UNIVERSITETET I BERGEN

Styre: Universitetsstyret
Styresak: 120/21
Møtedato: 28.10.2021

Dato: 20.10.2021
Arkivsaksnr: 2021/13901

Status og tiltak informasjonssikkerhet

Henvisning til bakgrunnsdokumenter

- Styresak 67/19 Internrevisjonsrapport - *Lokalt driftede IT-systemer*
- Styresak 16/20 *Styringsmodell for* IKT
- Styresak 70/20 Internrevisjonsrapport 2020/02 Test av informasjons- og cybersikkerhet

Saken gjelder:

Svak informasjonssikkerhet truer noen av universitetenes og forskningens mest grunnleggende verdier som integritet, autonomi og troverdighet, i tillegg til rene operasjonelle verdier som driftsstabilitet og økonomi.

Trusselnivået innen informasjonssikkerhet har økt vesentlig de siste årene, og universitets- og høyskolesektoren er attraktive mål. Dette stiller krav til vår operasjonelle sikkerhet og beredskap, i tillegg til gode strukturer og god organisering. I tillegg har de formelle kravene til rapportering og internkontroll økt vesentlig, noe som også krever ressurser og oppmerksomhet.

Formålet med saken er å gi styret en overordnet status for informasjonssikkerhet ved Universitetet i Bergen og en beskrivelse og forankring av tiltak. Tiltakene har budsjettmessige forutsetninger som fremmes i budsjettforslaget for 2022, i tillegg til organisatoriske justeringer.

Forslag til vedtak:

Universitetsstyret tar saken til orientering og ber universitetsdirektøren arbeide videre med prosess for oppfølging av anbefalte tiltak slik de er beskrevet i saksframstillingen.

Robert Rastad
Universitetsdirektør

20.10.2021/Maria Lundhaug/Tore Burheim (avd.dir)

Vedlegg:
1. Saksframstilling

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	120/21	28.10.2021	2021/13901

Status og tiltak informasjonssikkerhet

Bakgrunn

Svak IT-sikkerhet truer noen av universitetenes og forskningens mest grunnleggende verdier som integritet, autonomi og troverdighet, i tillegg til rene operasjonelle verdier som driftsstabilitet og økonomi. Dessuten er universitetenes IT-infrastruktur og IT-systemer attraktive som brohoder for angrep på andre offentlige og private virksomheter. Utfordringene med å ivareta god IT-sikkerhet er økende, både generelt i samfunnet og innenfor universitets- og høyskolesektoren. Nasjonal sikkerhetsmyndighet, e-tjenesten og PST har påpekt det økte trusselnivået i sine trusselvurderinger.

Da UiB sentraliserte sine IT-tjenester i 2006 ble «fagnære» IT-systemer igjen på institutt og i forskningsgrupper. Etter 2006 har flere miljøer flyttet sin drift til IT-avdelingen, men veksten i bruk av informasjonsteknologi gjør at en betydelig mengde IT-utstyr og IT-systemer brukt i forskning driftes og forvaltes spredt rundt på UiB. Samtidig har IT-avdelingen etablert tjenester for håndtering av sensitive data (SAFE), integrerte IT-løsninger i laboratorier (LabIT) og tjenester for tungregning (superdatamaskiner).

Gjennom to internrevisjoner er det dokumentert at UiB har vesentlig forbedringspotensial når det gjelder organisering, drift og forvaltning av IT-utstyr og IT-systemer på institutter og i forskningsgrupper. Dette omfatter i all hovedsak utstyr og systemer knyttet til forskning, men også noe til undervisning. Universitetsstyret har i forbindelse med behandling av disse rapportene etterspurt tiltak. Svak organisering med mangelfull kompetanse og kapasitet gjør oss sårbare og gir seg utslag i svekket informasjonssikkerhet.

IT-avdelingen har etablerte strukturer for å ivareta informasjonssikkerheten innenfor sitt ansvarsområde og sine tjenester. Basert på det økte trusselnivået har avdelingen iverksatt tiltak for å bedre sikkerheten. Det er nå behov for et mer omfattende arbeid for å rette opp svakhetene som ble avdekket i internrevisjonsrapportene på en strukturell måte. Dette arbeidet forutsetter tilførsel av ressurser og om nødvendig en endring av det operative ansvaret slik at ivaretagelse av informasjonssikkerheten blir bærekraftig over tid.

Gjennom endringene i UiBs Styringssystem for informasjonssikkerhet og personvern[1] har UiB i utgangspunktet en tilstrekkelig styringsstruktur og omforente krav for å ivareta informasjonssikkerheten. Det er nå nødvendig å sikre en organisering av drift og forvaltning som gjør det mulig å oppfylle disse kravene. Kravene er strengere enn dagens praksis, men i tråd med nasjonale anbefalinger. Endringene på området må gjøres på en slik måte at det ikke skader forskningsaktiviteter, men derimot har som mål å bedre kvaliteten i UiBs samlede e-infrastruktur og IT-tjenester til forskning. Dette er også i tråd med planen i UiB FRAM.

Kunnskapsdepartementet, Direktoratet for høyere utdanning og kompetanse (HK-dir) og øvrige myndigheter har økende oppmerksomhet på informasjonssikkerhet og personvern, blant annet gjennom eierstyring. Kravene til dokumenterte tiltak og etterlevelse av lover, forskrifter og andre retningslinjer øker, noe som også krever ressurser. Det gjør at ressurssituasjonen er krevende på hele området.

[1] Sist endret i styresak 16/20 *Styringsmodell for IKT*

Informasjonssikkerhet og universitetenes verdigrunnlag

Universitetene er kunnskapssamfunn som utvikler, forvalter og formidler kunnskap. Mye av denne kunnskapen springer ut fra, formidles gjennom, og bygger på informasjon og data i ulike former. Brorparten av denne informasjonen og disse dataene samles inn, bearbeides, prosesseres, og lagres ved hjelp av informasjonsteknologi. IT-systemer og IT-infrastruktur er derfor kritiske bestanddeler både innen forskning, undervisning, formidling og innovasjon. I tillegg er informasjonsteknologi kritisk nødvendig i universitetets administrative og operative virksomhet.

Dersom vi selv eller våre omgivelser ikke kan feste lit til våre data og behandlingen av disse, er mye av grunnlaget for vår forskning, undervisning, viten og vår kunnskap vesentlig svekket. Her holder det at det er tilstrekkelig usikkerhet om dataenes integritet, før det har skadet troen på våre forskningsresultater, kvaliteten i vår undervisning, eller kompetansen til våre studenter.

Dersom noen eksterne med overlegg og uten vår viten manipulerer våre data, vil våre forskningsresultater bli feilaktige. Vi kan med andre ord bli manipulert til å trekke feilaktige forskningsresultater. Tilsvarende vil vi kunne bli utsatt for utpresning dersom uvedkommende får tilgang til våre data eller sensitive opplysninger. Det samme vil være tilfelle dersom våre data eller systemer gjøres utilgjengelige gjennom kryptering.

I tillegg forvalter universitetssamfunnet betydelige verdier direkte gjennom eierskapet til data. Dette omfatter ofte data det er brukt år på å samle inn, bearbeide og prosessere. Det er også potensielt store verdier i resultatene ved bruk av disse dataene.

Universitetet i Bergen eier, drifter og forvalter en betydelig IT-infrastruktur. Sammen med universitetets gode omdømme gjør dette universitetet til et attraktivt brohode for angrep mot andre virksomheter. Datatrafikk fra UiB vil i utgangspunktet bli sett på som legitim. Dersom andre virksomheter begynner å tvile på vår IT-sikkerhet vil det medføre problemer for vår digitale samhandling og samarbeid med andre. Vi ønsker heller ikke å bli brukt som redskap for å skade andre eller for annen kriminell virksomhet.

Som det framgår, vil svak informasjonssikkerhet og brudd på informasjonssikkerheten kunne undergrave universitetets grunnleggende verdier, svekke vårt omdømme, og gi betydelige negative samfunnskonsekvenser. I tillegg kan alvorlige angrep ha vesentlige operative konsekvenser og betydelige kostnader. God informasjonssikkerhet er derfor nødvendig for å ivareta universitetets grunnleggende verdier, vår virksomhet og vårt samfunnsansvar.

Status informasjonssikkerhet

Litt skjematisk kan man dele informasjonssikkerhetsarbeidet i fire områder:

- styring og etterlevelse,
- operativ sikkerhet og beskyttelse,
- deteksjon og beredskap,
- informasjon og kompetanse.

I det følgende er det gjort rede for status på UiB for hvert av disse områdene på overordnet nivå.

Styring og etterlevelse

Dette omfatter styringsmodell, ansvar og myndighet, tiltak for etterlevelse lover, forskrifter og retningslinjer, intern- og eksternrevisjon og annen formell rapportering.
UiB er underlagt en rekke lover, forskrifter og formelle krav knyttet til informasjonssikkerhet og personvern. Det er for omfattende å ta med alle, men følgende kan nevnes:

- Grunnleggende er **e-forvaltningsforskriften**[2] og særlig dennes krav om et styringssystem for informasjonssikkerhet bygd på anerkjente standarder. UiB har et styringssystem bygd på ISO 27001, med konkrete sikkerhetsmål som bygger på NSMs grunnprinsipper for IKT-sikkerhet. Styringssystemet ble innført i 2015 og ble siste gang revidert i 2019. Systemet gir styringsmodell, organisering og rammene for arbeidet med informasjonssikkerhet på UiB. Styringssystemet inneholder også retningslinjer med blant annet krav til drift og forvaltning, lagring, tjenester på nett mv.
- Kunnskapsdepartementet har innført en **styringsmodell for informasjonssikkerhet** for hele sektoren bygd på ISO 27014. Her har HK-dir[3] en tilsynsrolle og UiB rapporterer årlig til HK-dir og får tilbakemeldinger. Tilbakemeldingene har jevnt over vært gode og anbefalingene i tråd med vårt arbeid med kontinuerlig forbedring og planlagte tiltak.
- Kunnskapsdepartementet besluttet med virkning fra 1. oktober 2020 en ny **policy for informasjonssikkerhet og personvern i høyere utdanning og forskning**[4]. Policyen er relativt omfattende med blant annet 55 enkeltkrav. UiB skal rapportere på etterlevelse på denne en gang per år til HK-dir, jfr. styringsmodellen for sektoren.
- Nasjonal Sikkerhetsmyndighets (NSMs) **grunnprinsipper for IKT -sikkerhet**. Disse grunnprinsippene får økende oppmerksomhet og det er en anbefaling til statlige virksomheter om bruk av disse blant annet i digitaliseringsrundskrivet[5]. Som eier av en stor infrastruktur bør UiB følge disse grunnprinsippene. De er derfor lagt inn i vårt styringssystem for informasjonssikkerhet, men med en tilpasning til universitetets egenart.
- Krav til håndtering av helsedata formulert i lover og forskrifter. **Norm for informasjonssikkerhet i helsesektoren** (Normen) er en omforent fortolkning av de tekniske sidene av lovverket. UiB legger Normen til grunn for all vår behandling av helsedata og andre personsensitive data, og har etablert rutiner og tekniske løsninger[6] som følger disse.
- **GDPR og personvernlovgivningen** er et omfattende lovverk der konsekvensene for brudd er vesentlige med høye bøter. EU-domstolens avsigelse av Schrems II-dommen[7] legger en del premisser for bruk av internasjonale skytjenester og vil påvirke rammene for vår bruk av slike. Etterlevelse av europeiske retningslinjer på området er omfattende, og det forutsetter et betydelig kartleggingsarbeid framover. Dette vil kreve strengere godkjenningsrutiner for anskaffelser av skytjenester på UiB.

---

[2] Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

[3] Fram til 1.juli 2021 var dette Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning.

[4] Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning https://www.regjeringen.no/no/dokumenter/f-04-20-policy-for-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning/id2769629/

[5] Dette ble poengtert i regjeringens pressemelding om datainnbruddet på Stortinget i 2020.

[6] SAFE er UiBs løsning for dette. SAFE står for Sikker adgang til forskningsdata og e-infrastruktur.

[7] https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/

I tillegg ble det i tildelingsbrevet for 2021 avklart at **Sikkerhetsloven** gjelder for universitetene. Det innebærer ytterligere krav til styringssystemer, krav til virksomheten og sikring av vår informasjonsteknologi.

UiB har gjennom siste revisjon av styringssystemet for informasjonssikkerhet og personvern et tilstrekkelig rammeverk for styring og krav til sikker drift og forvaltning. Ut fra det som kom fram i internrevisjonen av lokalt driftete IKT-systemer, senere sikkerhetstester samt oppfølging i ettertid, er det grunn til å anta at det meste av organisering av drift og forvaltning av IT-systemene på institutter og fakulteter ikke vil være i stand til å oppfylle nasjonale anbefalinger og krav. Dette er noe av bakgrunnen for det foreslåtte tiltaket med etablering av Prosjekt sikre forskningssystemer.

Som det framkommer over, er strukturen for styring, rapportering rimelig godt dekket selv om det er ressursknapphet. Krav til rapportering, vurderinger, dokumentasjon har økt vesentlig de siste årene og forutsetter tilførsel av ressurser.

Operativ sikkerhet og beskyttelse

Dette omfatter de faktisk eksisterende sikkerhetstiltak, og er summen av tekniske løsninger, adferd og kultur. Dette omfatter det som er implementert i systemer, eksisterende barrierer og beskyttelse, brannmurer, konfigurasjon, sikkerhetsarkitektur, påloggingsløsninger, passordpolicy, mv. De tekniske barrierene er det som beskytter oss når ingen er på jobb.

UiB har i 2020 og i 2021 innført en rekke nye tiltak for å bedre den operative sikkerheten i de sentrale systemene, blant annet tofaktor-pålogging, brannmur, bedre skjerming av sikkerhetskopier mot kryptoangrep, samt oppdeling av datanettet for bedre beskyttelse. UiB har også stått i bresjen for å få på plass en mer brukervennlig tofaktor-løsning for FEIDE. Innføring av tofaktor-pålogging for studenter forutsetter endringer i eksamensløsning som må gjøres utenom eksamensperioden og er planlagt tidlig i 2022.

UiB har i 2021 fått gjennomført en ekstern sikkerhetstest og en sikkerhetsskanning. Disse er fulgt opp med tiltak, men bekrefter tidligere funn i internrevisjoner. Det er nødvendig å etablere en bærekraftig struktur rundt drift og forvaltning av forskningssystemer og infrastruktur på institutt og forskningsgrupper. Her er det stordriftsfordeler, og dagens modell blir for fragmentert til å kunne ivareta informasjonssikkerheten på en god nok måte. Sikring av våre IT-systemer til forskning og andre svakt ivaretatte IT-systemer, samt etablere bærekraftige strukturer er hovedmålet i Prosjekt sikre forskningssystemer.

Deteksjon og beredskap

Dette omfatter vår evne til å håndtere avvik, avdekke innbrudd, og sørge for kontinuitet i tilfelle angrep. UiB har her etablerte rutiner for avvikshåndtering, beredskapsplaner og har gjennomført kontinuitetstester. En brann i elektrisitetsforsyningen og IT-avdelingens lokaler i 2018 testet beredskapen kraftig, der UiBs IT-systemer var tilbake i delvis drift 2 timer etter at brannen startet, og tilnærmet full drift etter 4 timer. Et 50-talls læringspunkter ble fulgt opp etter dette, med alt fra kontorforhold, HMS og mer IT-tekniske aspekter.

Innen deteksjon og varsling samarbeider UiB med sektorens overvåkning av forskningsnettet[8] i regi av Uninett AS og med Nasjonal sikkerhetsmyndighet NorCERT. I tillegg er UiB koblet på Varslingssystem for nasjonal digital infrastruktur (VDI) i regi av NSM. Det vurderes også ytterligere tekniske installasjoner på UiB for en kontinuerlig avdekking av sårbarheter samt bedre logging og overvåkning. Innen dette området er det ønskelig med

[8] Forskningsnettet er datanettet som knytter sammen universitet, høyskoler og andre forskningsinstitusjoner i Norge samt knytter dette til tilsvarende i resten av Europa.

oppbemanning, særlig på oppfølging og overvåkning av logging for å avdekke og følge opp unormal trafikk på en bedre måte. Her er det nødvendig å se det som skjer i applikasjoner og systemer i sammenheng med det som skjer i datanettet.

Informasjon og kompetanse

UiB søker å arbeide planmessig med informasjon og kompetanse i henhold til årsplaner i samsvar med styringssystemet. Her er nasjonal sikkerhetsmåned, kurs og møter med institutt og fakultet, oppslag i På Høyden mv viktige ingredienser. I forbindelse med IT-avdelingens «Sikkerhetssprint» i september og oktober 2021 var det blant annet en rekke oppslag i På Høyden og en egen side på UiBs ansattsider.

Det er etablert et nettkurs for ansatte og studenter, integrert opplæring for nyansatte og nye ledere og oppstartskurs for studenter. UiB deltar dessuten aktivt i arbeidet med sektorens fellesløsning sikresiden.no. Det arbeides kontinuerlig på dette området i takt med trusselnivå og generell oppmerksomhet.

Organisering og kapasitet

UiB har per september 2021 to ansatte som arbeider med informasjonssikkerhet på heltid i tillegg til personvernombud. Gjennom omdisponeringer på IT-avdelingen vil øke dette til tre i løpet av høsten 2021.

Tiltak

I tillegg til arbeidet som allerede er iverksatt basert på det økte trusselnivået, er de viktigste tiltakene oppsummert under.

Styring og etterlevelse

A. Det er behov for å styrke UiBs kapasitet innen saksbehandling, rådgivning, oppfølging og rapportering. Dette for å være i stand til å ivareta UiBs forpliktelser. Krav til nytt styringssystem iht sikkerhetsloven og sikkerhetslovens øvrige bestemmelser forsterker dette behovet. Man ser her for seg at dette kan dekkes gjennom omdisponering av stillinger i sentraladministrasjonen.
B. Det er behov for å operasjonalisere UiBs Styringssystem innen informasjonssikkerhet og personvern for å følge opp krav om sikker drift og forvaltning i hele UiBs organisasjon samt krav til systemer som eksponeres på nett. Dette realiseres gjennom årlig egenrapportering iht. styringssystemet, oppfølging i Prosjekt sikre forskningssystemer, samt oppfølging i henhold til UiBs Styringssystemet for informasjonssikkerhet og beredskap.

Operativ sikkerhet og beskyttelse

C. For å bedre informasjonssikkerheten i IT-utstyr og IT-systemer til forskning samt andre systemer og infrastrukturer, skal det gjennomføres et treårig prosjekt *Sikre forskningssystemer.* Prosjektet skal kartlegge, gjennomgå og sørge for sikker drift og forvaltning av IT-systemer og IT-utstyr på institutt, i forskningsgrupper og ellers på universitetet. Målet er å sikre disse og sørge for bærekraftig sikker drift og forvaltning med tilstrekkelig kompetanse og kapasitet. Det er et premiss for arbeidet at alle IT-systemer og IT-utstyr ved UiB skal være sikret i henhold til nasjonale retningslinjer og anbefalinger, og UiBs implementering av disse. God kommunikasjon og involvering av fagmiljøene i eventuell omlegging ansees som en nøkkelfaktor for et vellykket prosjekt. Det avsettes tid og ressurser til dette i prosjektet og i forvaltningsorganisasjonen. Omfanget her er såpass stort at det ikke er løsbart innen

IT-avdelingens eksisterende rammer, og det krever tilførsel av ressurser. Gjennomføring av prosjektet er estimert til 5 FTE i tre år.

D. Det etableres en tjeneste for sentral drift og forvaltning av IT-systemer og IT-utstyr til forskning på IT-avdelingen etter modell fra SAFE, LabIT og NRIS[9]. Tjenesten skal også tilby avansert brukerstøtte[10] samt bygge på helhetlige digitale tjenester med livsløpsperspektiv for forskningsdata med sammenhengende tjenester. Det er et mål at tjenesten skal gi bedre og sikrere IT-tjenester til forskning og en skal derfor legge vekt på brukerorientering i tillegg til sikker drift og forvaltning. Tjenesten bygges opp for å kunne ta imot systemer fra Prosjekt sikre forskningssystemer.

Deteksjon og beredskap

E. Gjennom i første gang omdisponeringer på IT-avdelingen vil kapasiteten innen deteksjon, overvåkning og logging økes. Man ser etter måter å øke kapasiteten ut over dette og det vurderes om UiB kan bidra med utviklingsarbeid for bruk av kunstig intelligens innen dette området forutsatt tilførsel av ressurser.

Informasjon og kompetanse

F. Ut over den økte informasjons og kommunikasjonsaktiviteten gjennom prosjekt sikre forskningssystemer vil det bli vurdert utvikling av flere nettkurs samt krav om en minimumsopplæring for å få brukerkonto på UiB.

Universitetsdirektøren sine kommentarer

Utfordringene knyttet til informasjonssikkerhet er vesentlig økt de siste årene. I eierstyringen med departementet og gjennom ny policy for sektoren samt digitaliseringsrundskrivet er det krav om at styret og ledelsen har oppmerksomhet på området.

Gjennom styringssystemet og den løpende oppfølgingen er det etablert gode strukturer. Det er klart at UiB gjennom en årrekke har hatt en noe liberal praksis med hensyn på lokal drift og forvaltning av IT-tjenester til forskning og andre IT-systemer. Trusselsituasjonen rundt oss og erfaringer fra andre private og offentlige virksomheter indikerer at dette ikke er tilfredsstillende.

Universitetsdirektøren vil arbeide videre med å legge til rette for gode prosesser for oppfølging av de anbefalte tiltakene. I forslag til budsjett for UiB for 2022 er det avsatt 3 mill. kr til Prosjekt sikre forskningssystemer. Tiltakene har en økonomisk ramme på 7 mill kr pr år i tillegg til investeringer som i 2022 antas å kunne dekkes av avsetningen til IT-infrastruktur. Eventuelle organisatoriske endringer som konsekvens av tiltakene vil bli håndtert i henhold til omstillingsavtale og i tett dialog med tillitsvalgte og verneombud.

20.10.2021/Maria Lundhaug/Tore Burheim (avd.dir)

[9] NRIS, Norwegian Research Infrastructure Services (tidligere Metasenteret) er et samarbeid mellom BOTT-universitetene og UNINETT Sigma2 der IT-avdelingen på UiB inngår i en virtuell organisasjon. De leverer avansert brukerstøtte og prosjektstøtte til forskningsprosjekter, tungregning og lagring.

[10] Avansert brukerstøtte er her etter modell fra Sigma2, SAFE og LabIT