# Vedlegg 1. Satsingsforslag for økt cybersikkerhet i kunnskapssektoren for 2026

## Innledning

*Sikt – Kunnskapssektorens tjenesteleverandør* er av Kunnskapsdepartementet (KD), gitt oppgaven som sektorvist responsmiljø (SRM). Sikt trenger tilstrekkelig, stabil og vedvarende finansiering for å kunne ivareta sine forpliktelser i denne rollen.

Nasjonal digitaliseringsstrategi 2024–2030 [1]trekker fram at dagens sikkerhetssituasjon er alvorlig, uforutsigbar og i stadig endring. Den peker på behovet for at «arbeidet med forbyggende sikkerhet samordnes, styrkes og forenkles» (pp. 38). Sikt sitt arbeid som SRM er et viktig bidrag i dette arbeidet. Strategien vektlegger også at dersom «vi skal nå målene med digitalisering, er vi avhengige av sterke og gode kunnskapsmiljøer innenfor IKT og av forskning og utvikling på områder som er viktige for Norge» (pp. 50). Med andre ord er kunnskapssektoren i seg selv en forutsetning for å oppnå nasjonale mål.

Sikt har hatt gode diskusjoner med Kunnskapsdepartementet rundt foreslåtte tiltakspakker gjennom 2024 og opplever stor forståelse både for behovet og at innretningen på de foreslåtte tiltakene vil møte behovet som Riksrevisjonen peker på og som også forsterkes gjennom Nasjonal digitaliseringsstrategi 2024-2030

## Hva er problemet, og hva vil vi oppnå?

Riksrevisjonen konkluderer i sine undersøkelser (Dokument 3:11 (2023–2024)[2]) med at forskningsdata «ikke er tilstrekkelig sikret mot dataangrep» (pp.10). Ikke minst sliter mange av virksomhetene med å gjennomføre tekniske tiltak, og har varierende eller dårlig evne til å oppdage angrep. Riksrevisjonen slår fast at cybersikkerhetssenteret til Sikt (eduCSC) «[ikke greier] å treffe behovene til virksomhetene» (pp. 19). Det trekkes fram at tjenestene i hovedsak brukerfinansieres, og Riksrevisjonen vurderer at tilbudet «i dag i for stor grad preges av den enkelte virksomhets etterspørsel og betalingsvilje, og i for liten grad av behovene til sektoren som helhet». Samtidig påpeker Riksrevisjonen at «Kunnskapsdepartementet får lite informasjon om den reelle sikkerhetstilstanden i sektoren» (pp. 8).

For å møte disse behovene og stå bedre rustet til å støtte kunnskapssektoren i utrygge tider foreslår vi derfor 3 tiltak. Tiltakene vil som helhet gi vesentlig økt evne til forebygging og deteksjon av cyberangrep, samt bedre samhandling i sektoren.

[1] Regjeringen. Fremtidens digitale Norge. Nasjonal digitaliseringsstrategi 2024–2030.
[2] Riksrevisjonen. Dokument 3:11 (2023-2024) Informasjonssikkerhet i forskning innenfor kunnskapssektoren

## Hvilke tiltak er relevante?

For å økt kapabilitet til overvåkning, analyse og respons foreslås det tre tiltak:

1. Etablere et Mini-sikkerhetsoperasjonssenter (Mini-SOC) som følger med på trusler mot sektoren, leter etter spor hos virksomhetene gjennom deres logger og koordinerer med lokale sikkerhetsteam for å gjennomføre eventuelle tiltak.
2. Etablere vern i forskningsnettet mot tjenestenekt-angrep
3. Planlegge og gjennomføre faste sektorøvelser for cybersikkerhet

### Mini-sikkerhetsoperasjonssenter (Mini-SOC)

En full SOC vil være omfattende og kostbar. Det foreslås derfor å avgrense arbeidet til logger som Sikt allerede besitter som forskningsnett og leverandør, samt sikkerhetslogger knyttet til klienter (datamaskiner) og e-postsystemer basert på løsninger fra Microsoft. Cybersikkerhetssenteret erfarer at det er her mange hendelser begynner og kan oppdages, eventuelt forebygges. Microsoft tilbyr i dag en løsning som lar dette bli realisert på sektornivå for deres tjenester.

Etablering skjer innledningsvis gjennom oppsett i samråd med Microsoft og deres partnere, samt kunder som ønsker å ta det i bruk. Cybersikkerhetssenteret må bygge kompetanse på løsningen hos sine medarbeidere, samt utvikle eventuelle integrasjoner mot interne løsninger som brukes i dag. Utover dette må rutiner utvikles i samråd med SRM, og ev. personvernskonsekvenser utredes (DPIA).

Enkelte loggkilder med høyt volum kan bli meget kostbare å lagre i en slik løsning. Det vil derfor parallelt bli jobbet med en alternativ løsning for rimelig og effektiv prosessering av store loggmengder. Sikt har tidligere erfaringer med lignende arbeid knyttet til såkalt historisk DNS. Det vil være naturlig å se dette opp mot annen data som Sikt besitter, for eksempel trafikk-metadata i forskningsnettet («flow»), samt eksisterende tekniske løsninger i sektoren som kan benyttes, der både NTNU og UiO har interessante løsninger.

Det vil være kostbart å etablere en full SOC som opererer døgnet rundt (24/7). Vi ønsker derfor ikke dette i første omgang. Etableringen av felles rutiner og innsamling hos vår Mini-SOC vil likevel gjøre det enklere å ta i bruk private leverandører som tilbyr slike tjenester, om sektoren er villige til å betale kostnadene. Den samme vurderingen gjelder for bruk av ekspertise fra private leverandører ved alvorlige IKT-hendelser.

### Etablere vern i forskningsnettet mot tjenestenekt-angrep

Det er blitt mer utfordrende å levere nett. Nasjonal kommunikasjonsmyndighet trekker fram en «betydelig endring i risiko- og trusselbildet for ekomtilbydere og datasenteroperatører de siste årene på grunn av den sikkerhetspolitiske situasjonen» (Risiko- og sårbarhetsanalyse for ekomsektoren (2024)[3], s. 2). Cyberangrep nevnes som en av de største utfordringene, forsterket av nye teknologier som KI og tjenester som blant annet tilbyr tjenestenektangrep (DDoS) mot betaling. Cybersikkerhetssenteret erfarer at DDoS er en vesentlig utfordring hos andre

[3] Nasjonal kommunikasjonsmyndighet. Risiko- og sårbarhetsanalyse for ekomsektoren (2024).

europeiske forskningsnett og at det brukes betydelige krefter på å etablere nye løsninger i form av vern.

Et DDoS-vern bruker en blanding av statistikk og/eller KI-baserte løsninger for å automatisk kunne utelukke uønsket trafikk fra nettet. Dette effektiviserer arbeidet betraktelig, men medfører også risiko for feil. Det er derfor nødvendig å evaluere eventuell løsning godt, iverksette tiltak som reduserer risiko og ikke minst hindrer uønskede konsekvenser for brukerne av forskningsnettet.

Det er nødvendig å vurdere ny teknologi og eventuelt leverandører hvor dette fører til at tjenestene realiseres fortere. Dette skjer i samarbeid mellom Cybersikkerhetssenteret og Forskningsnettet i Sikt. Det er naturlig å utforske muligheter for å realisere deler av DDoS-vernet via NORDUNET, samarbeidet mellom de nordiske forskningsnettene. Dette kan bidra til å redusere kostnader, øke kvaliteten og styrke det internasjonale samarbeidet Sikt er en del av. Totalberedskapskommisjonen trekker i NOU 2023: 17 [4] fram muligheten for «økt digital redundans og økt teknologi- og sikkerhetskompetanse på tvers av landene i Norden» (s. 314).

## Planlegging og gjennomføring av sektorøvelser med jevne mellomrom

Digitaliseringsstrategien forutsetter at Norge styrker «sikkerheten, beredskapen og kriminalitetsbekjempelsen» (pp. 6) fram mot 2030. God samhandling og kompetanse trekkes også fram som en viktig del av dette arbeidet. Regjeringen vektlegger i sin digitale sikkerhetsstrategi (Meld. St. 9 (2022-2023)) effekten av øvelser for bedre samhandling og kunnskapsdeling. Cybersikkerhetssenteret til Sikt har deltatt i slike tverrsektorielle og sivil-militære øvelser som del av det norske totalforsvaret, og opplever dette som svært nyttig for økt kunnskapsdeling og samhandling.

Digitaliseringsstrategien nevner sammenhengen mellom å «øke virksomheters digitale egenberedskap og gjennom dette Norges samlede digitale motstandskraft» (pp. 39). Riksrevisjonens undersøkelser i sektoren (Dokument 3:11 (2023-2024)) peker på at «uklare ansvarsforhold har flere steder hemmet framdriften i arbeidet» (pp. 76). De påpeker overordnet at virksomhetene «har utfordringer med å sikre at tiltak gjennomføres konsekvent i hele virksomheten» (pp. 12). Øvelser bidrar til å avkle slike samhandlingsutfordringer, slik at de kan utbedres.

Det har derfor vært ønskelig å øve mer også i norsk kunnskapssektor. I år måtte Sikt kansellere sektorøvelsen Morris grunnet manglende finansiering og påmelding fra institusjonene. Dette belyser en vesentlig utfordring med å ivareta et slikt sektorbehov utelukkende gjennom brukerfinansiering, jf. merknadene til Riksrevisjonen i Dokument 3:11 (2023-2024) og vår innledning her. En annen utfordring er at øvelser tar lang tid å planlegge og legger beslag på viktig personell, som er problematisk når det er usikkert om øvelsen faktisk blir gjennomført.

Vi anbefaler en større øvelse annet hvert år og en mindre øvelse i mellomliggende år.

## Finansiering

For å kunne styrke Sikt sin evne til overvåkning, analyse og respons er det behov for en stabil årlig finansiering av etablering, videreutvikling og drift av de foreslåtte tiltakene. Grunnen til at årlige beløp er å foretrekke foran en stor engangsfinansiering er følgende:

[4] NOU 2023: 17 Nå er det alvor – Rustet for en usikker fremtid

1. **Løpende behov:** Cybersikkerhet er ikke en engangsinvestering, men et kontinuerlig behov. Trusselbildet endrer seg stadig, og det er nødvendig med løpende overvåkning, oppdateringer og forbedringer for å holde tritt.
2. **Læring underveis:** Når man utvikler og implementerer cybersikkerhetstiltak, er det viktig å kunne lære underveis. En jevn årlig finansiering gjør det mulig å justere kursen basert på hva man lærer, og sørger for at man kan prioritere de mest presserende behovene.
3. **Bærekraftig utvikling:** En modell med jevn årlig finansiering fremmer en mer bærekraftig og langsiktig tilnærming til cybersikkerhet. Den gir organisasjonen mulighet til å planlegge og utvikle tiltakene over tid, i stedet for å måtte bruke alle ressursene på en gang.
4. **Finansiell stabilitet:** Jevn årlig finansiering gir finansiell stabilitet. Det gir sikkerhet for at det vil være tilstrekkelige ressurser tilgjengelig for å håndtere fremtidige cybersikkerhetstrusler.
5. **Innovasjon og fleksibilitet:** En modell med jevn årlig finansiering støtter en innovativ og fleksibel tilnærming til cybersikkerhet. Den gir organisasjonen frihet til å prøve nye løsninger og tilnærminger, og til å tilpasse seg endringer i teknologi og trusselbilde.

Mens prosjekttankegangen kan være effektiv for engangsinvesteringer eller kortvarige initiativer, er cybersikkerhet en kontinuerlig prosess, hvor sikkerheten totalt sett avhenger av sikkerheten lokalt, med et trusselbilde og teknologi i rask endring, og som dermed krever en annen tilnærming.

Tiltakene retter seg mot operasjonell sikkerhet og er egnet til satsningsfinansiering, med langsiktige muligheter for en økt andel brukerfinansiering. Tiltakene vil kreve investeringer de to første årene, og det er deretter foreslått en årlig finansiering til drift og kontinuerlig videreutvikling.

Satsningen har behov for følgende årlige økning (i tillegg til allerede eksisterende finansiering av SRM-rollen) av finansiering til drift, etablering og videreutvikling:

Tabell 1: Finansiering av etablering, drift og kontinuerlig videreutvikling.

| Tiltakspakke | År 1 | År 2 | År 3 | År 4 | År 5 |
|---|---|---|---|---|---|
| MiniSOC, DDos-vern og sektorøvelse | 10 MNOK | 10 MNOK | 7,5 MNOK | 7,5 MNOK | 7,5 MNOK |

## Hvilke prinsipielle spørsmål reiser tiltakene?

Personvern og datainnsamling: Ved etablering av et Mini-SOC vil det være nødvendig å samle inn og analysere logger fra ulike kilder. Dette vil innebære en viss risiko for personvern, da disse loggene kan inneholde sensitiv informasjon. Det er derfor viktig å følge strenge retningslinjer for personvern ved innsamling og analyse av logger. Dette kan inkludere å anonymisere data der det er mulig, og å sikre at dataene lagres på en sikker og regulert måte. Alle datainnsamlingsaktiviteter må være i samsvar med gjeldende lover og forskrifter, som GDPR. En personvernkonsekvensvurdering (DPIA) bør utføres før implementering for å identifisere og minimere eventuelle personvernsrisikoer.

Samarbeid og koordinering: Tiltakene vil kreve tett samarbeid mellom ulike aktører, både innenfor og utenfor sektoren. Det vil være nødvendig med en klar struktur for samarbeid og

koordinering, spesielt i tilfelle det vil bli avtaler med andre leverandører med noen av tjenestene. Videre er det allerede etablert samarbeid med andre aktører både nasjonalt og internasjonalt, der Cybersikkerhetssenteret i dag inngår i et internasjonalt nettverk av responsmiljøer, men med særlig fokus på koordinering nasjonalt med andre sektorvise og offentlige instanser.

Teknologisk utvikling og implementering: Implementering av DDoS-vern og innsamling og analyse av logger vil kreve bruk av avansert teknologi. Hvordan vil denne teknologien bli implementert, og hvem vil ha ansvar for å vedlikeholde og oppdatere den? Teknologisk utvikling og implementering: Implementering av teknologi bør være basert på forskning og testing, og bør være i samsvar med de beste praksisene innen cybersikkerhet. Vedlikehold og oppdatering av teknologien vil være et løpende ansvar som bør tildeles til et dedikert team eller enkeltpersoner med relevant kompetanse.

Kompetansebygging: Tiltakene vil kreve høy kompetanse innenfor cybersikkerhet. Hvordan kan man bygge og vedlikeholde kompetansen som behøves? Cybersikkerhetssenteret har et veletablert og sertifisert CERT (Cyber Emergency Response Team) som har vært virksomt i 30 år, og kompetanse og rutiner for håndtering av cybersikkerhetshendelser er veletablert og fungerende. En mini-SOC vil i slik måte fungere som en utvidelse av dette, og man vil benytte samme rutiner for kompetansebygging som i dag. Sikt er dessuten godt forankret i kunnskapssektoren, og er en attraktiv arbeidsplass for nyutdannede arbeidssøkere.

Risikohåndtering: Hva skjer hvis noe går galt? Hvilke beredskapsplaner vil være på plass for å håndtere potensielle sikkerhetsbrudd? Det bør være beredskapsplaner på plass for å håndtere potensielle sikkerhetsbrudd. Dette kan inkludere en krisehåndteringsplan, et dedikert respons-team, og jevnlige øvelser for å teste og forbedre responsprosedyrene.

Ansvar og eierskap: Hvem vil eie tiltakene, og hvem vil være ansvarlige for å sikre at de fungerer som de skal og gir de ønskede resultatene? Det er Cybersikkerhetssenteret i Sikt som vil ha ansvaret for at tiltakene gir de ønskede resultatene.

## Hva er de positive og negative virkningene av tiltaket, hvor varige er det, og hvem blir berørt?

### Positive ringvirkninger

*Bedre etterretning og styring*. Tiltaket vil gi økt synlighet og dermed bedre evne til å «følge med». Cybersikkerhetssenteret har i år begynt å levere teknisk-operative tilstandsrapporter. Mer detaljert informasjon om hendelser forsterker datagrunnlaget disse bygger på og øker dermed tilliten til eventuelle funn. Dette kan også øke kvaliteten på styringen av sektoren, for eksempel gjennom HK-dir og deres tilstandsvurderinger, da dataen gir et mer objektivt og målbart bilde av sikkerhetstilstanden.

*Billigere, bedre og sammen*. Å oppdage angrep krever spesialistkompetanse, som kan være utfordrende å bygge opp hos den enkelte virksomhet. Da er det mye bedre at denne ressursen kommer hele sektoren til gode. Samtidig vil angrep mot en institusjon kunne brukes til å forebygge tilsvarende hendelser hos *alle* virksomheter. Det er rimelig å anta at en mer målrettet tjeneste som dette også vil være rimeligere og bedre tilpasset sektorens kostnadsforventninger enn typiske private leverandører.

*Økt innovasjon, nye tjenester og KI*. Mer data og innsikt åpner for at Cybersikkerhetssenteret kan utvikle nye, innovative tjenester. Slik data er også muliggjørende for framtidige satsninger på KI,

og sikkerhetsløsning'en i Mini-SOC har også elementer av KI som del av sin funksjonalitet. Dette vil støtte opp om den nasjonale digitaliseringsstrategiens mål (4.2) om at norsk offentlig sektor skal være ledende på å ta i bruk KI for mer effektive og bedre tjenester.

*Et mer robust forskningsnett*. Digitaliseringsstrategien krever at «den digitale grunnmuren må bli mer robust, og redundansen og diversiteten må videreutvikles og styrkes» (pp. 20). Forskningsnettet er en viktig del av denne grunnmuren i norsk kunnskapssektor. Tjenestenektangrep forstyrrer tilgjengeligheten til tjenester. Dette er uakseptabelt om man skal nå målene om en mer digitalisert sektor. Bedre og enklere tilgang til trafikk-metadata fører også til kjappere deteksjon av trusler, enklere feilsøking ved driftsfeil og gir et godt grunnlag for å planlegge framtidig kapasitet.

*Økt evne til å oppdage og stå imot angrep*. Cybersikkerhetssenteret regner med at flere angrep i dag ikke oppdages fordi nye analyseteknikker på metadata ikke tas i bruk. Digitaliseringsstrategien trekker fram at Norge må «sørge for å ha tilstrekkelig kapasitet til å håndtere digitale angrep, som det blir stadig flere av» (pp 38). Dette understrekes av det alvorlige trusselbildet som Nasjonal kommunikasjon tegner, jf. innledningen.

*Sterkere samhandling og økt beredskapsevne*. Vi viser her til vurderingene i innledningen til dette punktet. Det er åpenbart et behov for sterkere samhandling internt i virksomhetene, og den nasjonale strategien peker helt klart mot betydningen av overordnet samhandling. Mini-SOC åpner for å dra i bruk løsninger og kompetanse som allerede finnes i sektoren, som øker gevinstrealiseringen av disse.

*Kompetanseheving*. Øvelser er en anledning til å bli kjent med den fulle bredden av nødvendige ferdigheter som må til for å håndtere sikkerhetsbrudd og kriser.

## Mulige negative virkninger

Her er noen mulige negative virkninger av de foreslåtte tiltakene:

*Personvern:* Samling og analyse av logger kan innebære risiko for personvern, da disse loggene kan inneholde sensitiv informasjon. Dette kan potensielt føre til personvernbrudd hvis dataene ikke håndteres på en sikker og ansvarlig måte.

*Falske positiver:* Automatiserte sikkerhetssystemer, som DDoS-vern, kan noen ganger generere falske positiver - det vil si, de kan identifisere legitim trafikk som en trussel. Dette kan forstyrre normale operasjoner og potensielt føre til unødvendige kostnader.

*Teknologiske utfordringer:* Implementering av nye teknologier kan medføre tekniske utfordringer. For eksempel kan det være vanskelig å integrere nye systemer med eksisterende infrastruktur, og det kan være utfordrende å holde tritt med raskt skiftende teknologitrender.

*Avhengighet av eksterne leverandører:* Tiltakene involverer samarbeid med eksterne leverandører, som Microsoft. Dette kan potensielt føre til avhengighet av disse leverandørene, noe som kan være problematisk hvis leverandøren endrer sine tjenester, øker prisene, eller opplever egne sikkerhetsproblemer.

*Ressursfordeling:* Tiltakene kan kreve betydelig tid og oppmerksomhet fra organisasjonens personell. Dette kan potensielt føre til at andre viktige oppgaver og prosjekter blir nedprioritert.

## Utvikle og benytte kompetanse i samfunnet

De foreslåtte tiltakene kan utvikle og benytte kompetanse i samfunnet på flere måter:

1. **Kompetansebygging:** Gjennom å etablere et sikkerhetsoperasjonssenter og implementere tiltak som vern mot DDoS-angrep, vil det være nødvendig å bygge opp kompetanse innenfor cybersikkerhet. Dette kan omfatte alt fra tekniske ferdigheter, som programmering og dataanalyse, til forståelse av cybersikkerhetstrusler og risikostyring.
2. **Utdanning og opplæring:** Planlegging og gjennomføring av sektorøvelser kan bidra til å utdanne og trene personell i ulike aspekter av cybersikkerhet. Dette kan bidra til å øke den generelle kompetansen i samfunnet.
3. **Samarbeid med utdanningsinstitusjoner:** Tiltakene kan også involvere samarbeid med utdanningsinstitusjoner, for eksempel gjennom forskning eller ved å tilby praksisplasser for studenter. Dette kan bidra til å utvikle kompetansen til fremtidige arbeidstakere.
4. **Deling av kunnskap:** Ved å dele kunnskap og erfaringer fra tiltakene, for eksempel gjennom rapporter, konferanser eller seminarer, kan sektoren bidra til å øke forståelsen for cybersikkerhet på tvers av virksomhetene i sektoren og i samfunnet som helhet.
5. **Bruk av eksisterende kompetanse:** Tiltakene kan også bidra til å mobilisere og utnytte eksisterende kompetanse i samfunnet. Dette kan være gjennom å rekruttere eksperter fra ulike felt, eller ved å samarbeide med andre organisasjoner eller sektorer som har relevant kompetanse.
6. **Stimulere til innovasjon:** Tiltakene kan stimulere til innovasjon innen cybersikkerhet, for eksempel gjennom utvikling av nye teknologier eller metoder for å håndtere cybersikkerhetstrusler. Dette kan bidra til å utvikle kompetansen innen dette feltet ytterligere.

## Automatisering og tjenestekjeder

### *Automatisering*

I vår stadig mer digitaliserte verden blir automatisering stadig viktigere. Automatisering innebærer bruk av teknologi for å utføre oppgaver som tidligere krevde menneskelig inngripen. Dette kan øke effektiviteten, redusere feil og frigjøre menneskelige ressurser til mer komplekse oppgaver. Innen cybersikkerhet kan automatisering bidra til raskere og mer pålitelig identifikasjon og respons på sikkerhetstrusler. Vi vil peke på noen områder der automatisering blir viktige:

1. **Effektivitet:** Ved å automatisere prosesser i sikkerhetssenteret (Mini-SOC) og DDoS-vern kan man raskt identifisere og respondere på trusler, noe som øker effektiviteten og reduserer potensiell skade.

2. **Konsekvens:** Automatisering bidrar til konsekvent overvåkning og respons. Den menneskelige faktoren, som kan føre til inkonsekvens og feil, reduseres.

3. **Skalerbarhet:** Automatiserte systemer kan enklere skaleres for å møte endringer i volumet av data eller trussellandskapet, noe som er spesielt relevant gitt den dynamiske naturen av cybersikkerhet.

4. **Tidsbesparelse:** Automatiserte prosesser kan spare tid for IT-teamene, slik at de kan fokusere på mer komplekse oppgaver som krever menneskelig inngrep.

*Tjenestekjeder*

En tjenestekjede refererer til sekvensen av aktiviteter som en tjeneste gjennomgår fra start til slutt. Dette inkluderer alle de forskjellige leddene som er involvert i å levere tjenesten, fra utvikling og produksjon, til levering og vedlikehold. I konteksten av cybersikkerhet kan en tjenestekjede inkludere aktiviteter som trusselovervåkning, risikovurdering, implementering av sikkerhetstiltak, respons på sikkerhetshendelser, og gjenoppretting etter et angrep. Ved å koordinere disse aktivitetene i en sammenhengende tjenestekjede, kan organisasjoner sikre en mer effektiv og helhetlig tilnærming til cybersikkerhet. Når det gjelder tiltakspakken med de tre tiltakenes om foreslås så vil følgende elementer være aktuelle:

1. **Integrert tilnærming:** De tre tiltakene henger sammen i en tjenestekjede som gir en helhetlig tilnærming til cybersikkerhet, som beskytter nettet (DDoS-vern), utvider dette vernet ut til sluttbruker (Mini-SOC) og forbereder sektoren gjennom øvelser på å stå imot et stadig mer alvorlig trusselbilde (sektorøvelser).
2. **Samordning:** En godt koordinert tjenestekjede sikrer at informasjon og innsikt deles effektivt mellom de forskjellige leddene, noe som forbedrer den generelle responsen på trusler.
3. **Kontinuitet:** Ved å se på disse tiltakene som en tjenestekjede, oppnås kontinuitet i sikkerhetsarbeidet. Dette sikrer at det er en enhetlig tilnærming til cybersikkerhet gjennom hele organisasjonen.
4. **Ansvarlighet:** En klar tjenestekjede definerer også ansvar og roller. Dette sikrer at alle aktører vet hva deres oppgaver er og bidrar til en mer effektiv håndtering av sikkerhetsspørsmål.

## Internasjonalisering

De foreslåtte tiltakene kan fremme internasjonalisering på flere måter:

*Samarbeid med internasjonale aktører:*

Ved å etablere et sikkerhetsoperasjonssenter i samarbeid med Microsoft og andre internasjonale partnere, vil det være muligheter for internasjonalt samarbeid og kunnskapsdeling. Vi er allerede i gang med å bygge nettverk ved at vi er representert i internasjonale fora og blir invitert inn på mange arena også utenfor kunnskapssektoren, for å holde innlegg.

*Felles standarder og praksis:*

Tiltakene kan bidra til å fremme bruk av internasjonale standarder og beste praksis innen cybersikkerhet. Dette kan styrke sektorens internasjonale konkurransekraft og bidra til å bygge tillit hos internasjonale partnere.

*Internasjonalt nettverk:*

Gjennom planlegging og gjennomføring av sektorøvelser, kan det være muligheter for å bygge et internasjonalt nettverk av aktører innen cybersikkerhet. Dette kan gi muligheter for internasjonalt samarbeid og kunnskapsdeling.

*Internasjonal eksponering:*
Ved å implementere avanserte tiltak som DDoS-vern, kan sektoren få internasjonal eksponering og anerkjennelse. Dette kan bidra til å tiltrekke seg internasjonale partnere og talenter.

*Samarbeid med NORDUNET:*
Det er foreslått å utforske muligheter for å realisere deler av DDoS-vernet via NORDUNET, samarbeidet mellom de nordiske forskningsnettene. Dette kan bidra til å styrke det internasjonale samarbeidet og bygge sterkere bånd med andre land.

Gjennom disse tiltakene kan sektoren bli mer globalt orientert, noe som kan bidra til å styrke dens evne til å håndtere internasjonale cybersikkerhetstrusler og fremme internasjonale samarbeid og partnerskap.

## Økonomiske gevinster

*Kvantitative gevinster*
For å kvantifisere gevinster av disse tiltakene, er det nødvendig å vurdere potensielle kostnader forbundet med cyberangrep. Dette kan inkludere direkte kostnader som gjenoppretting etter et angrep, tap av produktivitet, og indirekte kostnader som omdømmeskade.

1. **Kostnader for gjenoppretting:** Ifølge en rapport fra IBM i 2020 (Cost of A Data Breach), er den gjennomsnittlige totale kostnaden for et datainnbrudd globalt $3,86 millioner. Dette inkluderer kostnader for å identifisere og stenge bruddet, gjenopprette tapte data, og implementere nye sikkerhetstiltak for å forhindre fremtidige brudd.
2. **Tap av produktivitet:** Når et cyberangrep oppstår, vil det ofte være en nedetid hvor systemer er utilgjengelige. Dette kan føre til betydelige tap av produktivitet. For eksempel, hvis et universitet med 10 000 ansatte har en nedetid på en dag på grunn av et cyberangrep, og den gjennomsnittlige dagslønnen er 4000 kr, vil det totale produktivitetstapet være 40 millioner kr.
3. **Omdømmeskade:** Et cyberangrep kan føre til betydelig omdømmeskade, noe som kan påvirke en institusjons evne til å tiltrekke seg studenter, ansatte og forskningsfinansiering. Selv om det er vanskelig å kvantifisere denne kostnaden, kan den være betydelig.

Hvis vi antar at disse tiltakene kan redusere sannsynligheten for et cyberangrep med 50%, og at den gjennomsnittlige kostnaden for et cyberangrep er lik den globale gjennomsnittskostnaden, ville gevinsten være betydelig. I denne sammenhengen vil det være viktig å vurdere kostnadene ved å implementere tiltakene mot potensielle besparelser fra reduksjonen i cyberangrep.

## Hvilke tiltak anbefales, og hvorfor?

Alle de tre foreslåtte tiltakene - etablering av et sikkerhetsoperasjonssenter (Mini-SOC), vern mot tjenestenekt-angrep (DDoS), og planlegging og gjennomføring av sektorøvelser - spiller en integrert rolle i å styrke cybersikkerheten innenfor norsk kunnskapssektor. Her er hvordan de henger sammen og hvorfor de er viktige:

1. Mini-sikkerhetsoperasjonssenter (**Mini-SOC):** Dette tiltaket vil fungere som sektorens førstelinjeforsvar mot cybertrusler. Ved å overvåke og analysere logger, kan sikkerhetsoperasjonssenteret raskt identifisere potensielle trusler eller angrep, og koordinere med lokale sikkerhetsteam for å sette i verk nødvendige tiltak. I tillegg vil samarbeidet med Microsoft og deres partnere sikre tilgang til de nyeste sikkerhetsløsningene.
2. **Vern mot tjenestenekt-angrep (DDoS):** Dette tiltaket vil gi et ekstra lag med beskyttelse ved å forhindre at tjenestene blir utilgjengelige på grunn av overbelastningsangrep. Dette er spesielt viktig gitt den økende trusselen fra DDoS-angrep. Implementeringen av DDoS-vern vil også kreve samarbeid og koordinering med sikkerhetsoperasjonssenteret (Mini-SOC) for å sikre at alle trusler blir identifisert og håndtert på en effektiv måte.
3. **Planlegging og gjennomføring av sektorøvelser:** Dette tiltaket vil bidra til å styrke den samlede beredskapen og resiliensen i sektoren. Gjennom regelmessige øvelser kan aktørene i sektoren teste og forbedre sine responsprosedyrer, identifisere potensielle svakheter, og lære fra hverandre. Dette vil også bidra til å sikre at både Mini-SOC og DDoS-vernet fungerer som de skal under et faktisk angrep.

Sammen skaper disse tiltakene en omfattende og integrert tilnærming til cybersikkerhet. Ved å kombinere proaktiv overvåkning og analyse (Mini-SOC), spesifikk beskyttelse mot en vanlig trussel (DDoS-vernet), og kontinuerlig testing og forbedring av prosedyrer (sektorøvelser), kan sektoren sikre at den er godt forberedt på å møte et bredt spekter av cybersikkerhetstrusler.

## Hva er forutsetningene for en vellykket gjennomføring?

For å lykkes med gjennomføringen av disse tiltakene er det flere viktige forutsetninger som må være på plass:

1. **Finansiering:** Siden disse tiltakene krever betydelige ressurser, er stabil og tilstrekkelig finansiering en avgjørende forutsetning for suksess.
2. **Kompetanse og ekspertise:** Det kreves høy kompetanse innen cybersikkerhet for å implementere og vedlikeholde disse tiltakene. Det er derfor viktig med tilgang på dyktige medarbeidere og eventuelt eksterne eksperter.
3. **Teknologi:** For å etablere et sikkerhetsoperasjonssenter og et DDoS-vern, trengs det både avansert teknologi og infrastruktur.
4. **Samarbeid:** Tiltakene krever samarbeid både internt mellom ulike deler av organisasjonen, og eksternt med partnere som Microsoft og NORDUnet. En kultur for samarbeid og god kommunikasjon er derfor essensielt. Samarbeid med sikkerhetsmiljø i UH-sektoren som NTNU og UiO er også viktig.
5. **Forståelse og støtte fra ledelsen:** For å sikre nødvendige ressurser og prioritering av tiltakene, er det viktig med forståelse og støtte fra organisasjonens ledelse.
6. **Klare rutiner og prosesser:** For å sikre effektiv og sikker drift av tiltakene, er det viktig med klare rutiner og prosesser. Dette inkluderer alt fra hvordan logger skal samles og analyseres, til hvordan potensielle trusler skal håndteres.

7. **Personvern:** Med innsamling og analyse av data, er det viktig å ha robuste løsninger for å ivareta personvernet. Dette inkluderer både tekniske løsninger og klare retningslinjer for hvordan data skal håndteres.
8. **Tilpasningsevne:** Gitt det stadig skiftende landskapet innen cybersikkerhet, er det viktig å kunne tilpasse seg nye trusler og teknologiske utviklinger. En vilje og evne til å lære og tilpasse seg over tid er derfor en viktig forutsetning for suksess.

Sikt er godt rustet for å lykkes og har bygget opp betydelig og bred kompetanse de siste 3 årene. Vi ønsker å bygge videre på det gode arbeidet som er lagt ned de siste årene.