette kalles toleransenivå for sikkerhet. Toleransenivå gir føringer for hvilke tiltak og ressurser som må settes inn for at behandlingen ikke skal overskride det definerte toleransenivået.» Datatilsynets råd for iverksetting av styringssystem for informasjonssikkerhet er tilgjengelig på Etablere internkontroll | Datatilsynet. Sist besøkt 24.01.2024.

Involvering og oppmerksomhet fra universitetenes og høgskolens styre og toppledelse er en forutsetning for at arbeidet med informasjonssikkerhet og personvern gjennomføres og kontinuerlig forbedres.

Ledelsessystem for informasjonssikkerhet

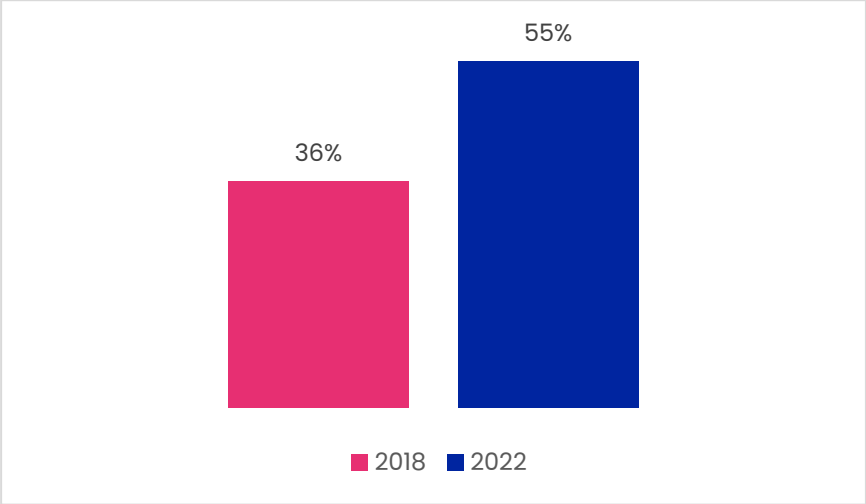
Universitetene og høgskolene skal ha et ledelsessystem for informasjonssikkerhet som er fullstendig dokumentert, og det skal praktiseres i alle deler av kjernevirksomheten. Dette innebærer å etablere, utføre, og rapportere på fullstendige rutiner og prosesser som konkretiserer hvordan organisasjonens krav til tilstrekkelig informasjonssikkerhet skal etterleves i det daglige arbeidet. Kravet til ledelsessystem for informasjonssikkerhet er, i likhet med kravet til internkontroll for personvern (GDPR), blant de mest krevende kravene å etterleve.

I 2020 hadde 3 institusjoner tilfredsstillende etterlevelse av kravet, mens de øvrige institusjonene etterlevde dette kravet på et moderat nivå. I 2022 hadde én av institusjonene blitt nedjustert fra tilfredsstillende til moderat nivå på dette kravet. De øvrige institusjonene holdt samme modenhetsnivå som i 2020.

Dette betyr ikke at sektoren ikke har hatt utvikling i etterlevelse av kravet til ledelsessystem for informasjonssikkerhet mellom 2020 og 2022. En rekke forbedringer ble gjennomført i denne perioden, slik utviklingen i de overnevnte kravene viser. Mangelen på utviklingen i etterlevelse av kravet på dette området viser imidlertid at 19 av 21 institusjoner ikke har klart å etablere fullstendige og implementerte ledelsessystemer for informasjonssikkerhet i egen virksomhet på fem år.

Moderat forbedring i 2018–2022

HK-dir gir en samlet modenhetsvurdering av hver enkelt høgskoles og universitets etterlevelse av kravene i policyen i forbindelse med de årlige Risiko- og tilstandsvurderingene. Figur 3 sammenligner institusjonenes etterlevelse av alle kravene i policyen i 2018 med 2022 ved å summere modenhetsnivåene av Hk-dirs overordnede vurderinger for begge årene.[13] Ved 100 prosentpoeng er samtlige krav i policyen etterlevd på et tilfredsstillende nivå hos alle universitetene og høgskolene.



[13] Se vedlegg 1 for en beskrivelse av metodikken vi har brukt for denne illustrasjonen av etterlevelse i sektoren.

Figur 3: Etterlevelse av policy 2018 og 2022

Figuren viser at universitetene og høgskolene har forbedret sin etterlevelse av kravene i policyen med 19 prosentpoeng mellom 2018 og 2022. Dette betyr at det gjennomsnittlige modenhetsnivået for etterlevelsen av Kunnskapsdepartementets policy for informasjonssikkerhet og personvern har forbedret seg fra et lavt til et moderat modenhetsnivå på fem år.

Utviklingstakten i etterlevelse av policyen var høyere i etableringsfasen i 2018-2019, enn i implementeringsfasen 2020-2022. Samtidig har deler av kravene i policyen hatt svært god utvikling også i perioden med implementering: for eksempel har kravene som retter seg mot de registrertes personvernrettigheter og toppledelsens involvering i arbeidet med informasjonssikkerhet økt med henholdsvis 17 og 14 prosentpoeng målt i modenhetsnivå.

Samlet ser vi at utviklingen i hvilke krav i policyen som etterleves mest og minst er svært forskjellig, og at utviklingen har vært ujevn mellom kravene som stilles til personvern og informasjonssikkerhet i policyen. Dersom vi sammenligner modenhetsnivåene for kravene som retter seg mot personvern med de som retter seg mot informasjonssikkerhet, ser vi at førstnevnte etterleves marginalt bedre enn sistnevnte i 2022.

Utviklingen i etterlevelse av policyen har gitt et bedre sikringsnivå for informasjonsverdier og personopplysninger i 2022 enn i 2018. Dette innebærer at universitetene og høgskolene som følge av økt modenhet i etterlevelse av kravene har forbedret sin evne til å forebygge, oppdage, og håndtere hendelser.

Behov for forbedringer

Det er viktig å skille mellom status i 2022, og utviklingen de siste årene. Det at alle universitetene og høgskolene har forbedret sin etterlevelse av kravene i policyen, betyr at alle institusjonene i 2022 har styrket sitt arbeid med informasjonssikkerhet og personvern i forhold til 2018. Samtidig er status i 2022 at kun 2 universiteter etterlever kravene i policyen på en tilfredsstillende måte.

Den manglende etterlevelsen av kravene innebærer at institusjonene ikke lykkes i tilfredsstillende grad med å forebygge, oppdage, og håndtere brudd på informasjons- og personopplysningssikkerheten. For eksempel har 12 av 21 institusjoner (31 prosentpoeng) oppnådd et høyere modenhetsnivå i 2022 enn i 2020 innen kravene som stilles til beredskaps -og kontinuitetsplaner.

Likevel er det fortsatt kun 4 av 21 institusjoner med tilfredsstillende etterlevelse av kravene på dette området i 2022. Konsekvensene av manglende etterlevelse av kravene til beredskaps- og kontinuitetsplaner er økt sannsynlighet for at gjenoppretting av drift etter en alvorlig hendelse blir mer tid- og kostnadskrevende enn nødvendig.

Også manglende etterlevelse av kravene til ledelsessystem, spesielt risikostyring og sikringstiltak, kan gi økt sannsynlighet for at institusjonene ikke klarer å forebygge avvik og brudd, eller oppdage at brudd og avvik oppstår. Denne svakheten er tydelig i Riksrevisjonens rapport om informasjonssikkerhet i forskning innenfor kunnskapssektoren.

Riksrevisjonen la frem en revisjon av informasjonssikkerhet i forskningssystemer i UH-sektoren i januar 2024.[14] Riksrevisjonens funn indikerer at de IT-tekniske sikringstiltakene i sektoren sannsynligvis er for svake til å hindre en trusselaktør i å få tilgang på viktige informasjonsverdier som forskningsdata. I tillegg viser rapporten at institusjonene sannsynligvis ikke har god nok oppdagelsesevne når slike brudd skjer. HK-dirs risiko- og tilstandsvurderinger viser at universitetene og høgskolene er bekymret for de samme sårbarhetene som Riksrevisjonen peker på i sin rapport.

Riksrevisjonens inntrengingstester hos forskningsinstitusjoner

Riksrevisjonen gjennomførte inntrengingstester mot tre forskningsinstitusjoner, og lyktes med å få full kontroll over IT-infrastruktur ved to av dem. Ved den siste institusjonen lyktes de kun med å få kontroll over forskeres IT-utstyr og skylagring. Testene ble utført med kjente metoder og uten forsøk på å skjule aktiviteten. Ved to av forskningsinstitusjonene ble få eller ingen av aktivitetene i testene oppdaget, hos den tredje ble testingen oppdaget etter fire dager.

Inntrengningstestene lyktes på grunn av sårbarheter som svake passord, mange brukerkontoer med vidtgående rettigheter, og sårbarheter i beskyttelsen av institusjonenes nettverk. I tillegg ble ikke aktiviteten fra testene oppdaget fordi overvåkningen av nettverkene var mangelfull. Riksrevisjonen mener at resultatet av testene gir grunn til å tro at lignende forsøk hos andre institusjoner i sektoren ville gitt tilsvarende resultater.

Det er derfor fortsatt et behov for å styrke arbeidet med informasjonssikkerhet og personvern hos universitetene og høgskolene. Som pekt på ovenfor, konkluderer Riksrevisjonen med det samme. Det er likevel enkelte positive utviklingstrekk utover institusjonenes etterlevelse som har bidratt til at sektorens informasjonsverdier, blant annet forskningsdata og personopplysninger, er mindre truet i 2022 enn tidligere. Nedenfor oppsummerer vi utviklingen i hendelser og brudd på informasjons- og personopplysningssikkerheten i perioden.

[14] Riksrevisjonens rapport er tilgjengelig på Dokument 3:11 (2023–2024) (riksrevisjonen.no). Sist besøkt 18.01.2024.

Hendelser og brudd 2018-2022

Hvert år siden den første kartleggingen har HK-dir spurt høgskolene og universitetene om hvor mange og hvilke typer uønskede informasjonssikkerhets- og personvernhendelser de har registrert det siste året.[15] Det gjør at vi kan følge endringer i antall og typer rapporterte hendelser. Dette gir viktig informasjon om hvilke trusler sektoren utsettes for og hvilke hendelser virksomhetene bør prioritere å forebygge, oppdage og håndtere.

Antall og typer informasjonssikkerhetshendelser

For de fire første årene (2018 til 2021) varierte antallet rapporterte informasjonssikkerhetshendelser – forsøk på brudd og reelle brudd på informasjonssikkerheten – mellom noe i overkant av 2000 og ca. 2500. Det handlet særlig om kompromittering av brukerkontoer (nettfiske), direktør- og fakturasvindel, misbruk av lokal datakraft til utvinning av kryptovaluta og utnyttelse av tekniske sårbarheter i internetteksponerte IT-løsninger.

Også avbrudd i tilgangen til tjenesteutsatte datasystemer/-tjenester var en gjenganger i denne perioden. Det samme gjaldt uautorisert eksponering av personopplysninger som følge av menneskelige feil eller uhell.

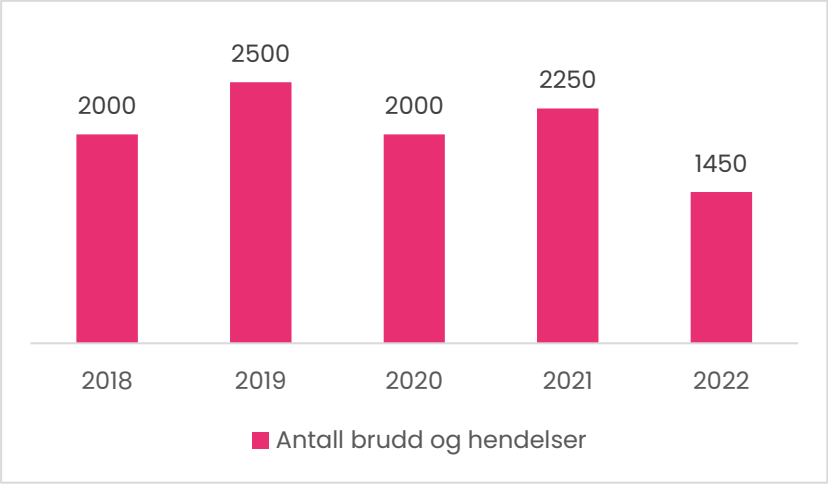
I løpet av denne perioden har sektoren i begrenset grad vært utsatt for svært alvorlige hendelser, for eksempel løsepengevirus (nedstengning av hele eller viktige deler av virksomhetenes datanettverk). Det har likevel vært rapportert om flere tilfeller hvor begrensede løsepengevirusangrep har lyktes. Det har også vært tilfeller hvor langt mer omfattende løsepengevirusangrep er avverget i siste øyeblikk.

Videre har det forekommet enkelte tilfeller av kunnskapstyveri som statlige eller statlig støttede hacker-grupper står bak. I perioder har sektoren også vært utsatt for elektronisk rekognoseringsaktivitet og digitale innbruddsforsøk, hvor det er grunn til å anta at statlige aktører var involvert.

Trendbrudd i 2022

Mens perioden 2018-2021 var kjennetegnet av et relativt stabilt antall informasjonssikkerhetshendelser, skjedde det en markant medgang i rapporterte hendelser i 2022. Nedgangen sammenliknet med året før var på omkring 30 prosent. Også sektorens cybersikkerhetssenter hos Sikt rapporterte om en nedgang i antallet hendelser registrert hos dem.

[15] Hendelser omfatter forsøk på brudd på informasjonssikkerheten og personvernet, faktiske brudd og registrerte avvik fra interne rutiner/retningslinjer for sikring av informasjonsverdier og behandling av personopplysninger.



Figur 4: Antall hendelser og brudd på informasjonssikkerheten 2018-2022

Det var også en nedgang i antallet mistenkte eller bekreftede forsøk på kunnskapstyveri, rekognosering, eller innbruddsforsøk fra statlige eller statsstøttede aktører. Vi merker oss at Nasjonal sikkerhetsmyndighet har registrert en liknende nedgang i denne typen trusselaktivitet rettet mot UH-sektoren.[16]

Trusselaktører

Basert på våre årlige kartlegginger i sektoren, antar vi at nettkriminelle grupper sto bak omkring 80 prosent av rapporterte informasjonssikkerhetshendelser i perioden 2018-2022. Antallet hendelser som trolig kan tilskrives statlige (eller statsstøttede) hackere, var langt mer beskjedent, men i 2021 var antallet noe høyere enn ellers. Også den elektroniske rekognoseringsaktiviteten rettet mot UH-sektoren var mer omfattende i 2021 enn hva vi har sett tidligere.

Det ble i tillegg rapportert om enkelte tilfeller av hacktivisme.[17] Hele perioden sett under ett var antallet slike hendelser svært begrenset.

Hendelser som ikke kan tilskrives trusselaktører – interne feil og uhell eller feil og uhell hos leverandører av datasystemer eller IT-tjenester – utgjorde noe i underkant av 20 prosent av alle rapporterte hendelser.

Antall og typer personvernhendelser

Antallet rapporterte personvernhendelser økte hvert år fra 2018 til 2021. Fra 2021 til 2022 var det imidlertid også her en nedgang (omkring 22 prosent). Den mest vanlige personvernhendelsen som virksomhetene rapporterte om, var mangelfull registrering av forskningsprosjekter i NSD/Sikt sitt meldingsarkiv, og manglende sluttmelding for slike prosjekter. Andre vanlige hendelser gjaldt blant annet manglende registrering av behandlinger i behandlingsprotokollen og feil lagring av personopplysninger.

Brudd på sikkerheten til personopplysninger som innebærer en risiko for personvernet til de registrerte, skal meldes til Datatilsynet. Også her følger utviklingen det samme mønsteret som

[16] Se «Nasjonalt digitalt trusselbilde 2023», side 10-11. Tilgjengelig på https://nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2023. Sist besøkt 07.11.2023.
[17] Dette er en form for sivil ulydighet hvor ulike aktivistgrupper benytter datainntrenging og dataangrep som virkemidler for å fremme eller skape oppmerksomhet om en politisk sak.

ovenfor: økning i antallet meldinger frem til 2021 og nedgang fra 2021 til 2022. Nedgangen fra 2021 var på 40 prosent.

Skadevirkninger

I tillegg til nedgang i hendelser og brudd på informasjonssikkerheten, rapporterte universitetene og høgskolene om få og lite alvorlige skadevirkninger som følge av bruddene i 2022 i forhold til perioden 2018-2021.

For eksempel førte det mest alvorlige tilfellet av vellykket direktørsvindel i 2022 til at en Dekan-månedslønn ble utbetalt til en trusselaktør.[18] I 2020 lyktes et titalls forsøk på direktørsvindel hvor ansatte ble lurt til å kjøpe gavekort til mellom 3000 og 10 000 kroner. I 2022 var det kun enkelte tilfeller av tilsvarende vellykkede forsøk på direktørsvindel.

Et annet eksempel er fra 2020, hvor en statlig eller statsstøttet trusselaktør lyktes med å få tilgang hos en av institusjonenes lokale datanettverk.[19] I 2022 rapporterte ingen av institusjonene om tilfeller av vellykkede forsøk på statlig hacking, men det var ett tilfelle av innsidevirksomhet med betydelig mediedekning hos en av institusjonene.[20]

Lavere trusselaktivitet

Tiden vil vise om nedgang i antallet informasjonssikkerhetshendelser i 2022 faktisk representerer et trendbrudd, eller om nedgangen er et midlertidig avvik fra mønsteret i 2018-2021. Dersom det viser seg å være et reelt trendbrudd, kan reduksjonen delvis skyldes at sektoren har forbedret sitt arbeid med informasjonssikkerhet og personvern, slik den økte modenheten i etterlevelse av kravene i policyen indikerer.

Heller ikke når det gjelder krenkelser av personvernet kan vi si for sikkert at nedgang i 2022 faktisk representerer et trendbrudd. Vi har likevel ingen indikasjoner på at nedgangen ikke er reell.[21] Uavhengig av om 2022 representerer et trendbrudd eller ikke, har nedgangen i antall hendelser og brudd påvirket risikoen for brudd på informasjons- og personopplysningssikkerheten.

---

[18] Risiko -og tilstandsvurdering 2019, s. 18-23, Risiko- og tilstandsvurdering 2020, s. 32-34, Risiko- og tilstandsvurdering 2021, s. 39-44, Risiko- og tilstandsvurdering 2022, s 34, og Risiko- og tilstandsvurdering 2023, s 34. Rapportene er tilgjengelige på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 09.01.2024.

[19] Risiko- og tilstandsvurdering 2021, s. 43, rapporten er tilgjengelige på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 11.01.2024.

[20] Se for eksempel PST om spionsiktet «gjesteforsker»: — Mistanken er styrket (khrono.no). Sist besøkt 11.01.2024.

[21] Vi har mindre tro på at et mulig trendbrudd kan skyldes mørketallsproblematikken, det vil si at virksomhetene har blitt mindre flinke til å oppdage og rapportere hendelser. Våre Risiko- og tilstandsvurderinger indikerer det motsatte: særlig de siste to-tre årene har sektoren iverksatt tiltak som styrker både oppdagelses- og rapporteringsevnen.

Utvikling i risiko for brudd og hendelser

I de fire siste av de fem risiko -og tilstandsvurderingene som Unit, og senere HK-dir, har publisert har risikoen for informasjonssikkerhetshendelser (risikoscenarioer) blitt vurdert. I tillegg er det blitt gitt vurderinger av om målene for informasjonssikkerhet og personvern i strategien for digital omstilling i UH-sektoren kan realiseres i løpet av strategiperioden. [22]

I dette kapittel beskriver vi utviklingen i vurderingen av risikoscenarioene som har blitt identifisert i de årlige risiko- og tilstandsvurderingene. [23] I neste kapittel gir vi en vurdering av hvilke tiltak som kan ha bidratt til å redusere risikoen for uønskede hendelser og brudd på informasjonssikkerheten.

Risikoscenarier og risikonivå 2019–2022

Risikoscenarioene som blir vurdert i de årlige risiko- og tilstandsvurderingene er brudd på informasjonssikkerheten som virksomhetene i UH-sektoren[24] rapporterte om eller uttrykte bekymring for.[25]

Det har vært noe variasjon i beskrivelsen av risikoscenarioer i risiko- og tilstandsrapportene. I risiko -og tilstandsvurderingen for 2019 (som vurderte risiko- og tilstand for arbeidet i 2018) ble sektorens arbeid med informasjonssikkerhet og personvern risikovurdert opp mot målsettingene i Strategi for digitalisering i høyere utdanning og forskning 2017-2021, og er derfor ikke med i denne oversikten. [26]

Listen nedenfor inkluderer alle risikoscenarioene som er blitt vurdert i perioden 2019-2022. Enkelte beskrivelser kan avvike noe fra formuleringene som er brukt i tidligere år, men skal innholdsmessig vise de samme risikoscenarioene:

- S1 = Løsepengevirus
- S2 = Statlig kunnskapsspionasje[27]
- S3 = Utilsiktede feil og uhell hos ansatte og leverandører av IT-systemer
- S4 = Direktør- og fakturasvindel

---

[22] Strategien er tilgjengelig på Strategi for digital omstilling i universitets- og høyskolesektoren 2021–2025 (regjeringen.no). Sist besøkt 11.01.2024.

[23] For en gjennomgang av rammeverket HK-dir bruker for vurdering av risiko se Risiko- og tilstandsvurdering 2021, s. 79-84 og 94-97, rapporten er tilgjengelige på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 11.01.2024

[24] Med UH-sektoren i denne sammenhengen mener vi til de 21 statlige universitetene og høgskolene, og de 7 øvrige forvaltningsorganene som er underlagt Kunnskapsdepartementets eierstyring.

[25] Risikoen for at brudd kan skje vurderes etter en skala med sannsynlighetsverdier i form av forventet hendelsesfrekvens, og en skala med konsekvensverdier etter alvorligheten av skadevirkningene av bruddet. Det er summen av rapporterte sårbarheter, tiltak, og vurdering av sikkerhetstilstand (modenhet i etterlevelse av kravene i policyen) som danner utgangspunktet for vurdering av risikoscenarioer- og nivå.

[26] Strategi for digitalisering i høyere utdanning og forskning 2017-2021 er tilgjengelig på Digitaliseringsstrategi for universitets- og høyskolesektoren - regjeringen.no. Sist besøkt 11.01.2024.

[27] Risikoscenariet (kunnskapsspionasje) er markert i to ulike celler, høy og lav, i risikomatrisen i Risiko- og tilstandsvurderingen for 2023. I 2019 gjelder er også utilsiktede feil og uhell vurdert til moderat og høy risiko (S3). Årsaken til dette er at Unit og senere HK-dir i disse tilfellene har vurdert risikoen til å være ujevnt fordelt i sektoren. I Tabell 1 er denne nyansen utelatt, og høyeste risikonivå er valgt for disse to scenarioene.

- S5= Tjenestenekt (DDoS)
- S6= Misbruk av lokale dataressurser (utvinning av kryptovaluta og dataangrep mot tredjeparter)
- S7= Kompromitterte brukerkontoer

I tabell 1 har vi samlet risikoscenarioene som oppsummerer risikovurderingene for hvert år det har blitt publisert risiko- og tilstandsvurderinger av informasjonssikkerhet og personvern:

Tabell 1: Utvikling i risikoscenarioer

Risikonivå/År	**2019**	**2020**	**2021**	**2022**
Høy	S3, S4, S7	S1, S7	S1, S2, S7	S1, S2
Middels	S1, S6	S3, S4	S3	S3, S5, S6
Lav	S5	S5	S4, S5	S4

Utvikling i scenarioer med middels til høy risiko

I risiko- og tilstandsvurderingen for 2020 (som vurderte risiko og tilstand for 2019) vurderte Unit risikoen som høy for brudd på informasjonssikkerheten som følge av utilsiktede feil og uhell (S3), direktør- og fakturasvindel (S4), kompromitterte brukerkontoer (S7).[28] Årsaken til at disse scenarioene ble vurdert til høy risiko på grunn av en kombinasjon av høy frekvens av forsøk på slike brudd, og moderat til høy grad av potensielle skadevirkninger. For eksempel ble kontaktinformasjonen til en person med hemmelig adresse tilgjengelig på internett som følge av en menneskelig feil hos en institusjon. Universitetene og høgskolene opplyste om at denne type hendelse (menneskelige feil og uhell) var vanlig dette året.

I 2020 ble risikoen for brudd som følge av utilsiktede feil og uhell vurdert til moderat risiko. Det samme ble direktør- og fakturasvindel. Årsaken var at konsekvensene av de utilsiktede feilene og uhellene som ble rapportert var mindre alvorlige enn året før. For svindelforsøkene var den største endringen at antallet rapporterte hendelser hadde blitt redusert, og høgskolene og universitetene opplyste i mindre grad om at de var bekymret for slike hendelser.

I de påfølgende årene har utilsiktede feil og uhell blitt holdt på et moderat nivå, hovedsakelig på grunn av de potensielle konsekvensene av denne typen brudd. Når det gjelder forsøk på direktør- og fakturasvindel er både antallet forsøk og vellykkede tilfeller falt betydelig. I tillegg var de få utbetalingene som ble utført som følge av direktør- og fakturasvindel lavere i 2021 og 2022 i forhold til tidligere år. Derfor ble risikoen for brudd på informasjons- og personopplysningssikkerheten vurdert som lav for denne typen hendelser i disse to årene.

[28] Nettkriminalitet ble for første og siste gang vurdert som et risikoscenario i risiko- og tilstandsvurderingen i 2019, s. 47. Scenarioet var ment som en samlekategori for ulike svindel -og tyveriforsøk, og datainnbrudd. I senere tilstandskartlegginger er denne typen forsøk fanget opp i S4 og S6. Rapporten er tilgjengelig på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 11.01.2024.

Kompromitterte brukerkontoer (S7) ble vurdert til å utgjøre en høy risiko for brudd på informasjons- og personopplysningssikkerheten fra 2019 til 2021. En trusselaktør som får kontroll over en eller flere brukerkontoer kan anvende tilgangene som følger kontoene til blant annet utsending av epost, datatyveri, og planting av skadevare. Skadevirkningene kan derfor bli omfattende.

I tillegg var kompromitterte brukerkontoer relativt vanlig blant universitetene og høgskolene: I 2019 oppga de fleste institusjonene om tilfeller av kompromitterte brukerkontoer, 2020 ble det rapportert om 300 tilfeller, og i 2021 rapportere institusjonene om 200 kompromitterte brukerkontoer. I 2022 hadde antallet kompromitterte brukerkontoer blitt redusert ytterligere i forhold til 2021.[29]

Både løsepengevirus (S1) og statlig kunnskapsspionasje (S2) er eksempler på brudd på informasjons- og personopplysningssikkerheten som kan gjennomføres ved å bruke kompromitterte brukerkontoer. Førstnevnte ble på grunn av få rapportere tilfeller og skadevirkninger vurdert til middels risiko i 2019, men har i de senere årene blitt vurdert til høy risiko. Risikoen økte i 2020 og 2021 blant annet på grunn av vellykkede tilfeller av løsepengevirus internasjonalt, og i andre sektorer i Norge.

I 2022 rapportere universitetene og høgskolene om 7 sannsynlige forsøk på løsepengevirusangrep, hvor ett av angrepene førte til kryptering av en datamaskin. Det sistnevnte angrepet ble håndtert ved å isolere datamaskinen fra nettverket, og dataene ble gjenopprettet via sikkerhetskopi. Skadevirkningene av et vellykket og omfattende løsepengevirusangrep kan bli svært omfattende, spesielt dersom viktige fellestjenester i UH-sektoren rammes.[30]

Statlig kunnskapsspionasje har blitt kommentert i Risiko- og tilstandsvurderingene også før 2022 versjonen, men da i sammenheng med APT-aktører og ikke som et eget risikoscenario. Årsaken til at dette ble et eget risikoscenario i 2021 er at enkelte institusjoner rapporterte om rekognoseringsaktivitet, og noen få tilfeller av datainnbrudd som sannsynligvis er utført av statlige eller statsstøttede trusselaktører. I tillegg har etterretnings- og sikkerhetstjenestenes opplyst om økt etterretningsaktivitet mot UH-sektoren i de årlige trussel- og risikovurderingene i 2022 og 2023.[31]

Skadevirkningene av vellykkede tilfeller av statlig kunnskapsspionasje kan være alvorlig for institusjonen som utsettes for bruddet, men også for nasjonale sikkerhetsinteresser. For institusjonen kan et slikt angrep ført til tap av forskningsdata i tillegg til andre skadevirkninger som omdømmetap.

---

[29] Årsaken til at dette kompromitterte brukerkontoer ikke er inkludert blant risikoscenarioene i 2022 er både på grunn av redusert hendelsesfrekvens og skadevirkninger, men også fordi kompromitterte brukerkontoer kan inngå som en del av de øvrige scenarioene som vurderes.

[30] Se for eksempel Vice Society Claims HAW Hamburg Data Breach From Dec 2022 (thecyberexpress.com). Sist besøkt 13.01.2024.

[31] Se for eksempel «Fokus 2022». Rapporten er tilgjengelig på Fokus - Etterretningstjenesten. Sist besøkt 15.01.2024. Se også «Sikkerhetsfaglig råd. Et motstandsdyktig Norge», side 53-57. Rapporten er tilgjengelig Sikkerhetsfaglig råd - Et motstandsdyktig Norge - Nasjonal sikkerhetsmyndighet (nsm.no). Sist besøkt 15.01.2024.

Når det gjelder de nasjonale sikkerhetsinteressene kan de skades ved at for eksempel forsking undergitt eksportkontrollforskriften og/eller internasjonale sanksjoner bli tilgjengelig for stater med interesse av å benytte forskningsresultatene til utvikling av masseovervåkning eller våpen.[32]

Utvikling i scenarioer med middels til lav risiko

I tillegg til løsepengevirus (S1), som er kommentert ovenfor, ble misbruk av lokale dataressurser (S6) vurdert til middels risiko i 2019, mens tjenestenekt eller DdoS-angrep (S5) ble vurdert til lav risiko. Misbruk av lokale dataressurser kan innebære at datamaskiner tilhørende universitetene og høgskolene benyttes av en trusselaktør til å angripe andre mål i og utenfor sektoren, eller for å utvinne kryptovaluta. De potensielle skadevirkningene av dette scenarioet er varierende, fra litt dyrere strømregning og tregere prosessering av forskningsdata hos en institusjon til kompromittering av sensitive data hos tredjeparter.

I 2019 og 2020 var det flere tilfeller av denne typen brudd, for eksempel ble datakraften fra ett tungregneanlegg misbrukt til utvinning av kryptovaluta over en lengre periode.[33] I 2021 og 2022 ble det rapportert om henholdsvis få og ingen slike brudd blant universitetene og høgskolene. Risikoen ble derfor vurdert til middels i 2019, og middel til lav i 2022 for denne typen hendelser.

Tjenestenektsangrep (DdoS) innebærer å angripe en tjeneste for å hindre bruken av den, for eksempel ved å overbelaste et nettsted med trafikk slik at den ikke blir tilgjengelig for sine brukere. Skadevirkningene av slike angrep kan være betydelige i UH-sektoren, for eksempel dersom slike angrep skjer under eksamensavviklingen.

Det har ikke blitt rapportert om betydelige skadevirkninger som følge av slike angrep i perioden 2018-2022. I 2022 ble imidlertid risikoen for tjenestenektangrep justert opp til middels, blant annet på grunn av at det ble registrert ett tilfelle av et større tjenestenektangrep i UH-sektoren dette året. Angrepet var trolig utført med bakgrunn i krigen i Ukraina.

---

[32] Se «Nasjonal trusselvurdering 2023», s. 20. Rapporten er tilgjengelig på NTV-2023 (pst.no), sist besøkt 15.01.2024. Se også NTNU-forsker: Frykter teknologien brukes til masseødeleggelsesvåpen – E24. Sist besøkt 19.01.2024.

[33] Risiko- og tilstandsvurderingen i 2021, s. 40. Rapporten er tilgjengelig på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 15.01.2024.

Effekter av arbeidet med informasjonssikkerhet og personvern

De målrettede tiltakene som har blitt gjennomført hos institusjonene har sannsynligvis bidratt til økt etterlevelse av kravene i policyen, og bidratt til at risikoen for at enkelte typer hendelser og brudd er redusert. I det følgende peker vi på et utvalg av slike tiltak, og beskriver deres effekt på arbeidet med informasjonssikkerhet og personvern.

Organisatoriske tiltak: økt kompetanse, kapasitet, og samarbeid i sektoren

I 2018 opplyste 19 av 21 institusjoner at de hadde for lite kompetanse og kapasitet til å gjennomføre det praktiske arbeidet med informasjonssikkerhet og personvern. Konsekvensen var, ifølge institusjonene, at mange oppgaver ikke ble utført, ble utført for sjelden, eller ble utført med mangelfull kvalitet.[34]

Institusjonene har i perioden fra 2018 til 2022 økt ressursinnsatsen som er avsatt til arbeidet med informasjonssikkerhet og personvern med 42 årsverk. Dette tilsvarer en økning på 62 prosent. Universitetene og høgskolene har også økt sin kapasitet i perioden ved å engasjere medarbeidere fra flere deler av organisasjonen. Dette har skjedd gjennom opprettelse av interne nettverk eller forum for informasjonssikkerhet og personvern.

Tabell 2: Endringer i antall årsverk universiteter og høgskoler, 2018-2022[35]

År	2018	2019	2020	2021	2022
Antall årsverk	69	82	89	100	111

Også økt bruk av tjenester fra konsulentselskaper og advokatfirmaer har bidratt til å dekke opp for noe av den manglende kapasitet og kompetanse hos institusjonene. I tillegg rapporterte flere av universitetene og høgskolene om at samarbeid med andre institusjoner i sektoren, blant annet gjennom felles møteplasser i sektoren, har styrket deres arbeid med disse forvaltningsområdene.

På sektornivå har Cybersikkerhetssenteret siden sin opprettelse i 2021 støttet opp under kompetansen og kapasiteten til universitetene og høgskolene med veiledere og sektortiltak som sårbarhetsskann.[36]

Flere institusjoner har også styrket sin oversikt over egne informasjonsverdier. Dette har skjedd gjennom at institusjonene har kartlagt forskningsdata, personopplysninger, tjenester og utstyr, leverandører og avtaler, og annen sensitiv informasjon som de forvalter.[37] Flere institusjoner

[34] Risiko- og tilstandsvurdering 2019, s. 30-34. Rapporten er tilgjengelig på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 16.01.2024.
[35] Tallene i tabellen er avrundet til nærmeste heltall.
[36] Se Cybersikkerhet for forskning og utdanning (sikt.no) for mer informasjon om Cybersikkerhetssenteret. Sist besøkt 18.01.2024.
[37] Se risiko- og tilstandsvurdering 2023, s. 22. Rapporten er tilgjengelig på Informasjonssikkerhet og personvern i høyere utdanning og forskning | HK-dir (hkdir.no). Sist besøkt 26.01.2024.

rapporterer om at slike oversikter benyttes i risikovurderingsprosesser, og har slik bidratt til at institusjonene også har forbedret sin risikostyring.

Den økte kapasiteten og kompetansen hos universitetene og høgskolene har sannsynligvis ført til at flere oppgaver blir løst på en bedre måte enn tidligere, og slik bidratt til at kravene i policyen etterleves på et høyere nivå i 2022 enn i 2018. Samtidig har kapasitetstilveksten tilført utvidet kompetanse, og dermed sannsynligvis økt evne til å forebygge, oppdage, og håndtere uønskede hendelser og brudd på informasjons- og personopplysningssikkerheten.

En annen viktig effekt av de organisatoriske tiltakene ovenfor, er at universitetene og høgskolene ser ut til å ha avdekket nye og større kompetansebehov i arbeidet med informasjonssikkerhet og personvern. Universitetene og høgskolenes rangering av de viktigste sårbarhetskategoriene ser ut til å underbygge dette: I 2020 rangerte universitetene og høgskolene kompetanse og kapasitet som henholdsvis den andre og tredje viktigste sårbarhetskategorien. I 2022 hadde kompetanse klatret opp på førsteplass, mens kapasitet var nå den fjerde viktigste sårbarheten.

Pedagogiske tiltak: Informasjon, opplæring, og øvelser

I tillegg til få hender i arbeid, rapporterte institusjonene om at det var lav bevissthet om arbeidet med informasjonssikkerhet og personvern i 2018. Informasjonssikkerhetsarbeidet var på dette tidspunktet hovedsakelig et anliggende for IT-avdelingene i sektoren, mens personvernarbeidet i all hovedsak ble ivaretatt av personvernombudene med støtte fra enkelte ansatte i administrasjonene. Konsekvensene av lav bevissthet om vanlige trusler, krav, rutiner, og hensikt med arbeidet med informasjonssikkerhet og personvern, var økt risiko for brudd og uønskede hendelser.

Både ledelsessystem for informasjonssikkerhet og internkontroll for personvern forutsetter bred involvering i organisasjonen for å kunne fungere etter hensikten. Dette var i liten grad oppnådd i 2018, noe universitetene og høgskolene ga uttrykk for ved å rangere manglende bevissthet om dette arbeidet som den største sårbarhetskategorien dette året.

I de påfølgende årene er det blitt gjennomført en rekke tiltak for å øke bevisstheten til ansatte og studenter i sektoren. Tiltakene varierte i omfang og målgruppe, for eksempel er deltakelse i sikkerhetsmåneden med nanolæringskurs for alle ansatte blitt vanlig siden 2020. Det samme har publisering og oppdatering av lagringsguider og nettvettregler for studenter og ansatte.

Universitetene og høgskolene har også gjennomført kurs for medarbeidere og ledere med særlig ansvar for arbeidet med informasjonssikkerhet og personvern. Kursene var ment å heve både bevissthet og kompetanse. Institusjonene har beskrevet effektene av tiltakene, for eksempel ved at personvernombudene mottok flere henvendelser om lovlig behandling av personopplysninger enn tidligere. Det samme gjorde enkelte IT-avdelinger om temaer som å medbringe IT-utstyr til utlandet.

Også årlige øvelser på håndtering av informasjonssikkerhetshendelser har blitt vanlig for de fleste institusjonene, selv om det under pandemien i 2020 og 2021 var noe mindre aktivitet på dette feltet enn i 2022. Universitetene og høgskolene beskriver effekter av øvelsene som for eksempel bedre samhandling i krise- og beredskapsgrupper, og forbedringer i beredskaps- og kontinuitetsplaner som følge av læringspunktene fra øvelsene.

For hvert år HK-dir har gjennomført risiko- og tilstandsvurderinger har institusjonene rapportert om stadig bedre bevissthet knyttet til informasjonssikkerhet og personvern blant administrativt og vitenskapelig ansatte. Dette har bidratt til økt modenhet blant universitetene og høgskolene i etterlevelse av kravene som retter seg mot kjennskap og bevissthet om regelverket om forsvarlig behandling av personopplysninger mellom 2018 og 2022. Det er også mulig at disse tiltakene har bidratt til at skadevirkningene fra utilsiktede feil og uhell hos institusjonene har falt i 2022.

Vi antar at også utviklingen av den internasjonale sikkerhetssituasjonen, for eksempel krigen i Ukraina, har bidratt til større bevissthet om egen sikkerhet.

Tekniske tiltak: Totrinnsinnlogging, sårbarhetsskann og sikkerhetskopiering

I 2019 uttrykte et flertall av institusjonene at den tekniske kompleksiteten ved flere av sektorens digitale løsninger utgjorde en sårbarhet for informasjons- og personopplysningssikkerheten. Blant annet gjorde tusenvis av brukerkontoer og datamaskiner, hundrevis av IT-systemer, og mange ulike lagringsløsninger det utfordrende å oppdage avvik og mistenkelig aktivitet.

Også på dette området har universitetene og høgskolene gjennomført tiltak for å utbedre sårbarheter. Eksempler på slike tiltak inkluderer redusert teknisk gjeld,[38] tatt i bruk eller forbedret interne sårbarhetsskann av eget datanettverk, forbedret systemer og rutiner for installasjon av sikkerhetsoppdateringer. Også tiltak som forbedret tilgangsstyring for brukerkontoer, utvidet totrinnsinnlogging, og anskaffelse av tjenester eller verktøy for logganalyse har bidratt til å styrke informasjonssikkerheten i perioden.

De nevnte tiltakene er i varierende grad innført hos universitetene og høgskolene. Vi mener likevel at innføringen av tiltakene har bidratt til at skadevirkningene og antallet vellykkede forsøk på brudd har blitt redusert i perioden. For eksempel mente flere av institusjonene at innføring av totrinnsinnlogging forklarte mye av nedgangen av kompromitterte brukerkontoer i 2021.[39]

Styringseffekt - HK-dir sitt bidrag til arbeidet med informasjonssikkerhet og personvern

HK-dir gir hvert enkelt universitet og høgskole tilbakemeldinger på sitt arbeid med informasjonssikkerhet og personvern. Dette skjer i brev med anbefalinger til det videre arbeidet med informasjonssikkerhet og personvern.

Anbefalingene har som hensikt å bidra til at universitetene og høgskolene gjennomfører tiltak som forbedrer etterlevelsen av kravene i policyen, og slik gir et høyere sikkerhetsnivå. I perioden 2020 til 2022 har stadig flere av HK-dirs anbefalinger blitt fulgt helt eller delvis av universitetene og høgskolene.

Tabell 3: Fulgte anbefalinger fra HK-dir

År	2020	2021	2022

[38] Institusjonene har redusert bruken av eldre og sårbare IT-systemer enten ved å avvikle dem, oppgradert til nyere versjoner, eller skjermet systemene bedre mot angrep via internett.

[39] Se Risiko- og tilstandsvurdering 2022, s. 33. Rapporten er tilgjengelig på Styring av informasjonssikkerhet og personvern | HK-dir (hkdir.no). Sist besøkt 19.01.2024.

Helt eller delvis fulgte anbefalinger	57%	69%	72%

Vi mener at effekten av HK-dir sine anbefalinger understøtter arbeidet med informasjonssikkerhet og personvern hos universitetene og høgskolene ved å gi en ekstern vurdering av retningen på deres arbeid og prioriteringer innen disse forvaltningsområdene. En tilbakemelding vi har merket er at kartleggingene og anbefalingsbrevene gir merverdi for institusjonene, spesielt ved at det pekes på konkrete avvik som må lukkes.

Konklusjoner

Moderat forbedring i etterlevelse av kravene

Siden 2018 har det gjennomsnittlige modenhetsnivået i etterlevelse av Kunnskapsdepartementets policy steget fra et lavt til middels nivå hos institusjonene. I løpet av perioden har alle universitetene og høgskolene etablert de viktigste rutinene i internkontroll for personvern, og den styrende delen av ledelsessystemet for informasjonssikkerhet. I 2022 etterlevde to av universitetene kravene i departementets policy for informasjonssikkerhet og personvern på en tilfredsstillende måte. Resten av institusjonene etterlevde deler av kravene i policyen.

Universitetene og høgskolene har forbedret seg mest når det gjelder kontinuitets- og beredskapsplaner, tiltak for å styrke bevissthet om personvernregelverket og rutiner for å ivareta de registrertes rettigheter. Samlet sett betyr dette at institusjonene har styrket seg noe mer i arbeidet med personvern enn arbeidet med informasjonssikkerhet.

Institusjonene har mest arbeid igjen med kravene som retter seg mot den utførende og kontrollerende delen av ledelsessystem for informasjonssikkerhet og internkontroll for personvern. Institusjonene har også behov for å jobbe videre med kontinuitets- og beredskapsplanverk, og tiltak for å øke kjennskap til og bevissthet om personvernregelverket.

Fra og med 2022 er det registrert en nedgang i hendelser og brudd på informasjons- og personopplysningssikkerheten. En rekke tiltak hos universitetene og høgskolene har trolig bidratt til økt evne til å forebygge, oppdage, og håndtere forsøk på brudd på informasjons- og personopplysningssikkerheten i perioden.

Risikoen for brudd på informasjons -og personopplysningssikkerheten forårsaket av løsepengevirus og statlig hacking (kunnskapsspionasje) har økt fra 2019 til 2022, og vurderes som høy. Risikoen for enkelte andre typer brudd, for eksempel direktør- og fakturasvindel, er redusert i løpet av perioden.

Et mer krevende trusselbilde gir nye utfordringer

Det er positivt at universitetene og høgskolene har økt sin etterlevelse av kravene i kunnskapsdepartementets policy, og forbedret sin evne til å forebygge, oppdage og håndtere uønskede hendelser og avvik. Det er også positivt at risikoen for at enkelte typer informasjonssikkerhetshendelser og krenkelser av personvernet er redusert.

Det er likevel enkelte utviklingstrekk som indikerer at det kan bli mer utfordrende å forebygge, oppdage, og håndtere alvorlige brudd på informasjonssikkerheten i de neste årene.

Et slikt trekk er endringene i den internasjonale sikkerhetssituasjonen. PST har i flere år pekt på at nettverksopperasjoner utgjør en stor del av russisk og kinesisk etterretningsaktivitet i Norge. Dette er operasjoner som også kan rette seg mot forskningsmiljøer i UH-sektoren. Etter invasjonen av Ukraina i 2022 forventer PST at Russland i større grad enn tidligere vil benytte seg av metoder som nettverksoperasjoner for å tilegne seg kunnskap innen strategisk viktige forskningsområder, for eksempel undervannsteknologi, kunstig intelligens eller bioteknologi.[40]

I tillegg har nettkriminelle grupper utviklet sine metoder i perioden. For eksempel virker det som at forsøk på nettsvindel, phishing, og datainntrenging er blitt mer personrettet og avanserte enn tidligere.[41] NSM forventer at de nettkriminelle gruppene fremover vil benytte seg av kunstig intelligens og store språkmodeller til å forbedre sine forsøk på svindel og datainntrenging.[42] Denne utviklingen øker behovet for å beskytte ansatte mer enn tidligere, og utfordrer både kapasiteten og kompetansen hos universitetene og høgskolene.

Endringene i trusselbildet og funnene fra HK-dir sine risiko- og tilstandsvurderinger, viser et behov for å forsterke arbeidet med informasjonssikkerhet og personvern i de kommende årene. Riksrevisjonens kontroll av informasjonssikkerheten i forskningssystemer peker på det samme.

Behov for mer kunnskap om effekten av iverksatte tiltak

Etter fem år med kartlegging av arbeidet med informasjonssikkerhet og personvern, ser vi nå et behov for mer kunnskap om effekten av de tiltakene virksomhetene har iverksatt. Selv om universitetene og høgskolene samlet sett har hatt moderat fremgang i arbeidet med informasjonssikkerhet og personvern, er det enkelte institusjoner som har styrket seg mer enn andre.

I tillegg varierer omfanget av institusjonenes egen testing av sikkerhetstiltak, og evaluering av gjennomførte tiltak.[43] De institusjonene som gjennomfører slike tester og målinger, velger selv om de rapporterer overordnet om dette til HK-dir i de årlige kartleggingene. HK-dir har derfor ikke detaljert innsikt i resultatene fra slike tester og målinger.

Slik vi ser det, vil nye sektortiltak som i større grad kan måle effekten av iverksatte tiltak kunne styrke institusjonens arbeid med informasjonssikkerhet og personvern. Mer kunnskap om effekten av tiltak vil også gjøre HK-dir bedre i stand til å støtte institusjonene, og gi departementet et bedre grunnlag for vurdering av sektortiltak og styring. Et mulig sektortiltak kan være periodiske revisjoner av arbeidet med informasjonssikkerhet og personvern hos universitetene og høgskolene.

---

[40] Se Nasjonal trusselvurdering 2023, s. 13-14. Rapporten er tilgjengelig på: NTV-2023 (pst.no). Sist besøkt 25.01.2024.

[41] Se for eksempel M-trends 2023, s. 71-77. Rapporten er tilgjengelig på Top Trends in Cyber Security | Cyber Attacks Trends | M-Trends (mandiant.com)

[42] Se «Nasjonalt digitalt trusselbilde 2023», s.12. Tilgjengelig på https://nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-digitalt-risikobilde-2023. Sist besøkt 25.01.2024.

[43] Riksrevisjonen fant også at gjennomføring av evalueringer og testing av sikkerhetstiltak varierte blant institusjonene som ble revidert. Se Riksrevisjonens rapport «informasjonssikkerhet i forskning innenfor kunnskapssektoren» s. 13-15. Rapporten er tilgjengelig på Dokument 3:11 (2023–2024) (riksrevisjonen.no). Sist besøkt 31.01.2024.

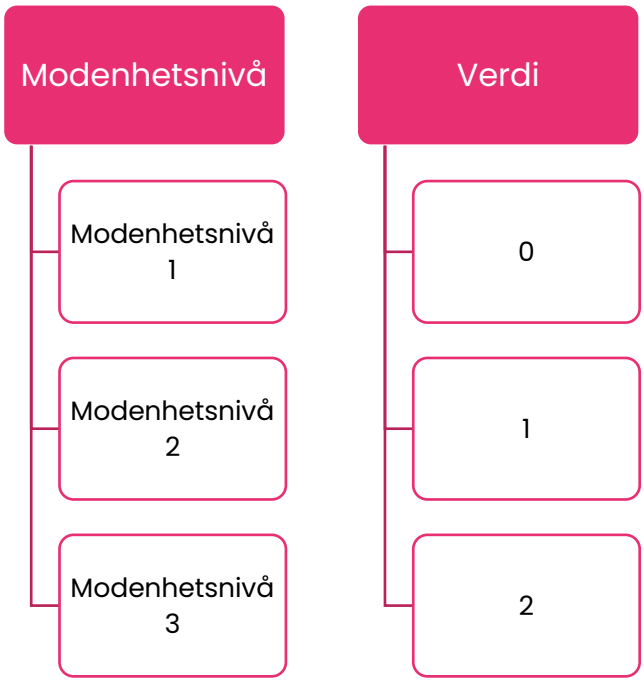
Vedlegg 1 – Metode og fremgangsmåte

Universitetene og høgskolene har årlig blitt fått vurdert sin etterlevelse av kravene i Kunnskapsdepartementets Policy for informasjonssikkerhet og personvern i perioden 2018 til 2022 av Unit, og senere HK-dir. Policyen har totalt 12 krav med 55 underpunkter, og samtlige krav blir vurdert av HK-dir. Vurderingene av kravene illustreres ved et modenhetsnivå på en skala med tre nivåer:

1. **Modenhet 1 - Lav grad av etterlevelse**: Det er behov for vesentlige forbedringer i arbeidet med kravet.
2. **Modenhet 2 - Moderat grad av etterlevelse**: Det er behov for enkelte forbedringer i arbeidet med kravet.
3. **Modenhet 3 - Tilfredsstillende grad av etterlevelse**: Etterlevelsen av kravet vurderes som tilfredsstillende.

Hvert modenhetsnivå har tilhørende kriterier som universitetene, høgskolene og de øvrige forvaltningsorganene og selskapene blir vurdert opp mot individuelt[4]. Policyen oppsummerer lovpålagte krav til arbeidet med informasjonssikkerhet og personvern, og derfor er kun tilfredsstillende (modenhet 3) akseptabel grad av etterlevelse av kravene for Kunnskapsdepartementet.

I temarapporten er hensikten med summering av modenhetsnivå per år å illustrere utviklingen av institusjonenes etterlevelse av kravene til informasjonssikkerhet og personvern over tid. Hvert modenhetsnivå er tilordnet en numerisk verdi, slik figur 5 viser.



Figur 5: Modenhetsnivå til verdier

Dette innebærer at hvert universitet og hver høgskole får en poengsum som tilsvarer deres modenhetsnivå i etterlevelse av policyen. Den aggregerte summen av de 21 universitetene og høgskolenes poengsum gir et bilde på universitetenes og høgskolenes samlede etterlevelse av kravene i departementets policy for informasjonssikkerhet og personvern.

Direktoratet for
høyere utdanning
og kompetanse

post@hkdir.no hkdir.no