Sikt
Kunnskapssektorens tjenesteleverandør

Saksdokument

Digitaliseringsstyret for høyere utdanning og forskning

Til	Digitaliseringsstyret
Dato	14.02.2022
Saksnummer	08/22
Saksarkivnr.	22/00202
Sakstype	V-sak
Saksansvarlig	Tom A. Røtting
Saksbehandler	Bjørn H. Kopperud

Ny fellestjeneste – Cybersikkerhetssenter for forskning og utdanning

Innledning

Nasjonal sikkerhetsmyndighet sier at vi står overfor et taktskifte innenfor digital risiko i Norge som har konsekvenser for vår stats- og samfunnssikkerhet. Antall alvorlige hendelser registrert hos Nasjonalt cybersikkerhetssenter i 2020 var tre ganger så mange som i 2019. Også i det siste året har en vesentlig økning i hendelser knyttet til krypteringsvirus og økonomisk motivert kriminalitet blitt oppdaget.[1] Avanserte aktører utfører komplekse spionasjeoperasjoner mot norske mål, inkludert der våre viktigste verdier forvaltes. Statlig styrt spionasje i det digitale rom representerer en vedvarende og alvorlig trussel, særlig for norske teknologiselskaper og forskningsmiljøer innenfor de sensitive fagområdene[2]. Det er ingen grunn til å tro at dette trusselbildet vil reduseres.

Kunnskap og informasjon som den norske kunnskapssektoren skaper, forvalter og deler, representerer store verdier, både for oss selv og for ulike trusselaktører. Eksempler på dette er store mengder personopplysninger og helsedata, nye banebrytende teknologier, og verdifulle IKT-infrastrukturer[3]. Det er høy risiko for uønskede informasjonssikkerhetshendelser og personvernkrenkelser dersom sektorens digitale verdier utsettes for betydelige trusler. Som sektor må vi sikre effektive tiltak for å redusere sårbarheter[4]. For å videreutvikle et helhetlig og riktig dimensjonert forebyggende sikkerhetsarbeid må vi sammen etablere et økosystem for digital sikkerhet i kunnskapssektoren.
Digital sikkerhet er et strategisk lederansvar som strekker seg ut over virksomhetenes IT-avdeling[5].

---

[1] Nasjonalt digitalt risikobilde 2021 - Nasjonal sikkerhetsmyndighet (nsm.no)

[2] Nasjonal trusselvurdering 2021 (pst.no)

[3] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no

[4] download (unit.no)

[5] Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor - regjeringen.no

Tiltaksområdene favner bredt, og omfatter både menneskelige, tekniske og organisatoriske aktiviteter. Vårt felles mål må være å skape robusthet gjennom forebyggende tiltak og evne til å beskytte, avverge, oppdage og håndtere de hendelser som rammer oss. Samarbeidet vil øke motstandsevnen, på tvers av virksomhetene i vår sektor.

Bakgrunn

I styringsdokumentasjonen for sikkerhetssatsingen (2019-2022), vedtatt i Digitaliseringsstyret 11. april 2019 sak 21/19, leser vi at:

«Deteksjons- og analysekapasitet skal forbedres, og det skal etableres et helhetlig og felles analysesenter for cybersikkerhet i sektoren. Uninett skal ivareta rollen som sektorvist responsmiljø, i tråd med NSMs «Rammeverk for håndtering av IKT-sikkerhetshendelser», og forbedre sektorens evne til å håndtere trusler. Både gjennom bedre tilrettelegging og organisering.» Videre står det at: «*Programmet skal etablere rådgivingstjenester for implementering og helhetlig praktisering av etablerte ledelsessystem for informasjonssikkerhet, samt etablere et program for heving av kompetanse innenfor informasjonssikkerhet og personvern for lederen, forskeren, studenten og øvrige ansatte. «*

Digitaliseringsstyret har drøftet «Cybersikkerhetssenteret for forskning og utdanning» i juni, oktober og desember i 2021. Det er en prinsipiell enighet om at det bør etableres et sektorsamarbeid innen informasjonssikkerhet og personvern for å møte de stadig større utfordringer innen dette området med felles virkemidler. Denne enigheten er i tråd med hver sektor sitt ansvar med å følge nasjonale føringer og rammeverk[6].

Digitaliseringsstyret har også konkludert med at det er nødvendig med en felles plattform og grunntjeneste for analyse og overvåking med mulighet for tilleggstjenester for virksomheter som ønsker og har behov for det. Et stort og kompetent fagmiljø har større forutsetninger for å være attraktivt for eksisterende og nye medarbeidere i et arbeidsmarked som er svært stramt for denne type kompetanse. Dette samlede fagmiljøet bør være en kombinasjon av sentrale ressurser i det sentrale Cybersikkerhetssenteret og de største sikkerhetsmiljøene hos universitetene som samarbeider tett om å finne de beste virkemidlene til å løse felles utfordringer.

I sine behandlinger av saken har Digitaliseringsstyret pekt på flere forhold som må utredes ytterligere før et endelig vedtak om «Cybersikkerhetssenter for forskning og utdanning» som en fellestjeneste i vår sektor kan fattes. Disse forholdene omhandler i hovedsak hvorvidt tjenestene treffer sektorens behov, et ønske om en bedre konkretisering av de ulike tjenestene, revurdere omfanget av obligatoriske vs. frivillige tjenester, finansiering og kostnader. Dette underlaget redegjør for disse forholdene, som ligger til grunn for det foreslåtte vedtaket.

Dette viser oppdatert behovskartlegging

Det ble gjennomført en workshop med BOTT og en ny behovskartlegging i UH-sektoren i november/desember 2021, med mål om å få ytterligere innsikt i behov og ønsker innenfor arbeidet med informasjonssikkerhet og personvern.

Totalt 61 respondenter ble invitert til å svare, i hovedsak fra universiteter og høgskoler som er direkte underlagt KD. Det var i hovedsak IT-direktører, CISO-er og sikkerhets- og beredskapsrådgivere som fikk tilsendt behovskartleggingen, hvor 24 av respondentene leverte svar. Hovedfunnene viser at virksomhetenes behov er ulike, men at mye også er felles. Jevnt over beskriver virksomhetene at de har bedre oversikt og kontroll på tjenester og systemer fra sentral IT-avdeling enn i kjernevirksomheten, og at forskningsområdet er særlig utfordrende. Arbeid med og oppfølging av ledelsessystem, verdioversikt og risikostyring peker seg ut som spesielt krevende å prioritere for

[6] Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren | Unit

mange av respondentene. De peker også på at bredden av arbeidsfeltet både har en tverrfaglighet og en strategisk betydning som strekker seg ut over den tradisjonelle IT-avdelingen. Dette medfører også at finansiering av sikkerhetsarbeidet oppleves som krevende i et allerede presset IT-budsjett. Gjennomgående ønsker alle et faglig felleskap for erfaringsutveksling og læring, og de ønsker støtte i et responsmiljø med kapasitet og evne til å hjelpe. I den videre utarbeidelsen av tjenestene fra Cybersikkerhetssenteret er disse funnene tatt med i betraktningen.

Tjenesterådet for IMDS, Universitetet i Bergen, Universitetet i Oslo, NTNU og Universitetet i Tromsø har gitt tilbakemelding om at den obligatoriske delen av Cybersikkerhetssenteret for forskning og utdanning må reduseres. Som følge av dette er nå leveranser som for eksempel tilgang til trusseldatabaser, sperrelister og fagfellesskap flyttet til den valgfrie delen av tjenesteporteføljen. Det samme gjelder tilgang til rammeavtaler, sikkerhetssertifikater og beste praksis dokumenter mv. Se vedlagte tjenesteoversikt for ytterligere detaljer.

Tjenester

Cybersikkerhetssenteret svarer opp om sektorens ulike behov og oppdraget i sikkerhetssatsingen med en tredeling av hvordan de ulike tjenestene tilbys:

1. Cybersikkerhetssenteret sin obligatoriske fellestjeneste
2. Cybersikkerhetssenteret sin valgfrie fellestjeneste
3. Valgfrie tilleggstjenester

Til grunn for denne inndelingen av tjenestene veier mandatene til Uninett CERT og sektorvist responsmiljø (SRM) tungt.

Obligatorisk fellestjeneste

Cybersikkerhetssenteret er utpekt som SRM av Kunnskapsdepartementet i overenstemmelse med gjeldende rammeverk for håndtering av IKT-sikkerhetshendelser og skal gjennom sitt mandat dekke alle KDs underliggende virksomheter. Tjenesten er utformet for å sikre denne funksjonen, og bidrar også til at øvrige kunder av forskningsnettet får videreført sitt vern gjennom den historiske rollen til Uninett CERT. Kostnadsfordelingen i det større fellesskapet dette medfører, bidrar til at også UH-21 får en lavere relativ enhetskostnad for tjenestene.

Dette miljøet følger opp nettmisbruk, blokkerer uønsket trafikk og distribuerer informasjon om kjente sårbarheter, trusler og trusselaktører basert på et stort nasjonalt og internasjonalt tillitsnettverk som virksomhetene selv blir en del av. I tillegg får alle ukentlige rapporter fra en kontinuerlig sårbarhetsscan. Virksomheter som blir utsatt for særlig alvorlige sikkerhendelser eller cyberangrep får ubegrenset bistand når disse pågår (avhengig av tilgjengelig kapasitet).

De obligatoriske tjenestene har en kostnad på 10 millioner for UH21, men den reelle kostnadsøkningen vil være 6,4 millioner kroner da dagens tilknytningsavgifter for forskningsnettet reduseres med 3,6 millioner kroner. Øvrige kunder tilknyttet forskningsnettet betaler for den delen av tjenesteporteføljen de benytter. Se vedlagte finansieringsmodell for ytterligere detaljer.

Valgfri fellestjeneste

Denne gir blant annet tilgang til fagfellesskap for erfaringsutveksling og kompetanseutveksling, prosessverktøy, maler for myndighetspålagte planer og rammeverk og til enhver tid oppdaterte sperrelister. Et ubegrenset antall sertifikater, dreiebok for øvelser og sentral lagring av logger som bidrar til forbedret trusseletterretning er også en del av denne pakken. Institusjoner som abonnerer på denne fellestjenesten får i tillegg 50 GB sentral lagring av loggdata uten begrensning på lagringstid, samt sensorer utplassert på sin nettilknytning for å avdekke trusler. Sentrale logger og sensorene er to viktige forutsetninger for at Cybersikkerhetssenteret kan avdekke uønsket aktivitet hos virksomheten.

Det er nødvendig å samle leveransene i en valgfri fellestjeneste som en pakke fordi en fragmentering av tjenestetilbudet og tilhørende finansiering medfører at kunnskapssektoren samlet får redusert beredskap og lavere kapasitet til å møte et stadig mer avansert trusselbilde. Forutsigbare økonomiske rammer er en forutsetning for et godt totalforsvar også i kunnskapssektoren.

Digitaliseringsstyret har etterspurt er mer detaljert oversikt over de konkrete tjenestene fra Cybersikkerhetssenteret for forskning og utdanning. Denne oversikten er nå utarbeidet og ligger vedlagt. I vedlegget fremkommer det at de *tekniske tjenestene* i de ulike delene er gjennomgående sortert i henhold til kategoriene i NSMs grunnprinsipper for IKT-sikkerhet[7] (Beskytte og opprettholde, Oppdage, Håndtere og gjenopprette). Nasjonalt cybersikkerhetssenter (NCSC-NSM) erfarer fortsatt at alle digitale hendelser kunne vært unngått eller skaden begrenset dersom virksomheter i større grad hadde implementert «NSM Grunnprinsipper for IKT-sikkerhet»[8]. Ved å følge dette rammeverket sikrer vi mulighet for god systematikk i virksomhetenes bruk og nytteverdi av våre tjenester, og en felles og sektortilpasset tilnærming.

Tjenester under rådgivning og kompetanseheving bidrar til virksomhetens arbeid med de *organisatoriske og menneskelige tiltaksområdene*. Dette omfatter mer prosessuelle aktiviteter, og møter de uttalte ulikheter i behov og prioriterte områder.

Den valgfrie fellestjenesten inneholder deler av dagens tjenestetilbud («Sikkerhetsanalyse», «DNS Brannmur» og «Sikkerhetssertifikater») som UH21 til sammen betalte 1,7 millioner kroner for også i 2021.

I vedlagte finansieringsmodell er det i budsjettet laget en prognose på at 17 av 21 virksomheter velger å ta i bruk den valgfrie fellestjenesten over en treårsperiode.

Valgfrie tilleggstjenester

Den siste kategorien består av tjenester som tilbys til alle virksomheter i norsk kunnskapssektor etter behov, og vil være basert på etterspørsel og tilgjengelig kapasitet i Cybersikkerhetssenteret. Alle i UH-sektoren har samme kjernevirksomhet, lovverk og felles krav fra KD, men prioriteringene hos den enkelte vil variere. Skreddersøm av tjenester rettet mot den enkelte virksomhet som Digitaliseringsstyret tidligere har etterspurt faller også inn under denne kategorien.

Tilleggstjenester faktureres etter forbruk fra den enkelte institusjon som bestiller tjenester.

Finansiering

En gjennomgående tilbakemelding fra Cybersikkerhetssenterets kunder og samarbeidspartnere er at IT-budsjettene på virksomhetene ikke strekker til når de både skal dekke nasjonale fellestjenester og lokal kapasitet innenfor informasjonssikkerhet og personvern.

I vedlagte forslag til finansiering av Cybersikkerhetssenter for forskning og utdanning er UH21 sin kostnad vesentlig redusert siden saken sist var til Digitaliseringsstyrets behandling. Den obligatoriske tjenesten vil innebære en netto kostnadsøkning på 6,4 mill. kroner i 2022, fordelt på UH21 som detaljert i vedlegget.

[7] nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

[8] Nasjonalt digitalt risikobilde 2021 - Nasjonal sikkerhetsmyndighet (nsm.no)

Forslag til vedtak

Digitaliseringsstyret vedtar at Cybersikkerhetssenter for forskning og utdanning etableres som en fellestjeneste i kunnskapssektoren, i tråd med beskrevne inndeling i obligatoriske og frivillige tjenester. Tjenestene forvaltes og videreutvikles av Sikt fra 2022, i tråd med sektorens samstyringsmodell.

Det skal jobbes videre med å etablere gode samarbeidsmodeller og god arbeidsfordeling mellom Cybersikkerhetssenteret og de lokale informasjonssikkerhetsmiljøene.

Vedlegg

- Vedlegg 08A: Tjenesteoversikt, Cybersikkerhetssenter for forskning og utdanning
- Vedlegg 08B: Finansieringsforslag, Cybersikkerhetssenter for forskning og utdanning