Illustrasjon: Shutterstock

Trusselvurdering 2026

DET DIGITALE TRUSSELBILDET MOT SPESIALISTHELSETJENESTEN

HELSE SØR-ØST HELSE NORD HELSE VEST HELSE MIDT-NORGE

Norsk helsenett
Helse- og kommuneCERT

INNHOLD

Sammendrag 3

Hovedvurderinger 4

1. Innledning 5
1.1. Trusselnivå 5
1.2. Sannsynlighetsord 5

2. Komplekse utfordringer i en usikker tid 6
2.1 Fortsatt usikkerhet i det sikkerhetspolitiske samarbeidet 7
2.2 Sammensatte trusler og sammensatt virkemiddelbruk 7
2.3 Helseberedskap og totalforsvaret 7
2.4 Konsentrasjonsrisiko 9

3. Trusselaktører 10
3.1 Organiserte kriminelle aktører 10
3.2 Statlige aktører 10
3.3 Hacktivister 10
3.4 Innsidere 10

4. Hva motiverer trusselaktørene 11

5. Aktuelle angrepsmetoder 13
5.1 Offensiv kunstig intelligens (KI) 13
5.1.1 Autonome KI-systemer for nettverkspenetrasjon 13
5.1.2 KI-støttet skadevareutvikling 13
5.1.3 KI-systemer som finner og lager utnyttelseskode for nulldagssårbarheter 14
5.2 Metoder for teknisk kompromittering 15
5.2.1 Medisinsk-teknisk utstyr og operasjonell teknologi 15
5.2.2 Kompromittert brukerstyrt endepunkt 15
5.2.3 Angrep mot skybaserte løsninger 16
5.2.4 Leverandørkjeder som angrepsvektor 18
5.2.5 Exploits og sårbarhetsutnyttelse 19
5.3 Sosial manipulering 21
5.3.1 ClickFix 21
5.3. Phishing 22
5.3.3 Målrettet svindel 23

6. Aktuelle trusler mot spesialisthelsetjenesten 24
6.1 Organisert cyberkriminalitet 24
6.2 Cyberspionasje 25
6.3 Innsidevirksomhet 26
6.4 Destruktive cyberangrep og sabotasje 28
6.4.1 Destruktive cyberangrep 28
6.4.2 Sabotasje 29
6.5 Hacktivisme 31

Referanser 32

SAMMENDRAG

Illustrasjon: Shutterstock

Det digitale risikobildet for spesialisthelsetjenesten i Norge det kommende året er skjerpet. Økt digitalisering gir betydelige gevinster for pasientsikkerhet, kvalitet og effektivitet, men skaper samtidig nye sårbarheter gjennom større angrepsflater, komplekse leverandørkjeder og økt avhengighet av skytjenester.

Utviklingstrekkene i internasjonale maktforhold går i negativ retning. Den sikkerhetspolitiske utviklingen globalt preges av økt stormaktsrivalisering, svekket internasjonalt samarbeid og økende bruk av sammensatte virkemidler. Spesialisthelsetjenesten påvirkes direkte av denne utviklingen, både som del av kritisk infrastruktur og som en sentral aktør i totalforsvaret. Økt geopolitisk interesse for Arktis og nordområdene forsterker også trusselbildet. I en mer ustabil sikkerhetspolitisk situasjon, der skillet mellom fred, krise og krig blir mindre tydelig, må helsesektoren forberede seg på mer sammensatte og alvorlige hendelser.

Det blir stadig tettere koblinger mellom de forskjellige kategoriene av trusselaktører. Trusselbildet er komplekst, noe som gjør det utfordrende å skille aktørene fra hverandre. Motivasjonen varierer fra økonomisk vinning og informasjonsinnhenting til ønske om politisk påvirkning og ideologisk overbevisning. Helsedata fremstår som et særlig attraktivt mål, både for økonomiske og strategiske formål.

Digitaliseringen av helsesektoren har ført til en mer kompleks teknologisk infrastruktur med større angrepsflate. Trusselaktørene ønsker å utnytte disse sårbarhetene, og benytter mange ulike angrepsmetoder mot spesialisthelsetjenesten. Angrepene blir stadig mer sofistikerte, og utnytter både teknologiske svakheter og menneskelige faktorer.

Hovedbildet viser at **organisert cyberkriminalitet utgjør den mest alvorlige trusselen**. Angrep drives primært av økonomisk motivasjon og retter seg mot sårbarheter i systemer, brukere og leverandørkjeder. **Innsidevirksomhet og cyberspionasje vurderes som høye trusler**, med særlig interesse for helsedata og strategisk informasjon. Statlige aktører, spesielt Russland og Kina, forventes å gjennomføre etterretningsoperasjoner mot sektoren. **Destruktive cyberangrep og sabotasje vurderes som en moderat** trussel, og slike angrep vil kunne ramme spesialisthelsetjenesten direkte eller indirekte i 2026. Trusselen fra **hacktivisme vurderes som moderat**, og med bakgrunn i den geopolitiske situasjonen vurderes angrep mot spesialisthelsetjenesten som mulig.

HOVEDVURDERINGER

Trusselen mot spesialisthelsetjenesten fra organisert cyberkriminalitet er meget høy

Spesialisthelsetjenesten er et ettertraktet og utsatt mål, og vi forventer økt oppmerksomhet fra utpressingsgrupper og deres samarbeidspartnere i kommende periode. Vi vurderer det som **meget sannsynlig** at spesialisthelsetjenesten vil bli utsatt for angrepsforsøk fra organisert kriminalitet og at trusselen er **meget høy.**

Trusselen mot spesialisthelsetjenesten fra cyberspionasje er høy

Statlige aktører gjennomfører cyberspionasjekampanjer mot vestlig helsevesen, noe vi tidligere har observert mot spesialisthelsetjenesten i Norge. Vi forventer at spesialisthelsetjenesten i Norge vil være et mål i 2026. Trusselen fra cyberspionasje mot spesialisthelsetjenesten er **høy**, og det er **meget sannsynlig** at spesialisthelsetjenesten vil utsettes for cyberspionasje fra aktører med direkte eller indirekte koblinger til russiske og kinesiske etterretningsorganisasjoner.

Trusselen mot spesialisthelsetjenesten fra innsidevirksomhet er høy

Spesialisthelsetjenesten er en sentral aktør i totalforsvaret og råder i tillegg over verdier med betydning for nasjonal sikkerhet. Vi vurderer at dette samlet sett gjør spesialisthelsetjenesten til et attraktivt mål for trusselaktører, som vil kunne ha stor nytte av å plassere innsidere i spesialisthelsetjenesten. Innhenting av informasjon gjennom rekruttering av innsidere utgjør en **høy** trussel mot spesialisthelsetjenesten. Dette gjør at vi vurderer det som **sannsynlig** at spesialisthelsetjenesten vil bli utsatt for innsidevirksomhet.

Trusselen mot spesialisthelsetjenesten fra destruktive cyberangrep og sabotasje er moderat

Den sikkerhetspolitiske situasjonen i verden bidrar til at statlige aktører har økt vilje til å bruke sammensatte virkemidler. Trusselen fra destruktive cyberangrep og sabotasje mot spesialisthelsetjenesten er **moderat**, og det er **mulig** at slike angrep vil kunne ramme spesialisthelsetjenesten direkte eller indirekte i 2026.

Trusselen mot spesialisthelsetjenesten fra hacktivisme er moderat

Det har ikke vært hacktivistangrep rettet direkte mot spesialisthelsetjenesten i foregående periode. Vi har imidlertid sett økt aktivitet fra hacktivister mot kritisk infrastruktur i Norge og Europa, og vurderer trusselen fra hacktivisme mot spesialisthelsetjenesten som **moderat**. Med bakgrunn i den geopolitiske situasjonen vurderer vi at angrep er **mulig.**

INNLEDNING

KAPITTEL 1

I denne trusselvurderingen ser vi på hvordan spesialisthelsetjenesten treffes av truslene som etterretnings- og sikkerhetstjenestene (EOS) presenterer, truslene mot helsesektoren globalt, samt hva som er de mest sannsynlige truslene mot spesialisthelsetjenesten det kommende året.

Kildegrunnlaget i denne vurderingen er basert på observerte og rapporterte hendelser, samt åpne rapporter og trusselvurderinger. Vurderingene er basert på informasjon innhentet fram til 14. april 2026 og må forstås deretter. Tidsperspektivet for vurderingene er ett år fra rapporten publiseres.

1.1. Trusselnivå

Trusselnivå brukes for å beskrive trusselaktørenes kapasitet til og intensjon om å gjennomføre skadelige handlinger og til å beskrive faren ved konsekvensene av tilsiktede hendelser.

Trusselnivå	Beskrivelse
Meget høy	En spesifikk trussel er kjent. Aktøren har kapasitet og intensjon og konkrete planer om et angrep.
Høy	En spesifikk trussel er kjent. Aktører har kapasitet, intensjon og/eller planer om å gjennomføre et angrep.
Moderat	En generell trussel eksisterer. Aktører har kapasitet, intensjon og/eller planer om å gjennomføre et angrep.
Lav	Det finnes mulige trusler fra aktører med begrenset kapasitet og/eller intensjon om å gjennomføre et angrep.
Svært lav	Ingen indikasjoner på angrep eller trusler.

1.2. Sannsynlighetsord

Sannsynlighetsord brukes for å si noe om muligheten for at en gitt hendelse eller et gitt scenario vil kunne inntreffe.

Fremtidsrettede vurderinger vil alltid inneholde en grad av usikkerhet. For å skape en mer ensartet beskrivelse av sannsynlighet i vurderingene, og dermed redusere uklarhet og misforståelser, benytter vi sannsynlighetsord.

Svært lite sannsynlig	Lite sannsynlig	Mulig	Sannsynlig	Meget sannsynlig
< 10 %	10-40%	40-60%	60-90%	90%

KOMPLEKSE UTFORDRINGER I EN USIKKER TID

KAPITTEL 2

Flere tiår med vestlig vekst, multilateralt samarbeid og relativ sikkerhet er i tilbakegang. Globale maktforhold er i endring [1], og den rettsbaserte verdensorden er under angrep. Stormakter bruker i stigende grad økonomiske og militære tvangsmidler til å forsøke å påtvinge andre sin vilje [2]. Dette påvirker tilliten og samarbeidet mellom landene i verden.

Trusselen mot kritisk infrastruktur i Vesten, og bruken av sammensatte virkemidler, øker [2, 3]. Skillet mellom krig og fred blir stadig mindre tydelig, og utfordres av både statlige og ikke-statlige aktører.

Norge er et høyt digitalisert land, og digitale løsninger utgjør en stadig større del også av spesialisthelsetjenesten. Digitalisering er en ønsket utvikling som styrker pasientsikkerheten, bidrar til bedre kvalitet på dokumentasjon og samhandling, i tillegg til at den effektiviserer og forenkler hverdagen. Samtidig er det digitale risikobildet skjerpet, og avanserte trusselaktører utgjør en stadig økende trussel mot spesialisthelsetjenesten.

Illustrasjon: Shutterstock

2.1 Fortsatt usikkerhet i det sikkerhetspolitiske samarbeidet

Stormakter prioriterer i økende grad egne interesser, og bruker makt til å nå sine mål. Det er hardere konkurranse om makt og innflytelse mellom demokratiske og autoritære krefter, trusselbildet er mer komplekst [4] og det forekommer mer uregulert maktbruk [1, 3]. Denne utviklingen gjør seg gjeldende også i Arktis [5]. Situasjonen preger i stor grad nordområdene, og det er en økt interesse for hva som skjer på Svalbard. Denne situasjonen påvirker trusselbildet også mot spesialisthelsetjenesten.

Russland anser seg for å være i konflikt med NATO, og utfører sabotasje og destruktive cyberangrep mot alliansen [2]. Usikkerheten knyttet til USAs rolle som garantist for Europas sikkerhet vil øke Russlands villighet til å intensivere sine hybride angrep mot NATO [2], og den militære trusselen fra Russland mot NATO vil stige. Russland utfører spionasje mot Norge av flere ulike årsaker. En av dem er for å skaffe seg informasjon som kan gi dem fordeler i en mulig krig mot NATO [2].

Kina bruker sin økonomiske makt og sin strategiske posisjon i leverandørkjeder til å legge press på andre stater, og understøtter Russlands krig i Ukraina. Landet utfordrer internasjonale spilleregler, samt verdier som er sentrale for norsk sikkerhet, vekst og velstand [1]. Kina forbereder seg på en skjerpet konflikt med Vesten, og har tydelige mål om å gjøre sin økonomiske og teknologiske utvikling uavhengig av andre land [2].

I takt med at amerikansk politikk blir stadig mer uforutsigbar, kommer trusselen mot vestlige demokratier ikke lenger bare fra Kina og Russland. Ukonvensjonell og konfronterende politikk fra USA, inkludert omfattende endringer i handelspolitikken, har skapt store spenninger og stor usikkerhet i forholdet mellom USA og Europa [1]. USA bruker nå sin økonomiske og teknologiske styrke som et maktmiddel, og utelukker heller ikke bruk av militær makt selv overfor allierte og partnere [2]. USAs trusler om å ta over Grønland har tydelig påvirket skandinavisk sikkerhetspolitikk.

2.2 Sammensatte trusler og sammensatt virkemiddelbruk

Begrepet sammensatte trusler benyttes av norske myndigheter til å omtale fremmede staters kombinerte- militære og ikke-militære- virkemiddelbruk som rammer norsk sikkerhet direkte eller indirekte [4]. Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt [6], og omtales også som hybride trusler eller gråsonekonflikt. Dette kan omfatte virkemidler som cyberangrep, innhenting av informasjon, påvirkningsoperasjoner og kartlegging av kritisk infrastruktur [3].

Trusselbildet mot kritisk infrastruktur øker, og både cyberoperasjoner, desinformasjon og menneskelig påvirkning er en del av dette bildet. Trusselaktørene tar i bruk et bredt spekter av virkemidler som kan brukes både hver for seg, og i samspill for å oppnå størst mulig effekt. Når virkemidlene kombineres kalles det sammensatt virkemiddelbruk.

Sammensatte virkemidler rammer bredt, og kan være krevende å forstå, oppdage, håndtere og motvirke. Metodene omfatter både lovlig og ulovlig virksomhet, og pågår gjerne over lang tid under terskelen for væpnet konflikt. Trusselaktørenes vilje og evne til å konfrontere Vesten og Norge ved å bruke sammensatte virkemidler synes å ha økt [7].

Spesialisthelsetjenesten blir påvirket av den sikkerhetspolitiske situasjonen. Spesielt USA og Kina benytter sammensatte virkemidler, der særlig økonomiske virkemidler har innvirkning på tjenester som spesialisthelsetjenesten er avhengig av. Spesialisthelsetjenesten er en relativt stor konsument av skytjenester, der leveransene er dominert av noen få amerikanske teknologiselskaper.

2.3 Helseberedskap og totalforsvaret

Norge har én, samlet offentlig helsetjeneste som skal virke både i krise og krig og yte helsetjenester til både sivilbefolkningen og Forsvaret [8]. Formålet med helseberedskapen er å verne liv og helse i krise og krig, og spesialisthelsetjenesten må kunne ivareta sine kjerneoppgaver overfor befolkningen samtidig som den understøtter militær innsats [7].

Behovet for digital motstandskraft blir tydeligere som følge av den sikkerhetspolitiske situasjonen,og omfanget av digitale sårbarheter og cyberangrep [7]. For å ivareta god helseberedskap må spesialist-helsetjenesten ha evne til å møte sammensatte trusler. Totalforsvaret, som er den gjensidige støtten og samarbeidet mellom sivil og militær sektor i fred, krise og krig, er viktig for å møte den alvorlige sikker-hetssituasjonen Norge og verden befinner seg i [3].

Spesialisthelsetjenesten er en del av grunnbered-skapen i Norge, og en sentral aktør i arbeidet med å begrense omfanget av og møte kriser [9]. Digital infrastruktur støtter opp under mange områder som inngår i helseberedskapen. Dagens trusselbilde gjør at spesialisthelsetjenesten må forberede seg på enda større hendelser, hvor det kan bli nødvendig både å redusere tjenestetilbudet lokalt eller regionalt, og å flytte pasienter og ressurser.

Forsvarskommisjonen trekker helseberedskapen frem som en sårbarhet i totalforsvaret og et område som særlig vil kreve oppmerksomhet [3]. Norge er utsatt og sårbart for sammensatte trusler i en tid der trusselbildet er blitt mer komplekst. Samfunnets totale motstandskraft må forsterkes [4]. Evnen til å opprettholde kontinuitet i kritiske samfunnsfunksjo-ner, deriblant helse, er viktig for motstandskraften [7].

En rekke utviklingstrekk legger premisser for den fremtidige helseberedskapen. Trusselnivået mot kritisk infrastruktur øker, det samme gjør bruken av sammensatte trusler [3]. Den strategiske betydnin-gen av nordområdene øker, noe som har forsterket stormaktenes interesse for regionen [2].

Illustrasjon: Shutterstock

2.4 Konsentrasjonsrisiko

Virksomheter som understøtter grunnleggende nasjonale funksjoner kan ha betydelige avhengigheter, gjennom verdikjeder og strategiske knutepunkter, til land som utgjør en etterretningstrussel mot Norge. Dersom disse kompromitteres, kan det medføre store konsekvenser for ivaretakelsen av nasjonale sikkerhetsinteresser. Avhengigheter til enkeltleverandører og enkeltland kan medføre økt risiko for bortfall av tjenester, noe som kan brukes for å utøve press og påvirkning [10]. I tillegg kan trusselaktører utnytte bortfall i leveranser til virksomheter som et pressmiddel [11, 12].

Stater som utgjør en sikkerhetstrussel mot Norge, benytter seg av sikkerhetstruende økonomisk virkemiddelbruk. Det er forventet at både Russland og Kina vil benytte seg av slike virkemidler for å oppnå tilgang til varer, tjenester og teknologi [11].

Det som imidlertid ikke har vært ansett som en konsentrasjonsrisiko tidligere, er sårbarheten og avhengigheten til amerikanske varer og tjenester. Vi belyste i fjorårets vurdering at det regulatoriske samarbeidet med USA har endret seg, og at vi må følge med på den sikkerhetspolitiske situasjonen. Det er fremdeles stor usikkerhet knyttet til i det sikkerhetspolitiske samarbeidet med USA, og uforutsigbarheten i amerikansk utenriks- og sikkerhetspolitikk vil fortsette å få konsekvenser for Norge og norske virksomheter.

Etter terrorangrepet 11. september 2001, har amerikanske myndigheter bygget et rammeverk for økonomiske og teknologiske sanksjoner mot land, virksomheter og individer. Den amerikanske regjeringen besitter nå et velutviklet juridisk rammeverk for å påvirke unike strategiske knutepunkter (choke points). Rammeverket benyttes i stadig større grad for strategisk påvirkning – også mot europeiske institusjoner [13]. Amerikanske teknologiselskaper og deres infrastruktur trekkes i stadig større grad inn som et virkemiddel under sanksjonsrammeverket [14].

De internasjonale teknologileverandørene er i økende grad pålagt restriksjoner, og gjerne ikke-kompatible krav, fra ulike stormakter. Skybaserte løsninger er blitt en sentral del av spesialisthelsetjenestens digitale infrastruktur, levert av et fåtall amerikanske teknologiselskaper [12, 2]. Det har forekommet trusler om å stenge tilgangen til amerikanskeide digitale tjenester [15]. Eiere av amerikanske teknologiselskaper uttrykker nå offentlig tvil omkring selskapenes mulighet til å forbli nøytrale teknologileverandører for Europa i framtiden [16].

Både USA og Kina viser økt og eksplisitt vilje til å bruke maktmidler som økonomiske og teknologiske sanksjoner, eksportrestriksjoner på kritiske råvarer og andre handelsbarrierer for å påvirke beslutningstakere. Amerikanske og kinesiske myndigheter bruker påvirkning som strategisk virkemiddel overfor andre stater. Kina benytter seg av strategisk posisjonering i leverandørkjeden knyttet til særlig medisinsk-teknisk utstyr. Kombinasjonen av disse virkemidlene kan utgjøre en trussel mot spesialisthelsetjenesten.

Dersom spesialisthelsetjenesten ikke kan stole på leverandørene, fører dette til alvorlige strategiske og operative konsekvenser. Spesialisthelsetjenesten har en viktig rolle i helseberedskapen og er, i likhet med resten av det norske samfunnet, stadig mer avhengig av digitale løsninger som leveres av et fåtall leverandører. Helseberedskapen må ta inn over seg denne utviklingen [3].

TRUSSELAKTØRER

KAPITTEL 3

Det blir stadig tettere koblinger mellom de forskjellige kategoriene av trusselaktører [17]. Trusselbildet er komplekst, noe som gjør det utfordrende å skille aktørene fra hverandre. For å kunne sikre spesialisthelse-tjenestens verdier, er det imidlertid viktig å kjenne til hvilke typer trusselaktører som truer verdiene våre.

3.1 Organiserte kriminelle aktører

Organiserte kriminelle aktører består av flere undergrupper som til sammen utgjør et komplekst økosystem. I denne rapporten ser vi særlig på kriminelle grupperinger som opererer i cyberdomenet. De er primært drevet av økonomisk vinning, og utnytter menneskelige eller tekniske sårbarheter for å utføre vinningskriminalitet. I tillegg selger disse aktørene tjenester til andre trusselaktører [18].

Ettersom organiserte kriminelle aktører for det meste er økonomisk motivert, er de mindre opptatt av hvem de rammer og er i liten grad begrenset av ideologi og politikk. Den teknologiske utviklingen har bidratt til økt effektivitet og profesjonalitet i cyberangrep utført av disse aktørene.

3.2 Statlige aktører

Statlige aktører er staters etterretnings- og sikkerhetstjenester, men inkluderer også aktører som er engasjert av disse. Formålet med cyberoperasjoner utført av statlige aktører er hovedsakelig å få tilgang til informasjon. Informasjonen kan bidra til situasjonsforståelse og beslutningsstøtte på strategisk og operasjonelt nivå, både militært og geopolitisk. Enkelte land benytter informasjonen for økonomisk vinning, for eksempel gjennom industrispionasje.

Trusselen fra statlige aktører er betydelig. De største statlige aktørene som er aktive mot Norge er Russland, Kina, Iran og Nord-Korea. EOS-tjenestene beskriver disse som en vedvarende cybertrussel i 2026 [19, 5, 12].

3.3 Hacktivister

Hacktivister kan være enkeltpersoner eller grupper som utfører digitale angrep for å formidle politiske eller ideologiske budskap. For en hacktivist er gjerne oppmerksomhet viktigere enn selve resultatet av angrepet. Aktivitetene er som regel sterkt knyttet til den geopolitiske situasjonen og nyhetsbildet, og trusselen fra hacktivister kan derfor endre seg raskt.

3.4 Innsidere

En innsider er en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen for å skade virksomheten til fordel for en annen virksomhet, en fremmed stat eller for egen vinning [20].

En person som ikke har intensjon om å skade kan bli brukt av en trusselaktør uten at vedkommende vet det selv, og dermed uaktsomt eller tilfeldig påføre arbeidsgiver skade eller tap. En bevisst innsider er en person som har til hensikt å begå skadelige handlinger som strider mot virksomhetens interesser [20].

Vanlige motiver er ideologisk overbevisning, økonomiske insentiver eller forhold på arbeidsplassen som fører til at en arbeidstaker ønsker å hevne seg ved å skade virksomheten [20, 21, 13].

HVA MOTIVERER TRUSSELAKTØRENE

KAPITTEL 4

Trusselaktørenes motivasjon for å gjennomføre cyberangrep endrer seg lite med tiden. Det som endres er metodene de benytter [17]. Geopolitisk og sikkerhetspolitisk ustabilitet kan imidlertid påvirke motivasjonen til alle typer trusselaktører, i tillegg til at det vil kunne påvirke både deres målutvelgelse og vilje til å gjennomføre angrep [13].

Aktørene kan ha mer enn ett motiv for å utføre et angrep, og motivasjonen kan også endres underveis i angrepet. Å forstå trusselaktørenes motivasjon gir oss nødvendig innsikt og kontekst for å kunne avdekke hvilke metoder de benytter, og for å kunne etablere god deteksjon og overvåking [17].

Ønsket om å tilegne seg informasjon motiverer statlige aktører til å gjennomføre cyberangrep. Statlige aktører kan bruke kunnskap om andre lands interne forhold til å understøtte sine egne målsetninger. De bruker gjerne cyberangrep som et virkemiddel for å oppnå strategiske fordeler, eller for å ivareta egne interesser [13].

Helsedata, inkludert store aggregerte datasett med anonyme eller indirekte identifiserbare helsedata, er et attraktivt mål for mange, og pekes på som en årsak til at helse- og omsorgssektoren er spesielt interessant for trusselaktører [3, 22].

Økonomisk vinning er en drivkraft for flere typer trusselaktører, og er den mest vanlige motivasjonsfaktoren blant disse [17]. Organiserte kriminelle aktører utnytter sine data- og systemtilganger til å berike seg selv økonomisk, mens innsidere kan være drevet av personlig økonomisk vinning. Enkelte statlige aktører gjennomfører cyberoperasjoner for å fremme landets økonomiske interesser, blant annet for å finansiere våpenprogrammer og militær opprustning [13].

Statlige aktører benytter sammensatte virkemidler for å nå politiske mål, påvirke sikkerhets- og geopolitiske forhold og posisjonere seg for fremtidige cyberangrep og påvirkningsoperasjoner. Formålet kan være å forsøke å endre oppfatningen til enkeltpersoner, grupper eller hele befolkningen i en retning som tjener trusselaktørens interesser [23], å skape frykt og usikkerhet, og å påvirke andre staters politiske prosesser eller beslutninger. Statlige aktører vil benytte sammensatte virkemidler for å forsøke å polarisere og destabilisere samfunn, svekke tillit, skape handlingslammelse og så tvil om hva som egentlig er sant. Helse- og omsorgssektoren kan være et mål for slike destabiliserende operasjoner, hvor formålet er å svekke publikums tillit til kritiske samfunnsfunksjoner.

Stormaktene har alle et ønske om økt tilstedeværelse og innflytelse i Arktis. Russland, Kina og USA har forskjellige interesser, men de ønsker alle å spille en større rolle i regionen [2]. Spenningsnivået og militariseringen har økt, og USAs sikkerhetspolitiske fokus på Arktis påvirker denne utviklingen [2]. Nordområdene er Norges viktigste strategiske område, og av stor betydning i dagens sikkerhetspolitiske situasjon [7]. Spesialisthelsetjenestens rolle i totalforsvaret gjør oss til et attraktivt mål for statlige aktører med interesse for å posisjonere seg i Arktis.

Ideologisk overbevisning kan motivere både grupper og individer til å utføre cyberangrep. Hensikten kan være å skape offentlig oppmerksomhet om trusselaktørens dagsorden eller budskap. Hacktivister er gjerne motivert av ideologi, og utfører cyberangrep for å fremme politiske eller sosiale endringer. Ideologisk overbevisning kan også være en motiverende faktor for personer som begår innsidevirksomhet.

Illustrasjon: KI-generert bilde ved bruk av OpenAI DALL·E

AKTUELLE ANGREPSMETODER

KAPITTEL 5

Digitaliseringen av spesialisthelsetjenesten skal bidra til at de samlede ressursene benyttes på best mulig måte. Samtidig fører digitaliseringen til økt kompleksitet og teknisk avhengighet, og skaper nye sårbarheter og angrepsflater [3]. Trusselaktørene utnytter disse sårbarhetene. I dette kapittelet belyser vi noen av de mest aktuelle metodene og truslene som vi forventer vil skape utfordringer for spesialisthelsetjenesten i den kommende perioden.

5.1 Offensiv kunstig intelligens (KI)

Store språkmodeller innlemmes i dag i et bredt spekter av arbeidsprosesser, systemer og verktøy. Det tekniske økosystemet rundt språkmodeller og KI-plattformer har nådd et modent stadium. Dette fører til at terskelen for bruk av KI reduseres.

Utvikling av nye metoder, og trening av grunnleggende språkmodeller som er state-of-the-art, er ikke lenger forbeholdt vestlige teknologiselskaper. Kina viser evne og vilje til å konkurrere i verdenstoppen på ytelse og teknisk innovasjon innen trening av store språkmodeller. Foreløpig velger kinesiske virksomheter å publisere egne ledende språkmodeller som åpen kildekode. Vi må forvente at det også finnes bedre modeller som ikke er offentlig kjent.

Cyberkriminelle og statlige trusselaktører har vist at de også bruker språkmodeller i eksisterende arbeidsflyt. Vi vet at de brukes til rekognosering, generering av phishing-innhold, til å lage ondsinnet kode og skadevarerammeverk, oversettelse av kommunikasjon med potensielle ofre og i påvirkningsoperasjoner [24, 25, 26]. Vestlige teknologiselskaper har over lengre tid observert hvordan trusselaktører fra Kina, Russland, Iran og Nord-Korea benytter deres språkmodeller for KI-støtte i større deler av angrepssyklusen [27, 24, 28, 29, 25].

Ledende sikkerhets- og trusseletterretningsleverandører beskriver hvordan det cyberkriminelle økosystemets tilbud av KI-løsninger i 2025 har økt i omfang og kvalitet, og at denne trenden trolig vil fortsette [28]. Bruken av KI effektiviserer etablerte angrepsmetoder og reduserer tekniske barrierer for ondsinnet aktivitet [26].

5.1.1 Autonome KI-systemer for nettverkspenetrasjon

KI-systemer som ganske effektivt og autonomt utfører angrep som er instruert av mennesker, er på forskningsstadiet. Innledende studier viser at autonome KI-systemer effektivt utnytter kjente sårbarheter der utnyttelseskode allerede er tilgjengelig, eller bruker kjente teknikker og verktøy som ikke detekteres og stoppes tidsnok [30].

Kjente konfigurasjonsfeil og sårbarheter, særlig der utnyttelseskode er offentlig kjent, vil trolig i økende grad kunne utnyttes automatisk. En mangeårig trend viser at tiden fra initielt fotfeste til trusselaktøren oppnår sine mål i snitt er redusert fra dager til timer [31].

Tid fra initiell kompromittering til aktøren tar aktive steg for å oppnå sine mål er redusert til 29 minutter i 2025, en reduksjon på 70% fra 2021 [26]. Hel eller delvis automasjon av angrepskjeden gjør det mulig for noen typer trusselaktører å utføre angrep langt raskere enn tidligere, og å skalere kampanjer mer effektivt. Krav til responstid og automatiserte mottiltak vil sannsynligvis skjerpes som følge av KI-støtte og automasjon.

Delvurdering

Store språkmodeller gjør foreløpig flere feil enn menneskelige eksperter med en avansert verktøyportefølje, noe som gjør angrepet lettere å oppdage. Vi vurderer derfor at det er **meget sannsynlig** at statlige aktører med høy teknisk kompetanse vil fortsette å benytte mennesker for utføre cyberspionasje og preposisjonering mot høyverdimål for å unngå deteksjon.

5.1.2 KI-støttet skadevareutvikling

En innledende analyse av et nytt skadevarerammeverk utviklet av en kinesiskspråklig trusselaktør, beskriver et omfattende og avansert rammeverk for kompromittering av Linux og container-tjenester i sky [32]. Påfølgende analyser avslørte at rammeverket mest sannsynlig er utviklet av én person ved hjelp av KI i løpet av meget kort tid [33]. Dette viser at KI vesentlig forenkler mange aspekter av skadevareutvikling, og er ressursbesparende for trussel-

aktørene. Dette er det første kjente eksempelet på at et helt skadevarerammeverk er utviklet med omfattende bruk av KI.

5.1.3 KI-systemer som finner og lager utnyttelseskode for nulldagssårbarheter

Etter hvert som språkmodeller har vist seg kapable på tvers av et stort antall problemområder, har interessen for og forskningen på autonome KI-systemer økt. Private og offentlige prosjekter har forsøkt, og lyktes i, å lage systemer som både finner nulldagssårbarheter og lager fungerende utnyttelseskode.

I perioden 2023-2025 viste deltagere i DARPAs[1] «AIxCC challenge» at autonome KI-systemer effektivt kunne avdekke og utnytte unike syntetiske[2] og reelle nulldagssårbarheter i mye brukt åpen kildekode [34]. Enkelte teknologiselskaper har på eget initiativ utviklet lignende systemer som benyttes til å finne og rapportere nulldagssårbarheter i åpen kildekode-prosjekter [35, 36, 37]. Enkeltforskere har i 2026 utviklet KI-systemer som ved hjelp av offentlig tilgjengelig språkmodeller finner nulldagssårbarheter og utvikler fungerende utnyttelseskode [38]. Anthropic rapporterer at deres siste KI-system for å avdekke sårbarheter og lage fungerende utnyttelseskode, har funnet over tusen nye sårbarheter i mye brukt åpen kildekode. Dette inkluderer alvorlige sårbarheter i operativsystemer og nettlesere som kontinuerlig er gjenstand for omfattende sikkerhetstesting [39].

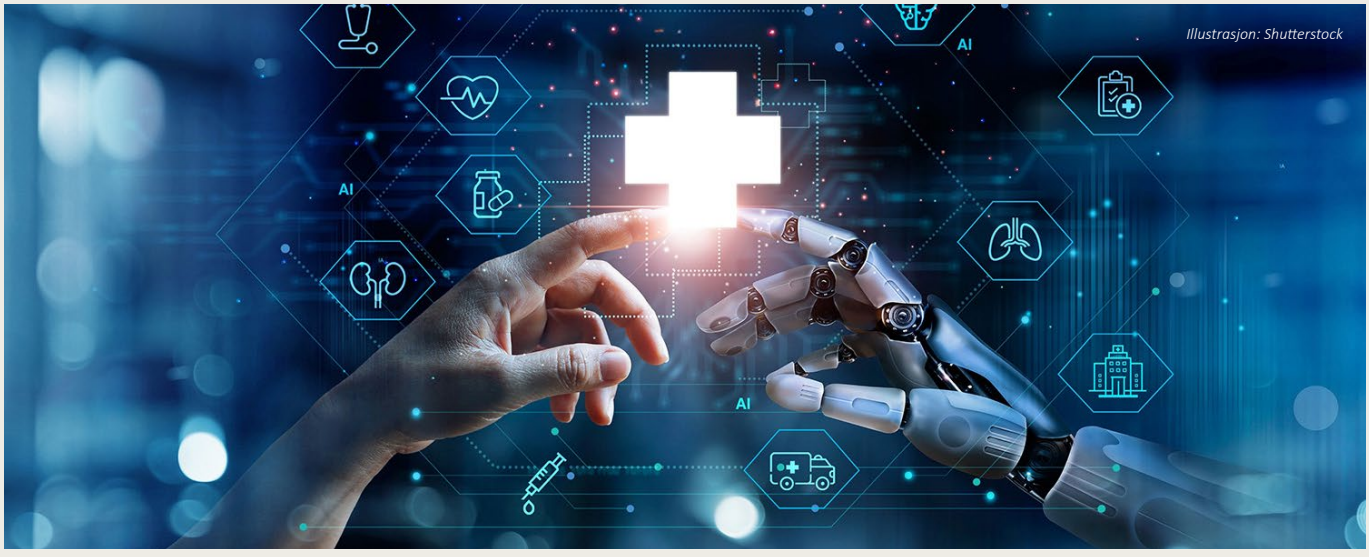
DARPAs AIxCC-konkurranse viser hvordan avanserte trusselaktører som systematisk leter etter og utvikler kode for utnyttelse av nulldagssårbarheter, kan finne og utnytte langt flere ved hjelp av KI. Tilgang til (lukket) kildekode forenkler oppdagelse og utnyttelse av ukjente sårbarheter ved hjelp av KI. Utviklingen i KI-modellenes evner innen cybersikkerhet ser ut til å akselerere.

Delvurdering

Det er grunn til å forvente at statlige aktører med faglig kompetanse og tekniske ressurser allerede, eller i nær fremtid, vil benytte autonome systemer for å avdekke, forstå og forenkle utnyttelse av n-dags- og nulldagssårbarheter.

Den overordnede utviklingen og tilgjengeligheten til KI-teknologien tilsier at det er **svært sannsynlig** at lavt og middels kompetente trusselaktør vil kunne gjennomføre mer sofistikerte angrep, utvikle fungerende skadevare og enklere omgå noen typer sikkerhetsmonitorering.

Det er **svært sannsynlig** at integreringen og bruken av KI i det kriminelle økosystemet vil øke i den kommende perioden, og at trusselaktører vil benytte KI-støtte for å finne nulldagssårbarheter og utvikle fungerende utnyttelseskode.



Illustrasjon: Shutterstock

[1] Defense Advanced Research Projects Agency.
[2] Typiske kodemønstre for utnyttbare sårbarheter ble brukt for å generere unike sårbarheter i produkter.

5.2 Metoder for teknisk kompromittering

Trusselaktørene benytter et bredt spekter av tekniske metoder for å få initiell tilgang, etablere fotfeste og utvide kontrollen i virksomheters digitale miljøer. I spesialisthelsetjenesten omfatter dette blant annet kompromittering av medisinsk-teknisk utstyr og operasjonell teknologi, brukerstyrte endepunkter, skybaserte løsninger, leverandørkjeder og utnyttelse av sårbarheter i internetteksponerte systemer.

Felles for disse metodene er at de retter seg mot teknologi som er tett integrert i kliniske og administrative prosesser, og som i mange tilfeller er krevende å overvåke, vedlikeholde og sikre. Den teknologiske utviklingen gir store gevinster for pasientbehandling og drift, men innebærer samtidig en større og mer sammensatt angrepsflate. Dette stiller økte krav til motstandsevne og evne til rask håndtering av kompromittering på tvers av virksomhetens systemer og verdikjeder.

5.2.1 Medisinsk-teknisk utstyr og operasjonell teknologi

Moderne pasientbehandling er i økende grad avhengig av medisinsk-teknisk utstyr (MTU) som samhandler med en stadig mer kompleks digital infrastruktur. Operasjonell teknologi (OT) omfatter systemer som styrer og overvåker fysiske prosesser, og brukes i spesialisthelsetjenesten både i støttefunksjoner og i klinisk nærliggende systemer. Økt bruk av digitale helsetjenester, inkludert digitalt hjemmesykehus, medfører også økt bruk av MTU i pasientenes hjemmemiljø. Dette utvider angrepsflaten og gjør det mer krevende å etablere og opprettholde robuste sikkerhetstiltak.

KI tas i økende grad i bruk i MTU. Leverandører benytter ofte referansearkitekturer der utstyr kommuniserer med øvrig infrastruktur og eksterne tjenester for å fungere optimalt. MTU kommuniserer i mange tilfeller kryptert med offentlige og private skytjenester hvor helse- og personopplysninger behandles av maskinlæringsalgoritmer. Dette kan øke spesialisthelsetjenestens angrepsflate, særlig gjennom leverandørkjederisiko knyttet til kompromittering av sky- eller produktleverandører. Kompromittering av disse tjenestene kan gi en trusselaktør nettverkstilgang, mulighet til å hente ut helsedata eller manipulere analyser og resultater.

Kryptering av nettverkstrafikk beskytter konfidensialitet og integritet, men reduserer samtidig muligheten for sikkerhetsovervåkning. Begrenset synlighet i nettverkstrafikken, kombinert med at MTU ofte er underlagt godkjenningsordninger, gjør det vanskeligere å herde eller oppdatere. Dette kan svekke evnen til å oppdage og håndtere sikkerhetshendelser. Bruken av eksterne tjenesteleverandører for sanntidsprosessering av MTU-data fører til en ny og skjerpet ekstern avhengighet. Dette skyldes at tjenestene til enhver tid må ha nettverkstilgang til leverandørens tjenester. Mange medisinske tjenesteleverandører benytter seg av offentlige skytjenester.

I 2024 standardiserte National Institute of Standards of Technology (NIST) de første algoritmene for post-kvantekryptografi (PQC) [40, 41, 42]. Flere store teknologileverandører har begynt å implementere disse i operativsystemer, edge-devices- enheter som brannmurer, VPN-servere og filsluser- og applikasjoner. Samtidig har mange MTU-enheter en forventet levetid som strekker seg langt forbi 2035, som er tidsfristen NIST har satt for utfasing av dagens asymmetriske kryptografiske algoritmer. På grunn av regulatoriske krav og medisinske godkjenninger, er vedlikehold og oppgradering av slikt utstyr en omfattende prosess. Mange enheter vil antagelig ikke få støtte for PQC i løpet av sin levetid. Flere leverandører anslår samtidig at kryptografisk relevante kvantedatamaskiner (CRQC[3]) kan bli tilgjengelige flere år før 2035, noe som øker risikoen for at data kryptert i dag kan blir dekryptert i fremtiden [43, 44, 45].

5.2.2 Kompromittert brukerstyrt endepunkt

Dersom en angriper får kontroll på et brukerstyrt endepunkt[4], utgjør dette en stor trussel for virksomheten. Angriperen kan få tilgang til informasjon lagret på enheten og tilganger enheten har til skyløsninger og virksomhetens nettverk. Veien inn til en virksomhets systemer skjer i mange tilfeller gjennom kompromittering av et brukerstyrt endepunkt. Vi må forvente at en angriper kommer på innsiden, og vi må derfor bygge infrastruktur på en slik måte at vi effektivt kan oppdage og kaste ut angriperen, samtidig som skade minimeres.

[3]Cryptographically Relevant Quantum Computer
[4]Utstyr som mobiltelefon, nettbrett, laptop eller stasjonær maskin med generelle operativsystemer.

Som følge av økende bruk i spesialisthelsetjenesten, utgjør mobiltelefoner og nettbrett en stadig større angrepsflate. Moderne arbeidsflyt i spesialisthelsetjenesten innebærer en dynamisk arbeidshverdag med digitale mobile arbeidsflater som gir tilgang til pasientinformasjon. Dette gjør at det er viktig med god visibilitet og deteksjon både på mobiltelefoner og nettbrett som har tilgang til helseinformasjon.

Uten kontroll på enheten er det ikke mulig å håndheve installasjon av sikkerhetsoppdateringer eller virksomhetens sikkerhetsprogramvare. En brukerstyrt enhet som mangler Endpoint Detection & Response (EDR)[5] gir hull i visibilitet med hensyn til deteksjon og håndtering av en hendelse. Sikkerhetsarkitekturen i Android og iOS gjør at EDR-agenter mangler grunnleggende synlighet for å være effektive. Mobiltelefoner og nettbrett er derfor ettertraktede mål for en angriper.

Ved kompromittering av en enhet er angriper avhengig av å kjøre kode på enheten. Dette skjer vanligvis via programmer som allerede er installert på endepunktet eller via skadevare. Ved å bruke programmer og tjenester som allerede er installert blir det vanskeligere å oppdage kompromitteringen. Det har vært en økning i angrep som bruker denne metoden [26].

Brukerstyrte enheter vil ofte ha lagrede passord og autentiseringsnøkler. Selv om disse ligger i et passordhvelv, vil en angriper med kontroll på enheten kunne hente dem ut når brukeren åpner hvelvet. En angriper vil også kunne utnytte tilganger på enheten, for eksempel ved å legge inn kode i kodebrønner, bruke enheten som et nettverksmessig brohode inn i virksomheten eller utnytte andre tilganger som krever en innrullert enhet.

5.2.3 Angrep mot skybaserte løsninger

Dette kapittelet tar for seg de alvorligste truslene mot skybaserte løsninger. Bruken av skytjenester har økt de siste årene. Dette har ført til at flere trusselaktører retter sine cyberangrep mot disse tjenestene og deres leverandører. Trusselaktører har de siste årene hatt en økende interesse for disse tjenestene, blant annet har andelen utpressingsangrep som involverer sky mangedoblet seg på få år [17].

Når flere virksomheter stoler på en tredjepart, slik som en skytjeneste, vil verdien av tredjeparten øke fra en trusselaktørs perspektiv. Trusselaktøren vil ha større gevinst av å kompromittere en skytjeneste med flere kunder enn av å bruke ressurser på å angripe hver av kundene individuelt. Denne typen sentralisering av verdier er et mer attraktivt mål for profittmotiverte cyberkriminelle enn enkeltstående virksomheter. Dette gjør skytjenester til et attraktivt mål [46].

Skytjenester har som oftest en arkitektur som er identitetssentrisk. Identitet er i mange tilfeller den eneste sikkerhetsbarrieren mellom tjenesten og internett. Kompromittering av identiteter har derfor en større konsekvens, særlig for skytjenester uten sekundære sikkerhetsbarrierer som kunden kan konfigurere.

Misbruk av gyldige kontoer og påloggingsinformasjon var også i 2025 den primære metoden for innledende tilgang til skyen [17, 26]. Trusselaktørene har skiftet fokus mot identitets- og tilgangsstyring for å infiltrere skymiljøer [47]. Vi har sett flere forsøk på slike angrep mot spesialisthelsetjenesten den siste perioden, først og fremst gjennom metoder som AiTM-phishing, passordspraying og infostealers på privat utstyr. Angrepsflaten er stor fordi man ofte kan få tilgang til kontoene i skyen fra privat utstyr og nettverk utenfor virksomhetens kontroll. Mer sofistikerte metoder for å utnytte identiteter i skyen kan være verdikjedeangrep gjennom ondsinnede OAuth-applikasjoner , nedgraderingsangrep eller svakheter i autentiseringen [17].

I et vellykket AiTM-angrep mot en skykonto, forsøker trusselaktøren ofte å opptre varsomt slik at brukeren ikke blir varslet om misbruk, blant annet ved å ikke endre påloggingsdetaljer. Dette gir angriper stabil tilgang til skymiljøet, og deteksjonsrisikoen blir lavere [48]. Skytjenester tilbyr ofte grensesnitt som gjør det mulig å programmatisk hente ut informasjon om brukere, rettigheter, applikasjoner, e-poster, chatter, filer og annet innhold [49]. Vi har sett at disse utnyttes av angripere som får tilgang til skykontoer

[5]Beskyttelse, monitorering og respons på endepunkt.
[6]Skadevare som har som formål å stjele brukernavn, passord og annen verdifull informasjon fra maskinen den er installert på.
[7]Applikasjoner som lurer brukere til å gi samtykke slik at angriperen kan handle på deres vegne i skyen.
[8]Angrep som tvinger pålogging over til svakere protokoller som kan utnyttes eller omgås.

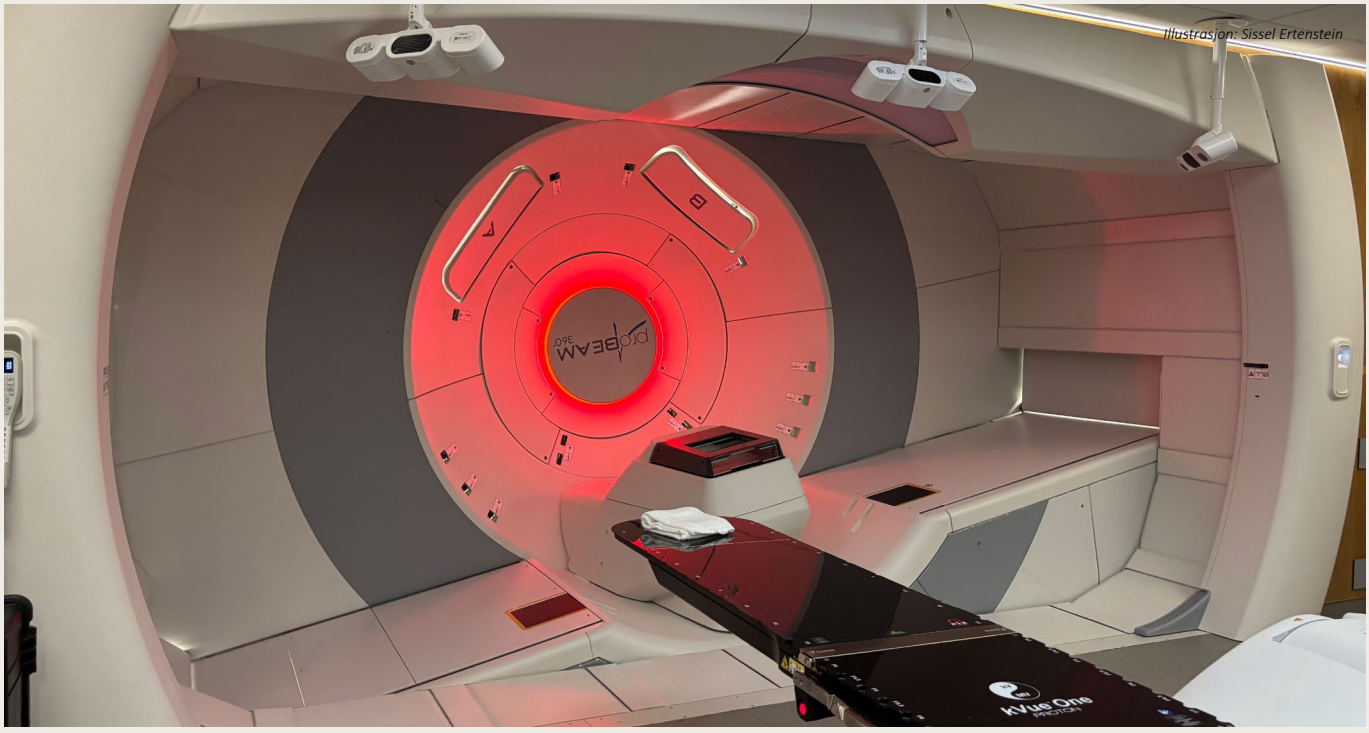
for deretter å raskt og automatisk samle inn informasjon som kan brukes videre i angrepet. Metoden er beskrevet i kapittelet om phishing.

Den delte ansvarsmodellen i skytjenester medfører begrensninger i kundens direkte innsyn i og overvåkning av den underliggende infrastrukturen. I slike tjenester har skytjenesteleverandøren et betydelig ansvar for sikkerheten i den underliggende plattformen, inkludert drift, grunnleggende sikring og deler av deteksjon og overvåkning. CSRB-rapporten om innbruddet i Microsoft Exchange Online sommeren 2023 er et eksempel på at leverandørens sikkerhetsstyring og deteksjonsevne kan være avgjørende for å oppdage og håndtere angrep, og at svakheter i disse mekanismene kan få store konsekvenser [50].

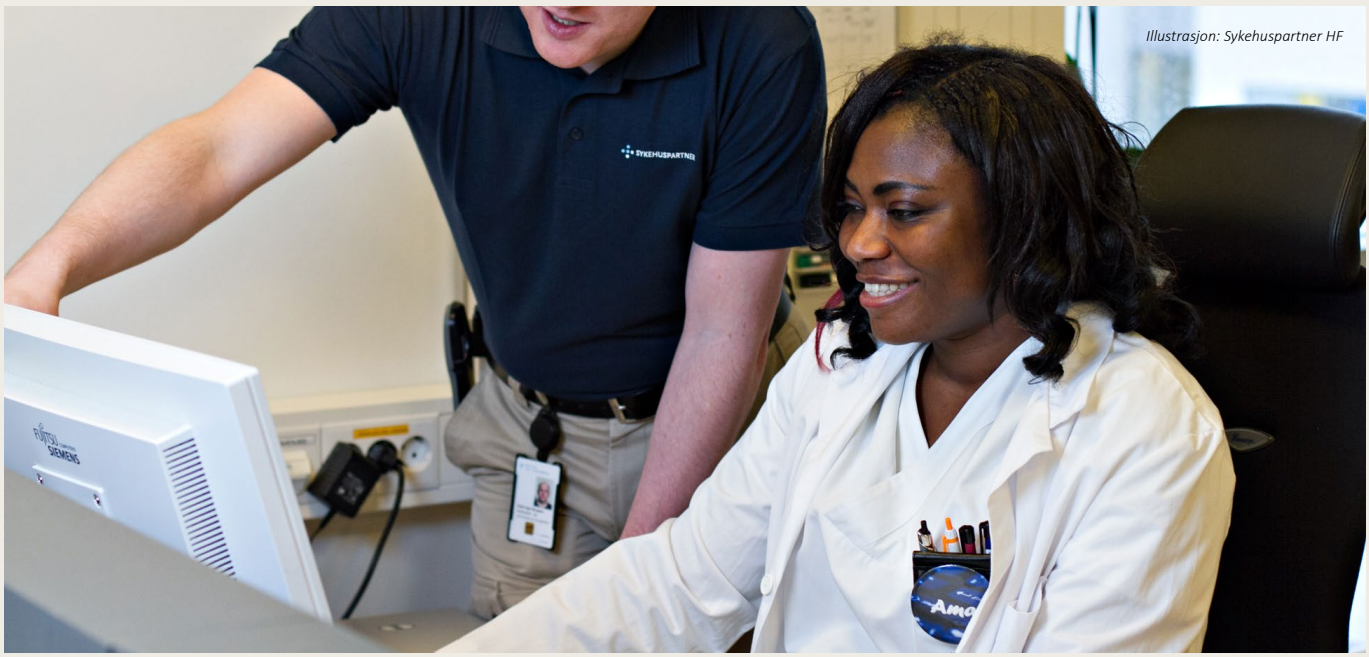
Mangel på alternative deteksjonskapabiliteter gjør kundene spesielt sårbare dersom skytjenesten blir utsatt for angrep, særlig dersom leverandøren ikke evner å detektere dette [51, 50, 52]. Dette understreker behovet for tydelig ansvarsavklaring mellom kunde og leverandør, samt aktiv bruk av tilgjengelige sikkerhets- og overvåkingsfunksjoner i skytjenesten. I et komplekst skymiljø med SaaS-applikasjoner, forskjellige rettighetsregimer og gjestekontoer, kan det også være vanskelig for organisasjoner å holde oversikt og kontroll over hvem som har hvilke tilganger [17]. De store skytjenestene er gjerne i rask utvikling for å holde seg konkurransedyktige, noe som bidrar til kompleksiteten.

Valg av skytjenester er ikke lenger bare en teknisk beslutning, men blir sterkt påvirket av geopolitiske forhold, som igjen medfører operasjonell og strategisk risiko for spesialisthelsetjenesten. Ved bruk av utenlandske skytjenester avgis også deler av kontrollen over egne data og systemer som følge av delt ansvarsmodell og jurisdiksjon [12]. Spesialisthelsetjenesten er avhengig av amerikanske teknologileverandører, herunder skytjenester. Dette skjer fordi vi i økende grad tar disse i bruk, og har tredjepartsavhengigheter via underleverandører som også benytter seg av skytjenester.

De største teknologileverandørene har i stor grad kontrollen over den globale digitale infrastrukturen, noe som kan gjøre tjenestene våre sårbare for handelshindringer og sanksjoner.



Illustrasjon: Sissel Ertenstein


Illustrasjon: Sykehuspartner HF

5.2.4 Leverandørkjeder som angrepsvektor

Geopolitiske spenninger kan føre til at leverandører som er underlagt statlig kontroll eller innflytelse blir instruert til å forsinke eller nekte leveranse av varer. På samme måte kan de bli pålagt av relevante myndigheter å bryte avtalte forpliktelser eller la være å gjennomføre nødvendige sikkerhetsoppdateringer. Enkelte leverandører er tidligere blitt mistenkt for å legge inn skjulte bakdører eller la være å håndtere kritiske sårbarheter. Dette gir trusselaktører en indirekte inngang til virksomheter som kan utnyttes videre [53]. Spesialisthelsetjenesten har mange leverandører, samt at vi utvikler programvare selv der eksterne komponenter inngår. Dette gjør oss eksponert gjennom mange verdikjeder.

Informasjonssystemer består av komponenter fra mange ulike produsenter, og gir potensielt lange leverandørkjeder. Det er krevende å kontrollere og styre risiko i verdikjedene [3]. Leverandører er attraktive mål for trusselaktører [54], og flere cyberangrep utnytter underleverandører for å ramme virksomheter [10]. Ved å kompromittere en underleverandør i verdikjeden, kan angriperne ramme selv godt sikrede mål [17].

De siste årene er det observert mer avanserte angrepsmetoder. Innenfor leverandørkjedeangrep er det to relaterte, men ulike teknikker- ***verdikjedeangrep*** og ***tredjepartsangrep*** [53, 46].

Et ***tredjepartsangrep*** innebærer at en trusselaktør utnytter en sårbarhet hos en tredjepart for å få tilgang til én eller flere virksomheter.

Eksempelvis kan en angriper kompromittere en tjenesteleverandør som har nettverksmessig tilgang til kundenes infrastruktur [18].

Et ***verdikjedeangrep*** er når en angriper kompromitterer noen som lager, vedlikeholder eller drifter programvare du bruker.

For eksempel kan angriperen opprette en form for bakdør i programvaren og vente på at brukeren installerer denne siste "oppdateringen" som del av sin vanlige vedlikeholdsrutine. Et annet eksempel er at de skaffer tilgang til en VPN-tilkobling som en leverandør bruker for å drifte infrastruktur hos brukeren [89].

Et ***verdikjedeangrep*** skjer før produktet eller produktoppdateringen tas i bruk, der skadevare eller sårbarhet skjules og bygges inn i kjente og populære produkter som benyttes av mange [54, 53]. I et slikt angrep endrer en trusselaktør eksisterende kode, eller legger inn ny kode i et produkt [54, 46]. Dette kan gjennomføres så langt nede i verdikjeden at det i praksis er nærmest umulig å ha full oversikt over alle involverte komponenter og avhengigheter [53]. Skadevaren kan ligge skjult lenge, og aktiveres under

bestemte forhold. Slike angrep gjør det da mulig for skadevaren å ligge latent og uoppdaget over lengre tid [54, 53]. Når programvaren oppdateres, blir skadevaren installert på kundenes systemer noe som kan gi trusselaktører tilgang til nettverket deres [54].

Verdikjedeangrep kan benyttes for å begå flere ulike kriminelle handlinger, og knyttes derfor ikke til en bestemt aktørprofil. Primært benyttes det av aktører som forsøker å tilegne seg uautorisert tilgang til et datasystem via programvare [46]. Verdikjeder for programvare utgjør en massiv sårbarhetsflate med mange involverte parter. Det benyttes i stor grad åpen kildekode, og vekstraten på bruk av åpen kildekode er stigende [53, 46]. Imidlertid kan slike angrep også skje i lukket kildekode dersom trusselaktøren allerede er på innsiden av utviklingsmiljøet.

I november 2025 kom ett av de større verdikjedeangrepene i nyere tid. Angrepet fikk navnet Shai-Hulud 2.0. Innen 72 timer var det over 25.000 kompromitterte GitHub-kodebrønner [55]. Skadevaren leter etter hemmeligheter fra AWS Secrets Manager og Azure Key Vault, som deretter lastes opp til trusselaktøren [56].

Verdikjedeangrep via programvare har i løpet av de siste årene gått fra å være en lite utbredt teknikk, til å være blant de raskest voksende teknikkene. Aktører bak slike angrep har vist seg å være tålmodige, ved at de bruker lenger tid på å komme seg i posisjon til å implementere en bakdør. Likevel krever ikke alle typer verdikjedeangrep tålmodighet eller særlig teknisk kompetanse [46].

Potensialet til å ramme svært mange virksomheter som følge av én kompromittert programvarekomponent er særlig bekymringsverdig. Et nylig eksempel på et omfattende verdikjedeangrep var da kinesisk etterretning tok over en oppdateringsserver for Notepad++ for å etablere en bakdør hos utvalgte mål [57].

I et ***tredjepartsangrep*** angriper trusselaktøren via en tredjepart for å ramme én eller flere virksomheter. Typiske angrepsvektorer er phishing, misbruk av lekkede eller stjålne brukernavn og passord samt utnyttelse av offentlig kjente sårbarheter eller nulldagssårbarheter i programvare [46].

Det kan være flere årsaker til at trusselaktører benytter seg av denne typen angrep. Kompromittering ett sted i verdikjeden kan gi tilgang til flere virksomheter. Andre forhold kan være tilfeller der en større virksomhet har gode sikkerhetsløsninger som vanskeliggjør tilgang. I slike tilfeller kan en trusselaktør utnytte en kjent sårbarhet hos en tilknyttet leverandør, og på den måten få tilgang til målet [46].

Trusler mot viktige samfunnsfunksjoner utøves i stor grad av statlige eller statsfinansierte aktører som kompromitterer IKT-systemer for å hente ut informasjon eller etablere varig tilgang. Motivene kan være forberedelser til fremtidige sabotasjeoperasjoner eller forberedelse til krig. Særlige mål er leverandører og utviklere knyttet til kritisk infrastruktur, for eksempel i forbindelse med plassering av digitale bakdører [22].

5.2.5 Exploits og sårbarhetsutnyttelse

Utnyttelse av sårbarheter i internetteksponerte systemer globalt utgjorde inngangsvektoren i 32% av angrep i 2025 [47]. Dette er det sjette året på rad at dette er den desidert største inngangsvektoren i cyberangrep, og representerer den nye normalen. De siste årene er det spesielt edge-devices, slik som brannmurer og VPN-mottak som har vært utsatt. Statlige aktører har systematisk utnyttet kritiske sårbarheter i produkter som er sentrale for en virksomhets arbeidsflate.

Edge-devices representerer en stor sikkerhetsrisiko for en virksomhet. De kan være eksponert mot internett, og har tilgang videre inn i virksomhetens nettverk. I tillegg har de som regel begrensede muligheter for sentralisert logging og monitorering. Dette gjør dem til naturlige mål for en angriper, noe som gjenspeiles i mengden nulldagssårbarheter[9] som er blitt utnyttet i edge-devices de siste årene. Det er estimert at over 25% av nulldagssårbarheter som er blitt utnyttet er i edge-devices [58]. I 2025 var halvparten av utnyttede nulldagssårbarheter i enterprise-programvare [59].

[9]En sårbarhet som er oppdaget og utnyttet før den er kjent for leverandøren og offentligheten.

Illustrasjon: Sykehuspartner HF

De siste årene har vi sett en drastisk nedgang i tiden det tar fra en sårbarhet blir kjent til den utnyttes. Der man før kunne forvente å ha flere dager på å oppdatere et produkt, må man nå ha beredskap for å håndtere kritiske sårbarheter 24/7. I 2023 tok det i snitt fem dager fra et produkt lukket en sårbarhet til den ble utnyttet [60]. Vi forventer at dette intervallet reduseres ytterligere.

Utnyttelse av nulldagssårbarheter skjer som regel først i målrettede angrep med begrenset omfang. Når angrepene oppdages og sårbarhetene blir kjent, tar det kort tid før de samme sårbarhetene masseutnyttes. Alle som har sårbart utstyr på nett må forvente å bli kompromittert i løpet av kort tid, gjerne innen et par døgn [61]. Utnyttelse av null-dagssårbarheter er nå så utbredt at, for sårbarheter som faktisk blir utnyttet, er gjennomsnittlig tidsfor-skjell mellom første utnyttelse og publisering av en sikkerhetsoppdatering **minus** 7 dager. Det vil si at disse sårbarhetene i snitt utnyttes omtrent én uke før de blir offentlig kjent [47].

En stigende trend de siste årene er bruken av flere sårbarheter i rekkefølge for å få kontroll på en edge-device, også kalt exploit chaining. Dette gjør at sårbarheter som tidligere virket mindre kritiske, og som kunne nedprioriteres, nå må vurderes sammen med andre sårbarheter. Vi har sett eksempler på denne typen utnyttelse i flere år og i produkter fra flere sikkerhetsleverandører [31, 62, 59].

Utnyttelse av sårbarheter i edge-devices, både enkeltsårbarheter og exploit chaining, er ikke forbeholdt statlige aktører. Organiserte cyber-kriminelle er gjerne blant de første som utnytter en sårbarhet når den er kjent. Under masseutnyttelse må man forvente at utpressingsaktører forsøker å komme seg inn. Det er derfor vesentlig for en virksomhet å redusere tiden det tar å oppdatere edge-devices, også der tilgjengelighet er kritisk og oppdatering derfor er krevende. Når tiden det tar fra en sårbarhet er kjent til den utnyttes går ned, må også tiden det tar fra en oppdatering slippes til den er installert ned.

5.3 Sosial manipulering

Sosial manipulering er et samlebegrep for metoder som benytter psykologiske virkemidler for å manipulere en person til å utføre en handling eller oppgi informasjon. Trusselaktører utnytter følelser som frykt, fristelser, tillit og tidspress, og benytter verktøy som sosiale medier, e-post, tekstmeldinger og telefonsamtaler til å gjennomføre sosial manipulering. Et målrettet cyberangrep kan bruke informasjon eller tilganger samlet inn via sosial manipulering.

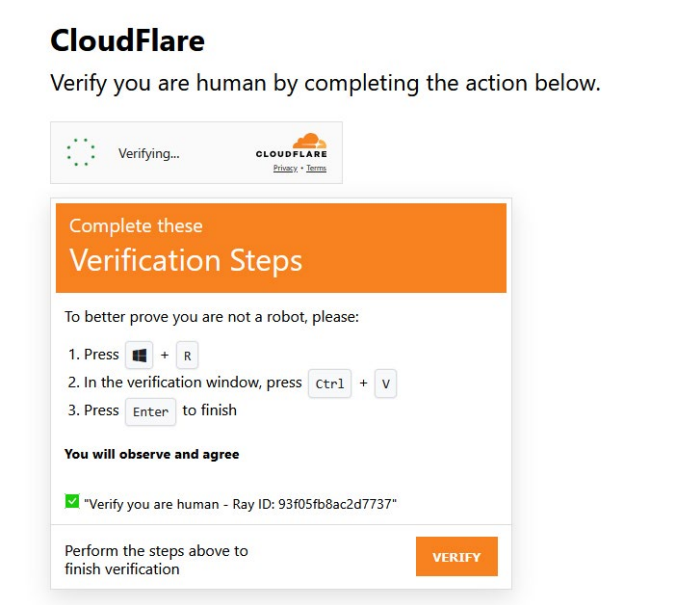
5.3.1 ClickFix

ClickFix er en angrepsmetode der en bruker lures til å kopiere og kjøre ondsinnet kode ved å utnytte tilliten brukere har til tilsynelatende legitime feilmeldinger, CAPTCHA-løsninger eller instrukser presentert på en nettside. Et vellykket angrep fører til at angriper får tilgang til maskinen og at lagrede brukernavn og passord stjeles eller at maskinen blir del av et botnet[10] [17, 63].

Fra de første rapporterte tilfellene tidlig i 2024 [63], har ClickFix nå utviklet seg til å bli én av de vanligste metodene for spredning av skadevare [17]. Flere sikkerhetsselskaper rapporterer at de har sett en mangedobling av denne typen angrep i 2025 [64, 65, 66]. I samme periode er det observert flere endringer i angrepsmetoden, både i hva som presenteres til brukeren og hva brukeren blir bedt om å gjøre. Endringene er sannsynligvis gjort for å unngå deteksjon, og for å gjøre det vanskeligere å finne ut hva som har skjedd under en hendelse.

Et ClickFix-angrep starter i mange tilfeller med at brukeren lokkes inn på en nettside kontrollert av angriperen. Dette kan skje gjennom phishing, kompromittering av en legitim side, søkemotoroptimalisering[11] eller andre sosiale manipuleringsteknikker. Når brukeren åpner nettsiden, møtes de med et problem som kan løses ved å følge enkle instruksjoner. Dette innebærer i praksis at brukeren kopierer og kjører ondsinnet kode.

Metoden brukes av både cyberkriminelle og statlige aktører. Aktører knyttet til Russland, Nord-Korea og Iran har benyttet ClickFix i enkelte angrepskampanjer [67]. Mot slutten av 2024 rapporterte ukrainske myndigheter om slike angrep, trolig utført av en russisk statlig aktør med formål om å hente ut sensitiv informasjon [68].



Bilde: Eksempel på en typisk ClickFix-nettside med et manipulert CAPTCHA-krav. Angripers kode legges automatisk i utklippstavlen slik at den limes inn når bruker trykker Ctrl+V.

Også i spesialisthelsetjenesten har vi sett flere tilfeller av ClickFix-angrep det siste året. Dette inkluderer både kompromitterte nettsider rettet mot sektoren, og tilfeller der enkeltbrukere er blitt rammet når de har brukt arbeids-PC til privat bruk.

Delvurdering

Det er **meget sannsynlig** at flere av våre brukere er blitt utsatt for slike angrep på private enheter hvor sikkerhetsmekanismene gjerne er svakere. Disse enhetene utgjør en trussel mot spesialisthelsetjenesten fordi de ofte har tilganger til arbeidsgivers systemer.

[10] Botnet; en samling nettverkstilknyttede enheter som kan fjernstyres av en operatør (robotnettverk), med eller uten eiers samtykke.
[11] En teknikk for å forbedre en nettsides plassering i søkeresultater. Ondsinnede nettsider kan gjøre dette for å bli rangert høyere enn legitime resultater for å lure brukere til sin side.

5.3.2 Phishing

Phishing er en av de mest utbredte metodene for å skaffe seg tilgang til interne systemer [17, 48]. Angrepsformen benyttes i både opportunistiske og målrettede angrep.

Innebygde filtre fra leverandører og egendefinerte regler basert på kjente trusler, stopper de fleste phishing-e-poster før de når mottaker. De e-postene som kommer frem til mottaker er imidlertid i mange tilfeller sofistikerte og vanskeligere å oppdage.

Adversary-in-the-middle-phishing (AiTM) er en type phishing der angriper lurer offeret til å logge inn på sin infrastruktur og videresender innloggingsinformasjonen til den legitime tjenesten, inkludert flere typer multifaktorautentisering. På denne måten blir angriper sittende igjen med en gyldig sesjon til den legitime tjenesten.

AiTM-phishing er en vedvarende trussel mot spesialisthelsetjenesten. I perioden har vi observert flere AiTM-kampanjer som har truffet spesialisthelsetjenesten og våre leverandører. Når en virksomhet først er kompromittert, benytter angriperne gjerne den legitime e-postkontoen til å sende phishing-e-poster – ofte til kontakter den kompromitterte kontoen tidligere har kommunisert med. Dette øker sannsynligheten for at mottakere stoler på innholdet og klikker på lenker, og dermed bidrar til videre spredning innad i en virksomhet eller et fagmiljø. En høy andel av våre brukere blir lurt av slike angrep. Vi har observert vellykkede AiTM-angrep mot spesialisthelsetjenesten i perioden. Angrepene virker å være økonomisk motivert.

Med økt bruk av mobiltelefoner til jobbformål, øker også risikoen for vellykkede phishingangrep ettersom flere sikkerhetsmekanismer gjerne mangler på slike enheter. Flere phishingvarianter er spesifikt utformet for å få brukere til å åpne lenker på mobiltelefon, inkludert SMS-phishing (smishing) og QR-phishing (quishing) [53]. Enkelte phishingsider sjekker enhetstype før de viser innhold, og omdirigerer brukere til uskyldige sider dersom de ikke benytter mobiltelefon – en metode som bidrar til å unngå deteksjon.

De mest avanserte phishing-e-postene vi ser mot spesialisthelsetjenesten er formulert på godt norsk. KI benyttes til oversettelse og språklig tilpasning i disse e-postene, noe som øker troverdigheten og dermed sannsynligheten for vellykkede angrep. Statlig tilknyttede aktører fra Iran og Nord-Korea har tatt i bruk språkmodeller i rekognoseringsfasen og for tilpasning av phishing-innhold [28]. Én ansatt hos Trend Micro laget i løpet av 24 timer en brukervennlig proof-of-concept-løsning som automatisk gjennomfører rekognosering ved hjelp av åpne kilder mot alle ansatte i en virksomhet. Deretter lages tilpassede målpakker mot hver enkelt ansatt ved hjelp av KI [69]. KI-agenter gjør det nå mulig å skalere og effektivisere angrepskampanjer med lav kostnad [17].

Det har vært en markant økning i angrepsformen kalt voice-phishing (vishing)- phishing som gjøres gjennom telefonsamtaler [48, 26]. Et vishing-angrep skjer for eksempel ved at angriperen utgir seg for å være IT-support og ringer en ansatt, eller kontakter IT-support og utgir seg for å være en ansatt [48, 53]. Angriper forsøker å overtale vedkommende til å laste ned skadevare eller starte skjermdeling. Vi har observert slike angrep mot ansatte i spesialisthelsetjenesten der hensikten var økonomisk svindel. I enkelte avanserte angrep kan KI brukes for å klone stemmer, noe som gjør det svært utfordrende å avsløre.

For å beskytte seg mot phishing kan det iverksettes flere tiltak, inkludert geoblokkering der man begrenser hvilke land det tillates at det kommuniseres med. Dette har angripere tilpasset seg ved å automatisk sende trafikken sin gjennom residential proxies[12]. Trafikken ser dermed ut til å komme fra et norsk hjemmenett, noe som i mange tilfeller er nok til at trafikken unngår deteksjonsmekanismer. Flere rammeverk for å gjennomføre AiTM-angrep lar angriper automatisk velge en proxy som er i geografisk nærhet til offeret, noe som ytterligere reduserer sannsynligheten for deteksjon.

Det er gjerne en forsinkelse fra AiTM-angrepet skjer til det blir oppdaget. Forsinkelsen kan være fra noen minutter til flere timer, og av og til blir det ikke

[12]Utstyr hos privatpersoner, ofte kompromittert, som man kan rute trafikken gjennom som en VPN.

fanget opp i det hele tatt. I dette tidsvinduet kjører angriper automatiserte handlinger som henter ut informasjon eller legger inn autentiseringsmetoder som de kan benytte senere. Informasjon som hentes ut kan være navn, e-post, jobbtittel, Teams-meldinger og hvilke arbeidsområder brukeren har tilgang til. Denne innhentingen gjør det mulig for angriperen å gjøre en enkel vurdering når det gjelder hvilke kontoer det er verdt å bruke og hvilke måter de kan brukes på. Noen kontoer kan være best brukt til å sende ut phishing-eposter, mens andre kan inneholde verdifull informasjon eller ha verdifulle tilganger.

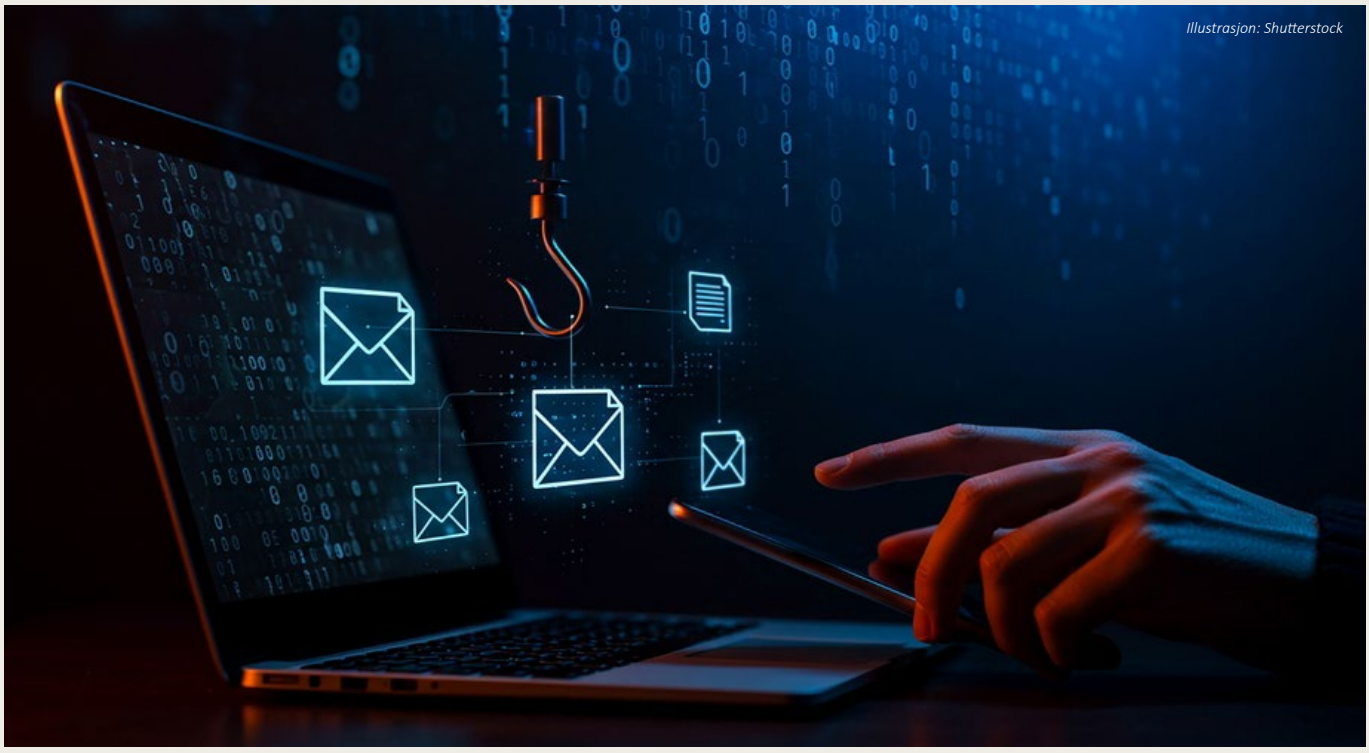
5.3.3 Målrettet svindel

I en årrekke har spesialisthelsetjenesten vært utsatt for forskjellige typer svindelforsøk, og noen er mer målrettede enn andre. Med målrettet svindel mener vi svindelforsøk som er tilpasset den enkelte mottaker.

Vi observerer årlig forsøk på målrettet fakturasvindel mot spesialisthelsetjenesten. De mest alvorlige tilfellene vi har observert gjelder forsøk på å stjele flere millioner kroner. I disse tilfellene har svindleren brukt offentlig tilgjengelig informasjon for å lure til seg informasjon fra en reell leverandør, og deretter brukt denne informasjonen for å forsøke å svindle virksomheten.

Trusselaktører kan utføre målrettet svindel ved å skaffe tilgang til legitime ubetalte fakturaer, og endre mottakerkonto. Et eksempel på et slikt angrep er da spesialisthelsetjenesten tidlig i 2026 opplevde et slikt angrep fra en trusselaktør som utga seg for å være SSB og ba om innsyn i fakturaer.

Helsesektoren forvalter betydelige deler av statsbudsjettet, og har jevnlige prosjekter og innkjøp fra mange forskjellige leverandører som involverer store beløp. Spesialisthelsetjenesten er underlagt lov om offentlige anskaffelser, noe som fordrer at informasjon om større innkjøp offentliggjøres. Vi har de siste årene sett flere tilfeller der informasjon fra anbudsprosesser utnyttes av svindlere for å forsøke å lure ansatte i spesialisthelsetjenesten til å gjennomføre innbetalinger til angripers bankkonto.



Illustrasjon: Shutterstock

AKTUELLE TRUSLER MOT SPESIALISTHELSETJENESTEN

KAPITTEL 6

For å kunne beskytte verdiene til spesialisthelsetjenesten er det viktig å forstå hva trusselaktørene er ute etter og hvilke metoder de bruker for å nå sine mål. I dette kapittelet vurderer vi de største truslene mot spesialisthelsetjenesten.

6.1 Organisert cyberkriminalitet

Organiserte cyberkriminelle bruker stadig mer målrettede, langsiktige digitale angrep, utført av kompetente aktører, som kan beskrives som sofistikerte angrepsformer. Spesialisthelsetjenesten opplever kontinuerlige angrep fra organiserte cyberkriminelle. Dette kan være svindelforsøk, forsøk på utnyttelse av eksponerte sårbarheter eller forsøk på å få fotfeste på klientmaskiner. I likhet med andre virksomheter ser vi at trusselen mot spesialisthelsetjenesten forsterkes ved bruk av KI og sofistikerte utpressingsmetoder.

Det er stor variasjon i angrepsmetodene til de organiserte cyberkriminelle. Et komplisert aktørlandskap gjør det enda mer utfordrende å identifisere de ulike aktørene. De økende geopolitiske spenningene har fått større påvirkning på forholdet mellom ulike aktører, og er med på å forsterke allerede uklare skillelinjer mellom statlige aktører, hacktivister og profittmotiverte organiserte cyberkriminelle aktører. Det finnes flere utpressingsaktører som velger mål for profitt, men også for å imøtekomme ulike geopolitiske interesser [48, 46]. I 2026 vil utpressingsangrep være den mest fremtredende angrepsmetoden [26] .

Norske og utenlandske myndigheter har rapportert om ulik grad av samarbeid og erfaringsutveksling mellom kriminelle aktører og statlige aktører. Samarbeidet innebærer at verktøy, metoder og skadevare blir overført fra en ak¬tør til en annen [46]. Noen ganger skjer dette uten at det nødvendigvis er et direkte samarbeid, men fordi cyberdomenet er så sammenvevd at aktørene lærer av hverandre uten at de samarbeider direkte [18].

Flere av angrepene som observeres mot spesialisthelsetjenesten antas fremdeles å komme fra organiserte kriminelle som kobles tett til utpressingsaktører. Utpressingsangrep er hendelser der en aktør har fått tilgang til systemer, og kan ha stjålet eller kryptert data og dermed gjort systemer utilgjengelige. En utpressingsaktør vil presse et offer for penger mot å dekryptere data og ikke publisere det som er stjålet.

Stjålne data kan inneholde verdifull informasjon. Dersom en angriper får ut e-poster eller filer, vet vi av erfaring at disse kan inneholde passord, nettverksskisser eller beskrivelser av interne forhold som kan benyttes ved et senere angrep. Dette øker trusselen mot spesialisthelsetjenesten ved at påloggingsinformasjon til virksomheten kan komme på avveie eller at aktører kan presse offeret til å gi fra seg slik informasjon.

Cyberkriminelle bruker KI for å redusere tiden fra en sårbarhet blir kjent til den blir utnyttet til bare noen timer. Dette betyr at sårbarhetshåndtering som tidligere kunne gjøres rutinemessig, er blitt et kappløp mot automatisk sårbarhetskartlegging og påfølgende utnyttelse [17]. Utviklingen fremover vil være preget av at det digitale integreres stadig tettere med kriminalitetsutøvelse [18].

Cyberkriminelle står for en stor del av angrepene mot digital infrastruktur, og drives av økonomisk vinning. Over halvparten av alle cyberangrep er drevet av utpressing eller løsepengevirus med økonomisk motiv, mens spionasjeangrep utgjorde bare noen få prosent [12, 17].

Cyberkriminelle fortsetter å rette angrep mot virksomheter som er del av samfunnsviktige tjenester som kan ha direkte og umiddelbar innvirkning på folks liv om de kompromitteres. Sykehus og andre offentlige virksomheter er særlig utsatt, både fordi de lagrer sensitive data og fordi de har varierende sikkerhetstilstand. Cyberangrep mot helsesektoren kan få alvorlige konsekvenser, som forsinket akutt og elektiv medisinsk behandling, forstyrrede nødetatstjenester og avlyste timeavtaler. Trusselaktører som spesialiserer seg på utpressingsangrep retter seg spesifikt mot disse virksomhetene på grunn av deres begrensede handlingsrom [17, 70].

Vurdering
Spesialisthelsetjenesten opplever kontinuerlig angrep fra organiserte kriminelle. Vi vurdere at de fleste angrep spesialisthelsetjenesten står overfor i dag kommer fra opportunistiske kriminelle. Angrep fra organiserte kriminelle som rammer spesialisthelsetjenestens evne til å levere helsetjenester vil kunne påvirke liv og helse, men også redusere befolkningens tillit til at de vil få god og trygg behandling av det offentlige helsevesenet.

Spesialisthelsetjenesten er et ettertraktet og utsatt mål, og vi forventer økt oppmerksomhet fra utpressingsgrupper og deres samarbeidspartnere i kommende periode. Vi vurderer det som **meget sannsynlig** at spesialisthelsetjenesten vil bli utsatt for angrepsforsøk fra organisert kriminalitet og at trusselen er **meget høy**.

6.2 Cyberspionasje

Cyberspionasje handler om å få tilgang til sensitiv informasjon i informasjonssystemer uten å bli oppdaget. For å oppnå dette er det viktig at den tekniske gjennomføringen ikke skaper forstyrrelser i systemet. Hensikten er å etablere en tilgang hvor trusselaktøren kan hente ut informasjon uforstyrret, gjerne over tid. Cyberspionasje gjennomføres i stor grad med samme metoder som andre trusselaktører benytter for å få tilgang til systemer. Den teknologiske utviklingen og digitaliseringen gjør cyberspionasje til den foretrukne metoden for etterretningsvirksomhet [19, 12, 71].

Statlige aktører bruker cyberspionasje for å få tilgang til sensitiv informasjon fra norske virksomheter, og virksomheter som er del av norsk kritisk infrastruktur er særlig utsatt. Cyberspionasje brukes bredt av statlige aktører til etterretningsvirksomhet for å fremme deres militære, diplomatiske og økonomiske mål. Informasjonen som innhentes brukes oftest til etterretningsformål for å bidra til situasjonsforståelse og beslutningstøtte.

KI-teknologier er blitt en driver for teknologiske framskritt i samfunnet. Disse teknologiene, spesielt generativ KI, tilfører imidlertid også trusselaktørene en økt kapabilitet. En organisasjons digitale fotavtrykk kan enkelt og maskinelt benyttes for rekognosering i stor skala. I 2026 forventes det at trusselaktører vil bruke KI til målrettet sosial manipulering mot ansatte i virksomheter [26, 17, 54]. Dette vil gjøre det lettere for trusselaktører å rekruttere menneskelige kilder eller skaffe seg påloggingsinformasjon til systemer ved hjelp av sosial manipulering.

Den største cyberspionasjetrusselen mot spesialisthelsetjenesten kommer fra etterretningsorganisasjoner i Kina og Russland. I 2025 er det observert en økning i forsøk på cyberspionasje fra russiske og kinesiske aktører mot helsesektoren globalt og i Europa [26, 49].

Russland utfører cyberspionasje mot Norge, blant annet for å tilegne seg informasjon som kan gi dem fordeler i en mulig krig mot NATO [2, 19]. Russland har økt søkelys på kartlegging av kritisk infrastruktur og virksomheter som leverer tjenester som understøtter disse funksjonene eller tjenestene. Hensikten med kartleggingen er å identifisere sårbarheter som kan utnyttes ved sabotasje eller i en militær konflikt [5, 19, 12]. Spesialisthelsetjenesten som del av totalforsvaret har en viktig rolle i en militær konflikt, og vil derfor være interessant for russisk etterretning.

Nordområdene er av særlig interesse for Russland, Kina og USA som alle ønsker å øke sin tilstedeværelse i regionen. Amerikanske myndigheter har den siste tiden uttrykt et sterkt behov for å øke sin tilstedeværelse i Arktis, med særlig fokus på Grønland. Arktis har fått større strategisk betydning, noe som er med på å forsterke en allerede spent sikkerhetspolitisk situasjon. Den norske tilstedeværelsen i Arktis gjør at spesialisthelsetjenesten også er mål for spionasje [2, 19, 5].

Kina bruker cyberspionasje for å få tilgang til forskningsdata og teknologi for å fremme landets økonomiske interesser, og utnytter forskingssamarbeid systematisk i sin etterretningsvirksomhet [19]. Kinas kapasitet innen cyberspionasje har økt betraktelig, og de viser en større risikovilje i sin målutvelgelse enn tidligere. Dette kommer av at de har større kapabiliteter til å operere fordekt, økt profesjonalitet og et større system som understøtter

deres operasjoner [19, 49, 48]. Kinesiske trusselaktører har gjennomført cyberspionasjekampanjer mot vestlig helsevesen over tid, og vi forventer at dette også vil kunne ramme spesialisthelsetjenesten i Norge [5, 17, 72].

Statlige aktør har gjennom flere år vist en betydelig interesse for forskningsinstitusjoner. Spesialisthelsetjenesten forvalter store mengder medisinsk forskningsdata, og akademia er en arena hvor ettretningstjenester kan få tilgang til informasjon, menneskelige ressurser, teknologi og laboratorier [19, 73].

Vurdering

Teknologiutviklingen gjør at cyberspionasje kan gjennomføres mer effektivt, i større omfang og med lavere risiko for oppdagelse. Et stadig skiftende trusselbilde og mer bruk av sammensatte virkemidler gjør det vanskelig skille cyberspionasje fra andre typer cyberangrep.

Statlige aktører gjennomfører cyberspionasjekampanjer mot vestlig helsevesen, noe vi tidligere har observert mot spesialisthelsetjenesten i Norge. Vi forventer at spesialisthelsetjenesten i Norge vil være et mål i 2026. Trusselen fra cyberspionasje mot spesialisthelsetjenesten er **høy,** og det er **meget sannsynlig** at spesialisthelsetjenesten vil utsettes for cyberspionasje fra aktører med direkte eller indirekte koblinger til russiske og kinesiske etterretningsorganisasjoner.

6.3 Innsidevirksomhet

I en tid med økende geopolitisk spenning har statlige aktører økt bruken av innsidere for å kunne tilegne seg kunnskap [17]. Dette er gjerne langvarige operasjoner som er vanskelige å avdekke, der angriper bruker lang tid på å etablere en relasjon. Slike operasjoner er ressurskrevende, og som regel forbeholdt trusselaktører med store ressurser og god tid.

Bruk av innsidere er en del av etterretningstrusselen. En innsider kan legge til rette for spionasje eller sabotasje fra innsiden av virksomheten, og bidra til at trusselaktører får tilgang til verdier som er av betydning for nasjonal sikkerhet [7]. Rekrutterte innsidere kan bli bedt om å fremskaffe informasjon om sårbarheter som kan bli utnyttet i fremtidige etterretnings-, påvirknings- og sabotasjeoperasjoner. Personer med tilgang til sensitiv eller gradert informasjon er spesielt utsatte for forsøk på rekruttering [19]. Bruk av innsidere er en del av sammensatt virkemiddelbruk, og i en tid med geopolitisk spenning har statlige aktører økt bruken av innsidere for å få tilgang til informasjon [17].

Rekruttering av kilder er en sentral del av fremmede staters etterretningsvirksomhet, og EOS-tjenestene peker på at fremmede staters etterretningstjenester også i 2026 vil forsøke å rekruttere kilder og medhjelpere i Norge. Flere land bruker både fysiske og digitale virkemidler for å påvirke eller legge press på personer med tilgang til verdifulle data eller kritiske systemer. Helse- og forskningsdata er særlig attraktive mål. Spesialisthelsetjenesten forvalter store mengder sensitiv informasjon. Tilgang til systemer og data kan misbrukes, for eksempel til å identifisere hvor navngitte personer oppholder seg eller til å få innsikt i forskning og kritisk infrastruktur.

Rekruttering og kontaktetablering foregår både i det fysiske og i det digitale rom, men blir i stadig større grad utført via digitale kanaler, for eksempel gjennom sosiale medier. Trusselen er størst fra russiske og kinesiske etterretningstjenester, men også iranske etterretnings- og sikkerhetstjenester bruker menneskelige kilder for å innhente informasjon [19].

I mars 2026 ble det kjent at en iransk legestudent som var ansatt ved Lærdal sykehus i Helse Førde hadde spilt inn en TikTok-video der han truet med å lekke helseopplysninger om navngitte regimemotstandere [74]. Legestudenten hadde i tillegg publisert flere innlegg på sosiale medier der han uttrykte støtte til det iranske regimet. Videoen er spilt inn på sykehuset, og legestudenten er iført norsk helseuniform. Dette eksempelet viser hva konsekvensene av en innsider i spesialisthelsetjenesten kan være, der helseopplysninger ble forsøkt brukt som pressmiddel mot regimemotstandere.

Norske mottiltak og mer årvåkenhet i den norske befolkningen gjør at russiske etterretningstjenester

må finne nye metoder for å innhente informasjon. Som følge av at norske myndigheter siden 2022 har redusert antallet russiske etterretningsoffiserer som er her under diplomatisk dekke, benytter russiske etterretnings- og sikkerhetstjenester i mange tilfeller stedfortredere til å gjennomføre operasjoner, både fysiske og digitale [19, 5]. For informasjonsinnhenting støtter Russland seg blant annet i stor grad på slike stedfortredere uten formell tilknytning til russiske myndigheter [5]. Politiets sikkerhetstjeneste (PST) forventer at Russland i 2026 vil øke sine forsøk på å rekruttere via digitale kanaler. I tillegg vil russiske etterretningsoffiserer under diplomatisk dekke rekruttere kilder og bedrive informasjonsinnhenting.

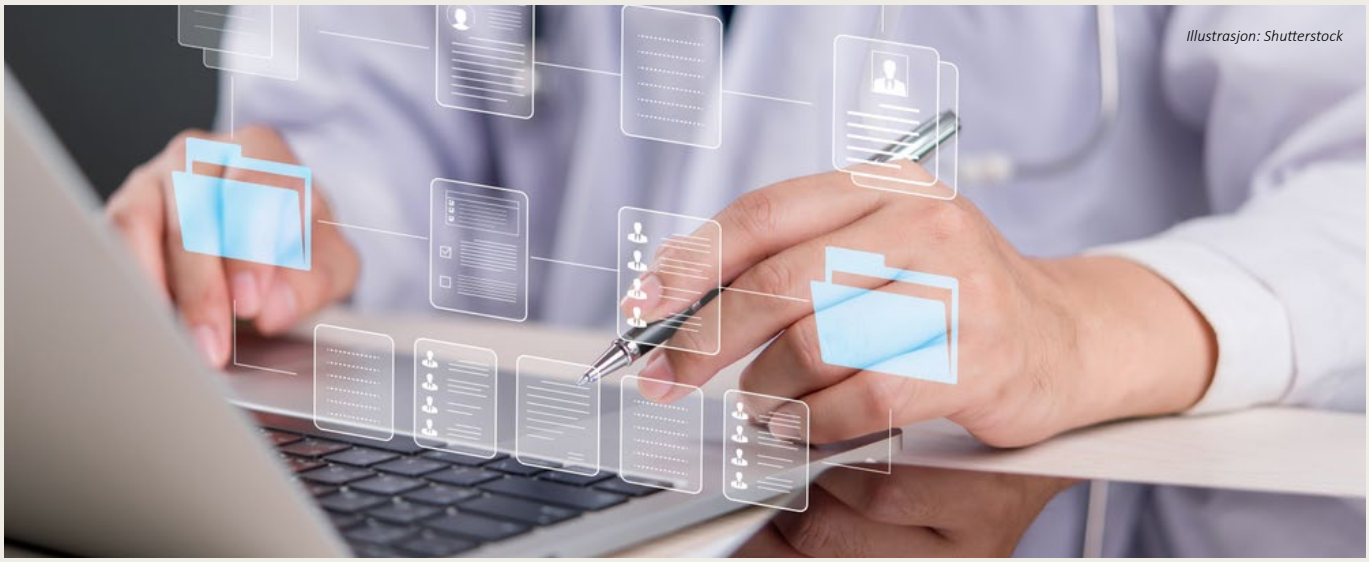
Kinesiske etterretningstjenester har økt evne til å drive etterretningsoperasjoner i Norge, og forsøker å rekruttere norske borgere for å få tilgang til sensitiv og gradert informasjon [19]. Det er også en økende trend at kinesiske etterretningstjenester oppfordrer kildene sine til å rekruttere egne kildenettverk, det vil si at personer rekrutteres indirekte for eksempel via sosiale medier. Denne trenden bidrar til å øke kinesiske etterretningstjenesters kapasitet til å innhente informasjon gjennom menneskelige kilder.

PST skriver i sin nasjonale trusselvurdering for 2026 at effektiv sosial manipulering var et sentralt element i vellykkede cyberoperasjoner i 2025. Ett eksempel på digital rekruttering ved bruk av sosial manipulering er Nord-Koreas "DreamJob"-kampanjer, som er en form for sosial manipulering. Teknikken brukes også av andre land, slik som Iran, og av organiserte cyberkriminelle. Rekrutteringsforsøket starter med at en ansatt kontaktes gjennom sosiale medier, for eksempel LinkedIn, med et tilbud om en god jobb. Formålet med operasjonen er ikke den ansatte i seg selv, men å få kontroll på et endepunkt som gir tilgang inn i virksomheten. Operasjoner som bruker denne teknikken retter seg ofte mot IT-arbeidere slik som utviklere og prosjektledere [75]. Spesialisthelsetjenesten har mange ansatte med slike roller, og vi kan være utsatt selv om vi så langt ikke har sett teknikken brukt mot oss.

Vurdering

Helsedata er et attraktivt mål, og er en årsak til at helse- og omsorgssektoren er interessant for trusselaktører. Spesialisthelsetjenesten er en sentral aktør i totalforsvaret og råder i tillegg over verdier med betydning for nasjonal sikkerhet. Vi vurderer at dette samlet sett gjør spesialisthelsetjenesten til et attraktivt mål for trusselaktører, som vil kunne ha stor nytte av å plassere innsidere i spesialisthelsetjenesten.

Innhenting av informasjon gjennom rekruttering av innsidere utgjør en **høy** trussel mot spesialisthelsetjenesten. Dette gjør at vi vurderer det som **sannsynlig** at spesialisthelsetjenesten vil bli utsatt for innsidevirksomhet.



Illustrasjon: Shutterstock

6.4 Destruktive cyberangrep og sabotasje

Destruktive cyberangrep er digitale angrep hvor hensikten er å ødelegge eller endre informasjon, data, programvare eller maskinvare. Et angrep kan ha omfattende konsekvenser for tjenestene som leveres. Et eksempel på et destruktive cyberangrep er wiper-angrep som sletter data. Dataene er da tapt, og kan ikke gjenopprettes. Dette skiller seg fra utpressingsangrep hvor filene blir kryptert og den som blir utsatt for angrepet kan få gjenopprettet filene. Wiper-angrep er blitt brukt av russiske trusselaktører i Ukraina, men også mot andre land i regionen. I krigen i Ukraina er det flere eksempler på hvordan destruktive angrep brukes i kombinasjon med andre fysiske virkemidler [17].

Den 29. desember 2025 ble det gjennomført et destruktivt cyberangrep mot en av Polens kombinerte varme- og kraftanlegg med kjøring av wiper-skadevare. Målet med angrepet var irreversibel ødeleggelse av data lagret på enheter innenfor organisasjonens interne nettverk. Aktøren innledet angrepet etter å ha infiltrert nettverket og etablert fotfeste over tid, noe som ga dem tilgang til sensitiv informasjon. Dette resulterte i at aktøren fikk til gang til privilegerte kontoer i Active Directory-domenet, noe som igjen som muliggjorde ubegrenset lateral bevegelse i organisasjonens systemer. Imidlertid ble angrepet stoppet av EDR-løsningen til virksomheten som blokkerte angrepet [76].

Sabotasje er å fysisk skade eiendom, produksjonsmiljøer eller tekniske systemer med hensikt, og er et effektivt sammensatt virkemiddel. Formålet kan være å ødelegge infrastruktur for å øke effekten av militære operasjoner eller påvirke politiske beslutninger.

Destruktive cyberangrep og sabotasje kan ramme spesialisthelsetjenesten eller andre samfunnsviktige funksjoner indirekte eller direkte. Destruktive cyberangrep og sabotasje kan føre til betydelig skade på fysiske objekter eller personer. Både Russland, Iran og Nord-Korea benytter destruktive cyberangrep som et virkemiddel mot andre land [2, 5, 19, 12].

6.4.1 Destruktive cyberangrep

Flere trusselaktører har kapasitet til å gjennomføre destruktive cyberangrep mot spesialisthelsetjenesten, men viljen til å gjennomføre slike angrep vil variere ut fra strategiske målsetninger. De siste årene har bekymringen i Europa for å bli rammet av destruktive cyberangrep og sabotasje økt. Det er flere eksempler på slike angrep, både fysiske og digitale. Russlands risikovilje knyttet til bruk av sammensatte virkemidler, inkludert destruktive cyberangrep og sabotasje av kritisk infrastruktur, har økt [19, 53, 26].

Siden 2023 har russiskstøttede hacktivistgrupper gjennomført destruktive cyberangrep mot vestlig kritisk infrastruktur. Felles for målene er at de har hatt et lavt modenhetsnivå innen sikkerhet, og virksomhetene har hatt få tiltak for å beskytte seg mot cyberangrep [2]. Russlands bruk av destruktive cyberangrep i krigen i Ukraina viser tydelig intensjon om og kapasitet til å lamme kritisk infrastruktur og kritiske samfunnsfunksjoner [2, 19].

I mars 2026 ble det kjent at selskapet Stryker var utsatt for et datainnbrudd. Angriperne hevder at de stjal store mengder data fra Strykers systemer, og brukte innebygd funksjonalitet for å slette data fra enheter tilkoblet Strykers Windows-miljø. Stryker leverer MTU og programvare til norske sykehus.

Angrepet ble utført av en iransk gruppe som antas å være knyttet til iransk etterretning. I en uttalelse sa gruppen at motivasjonen for angrepet var hevn for et missilangrep mot en jenteskole i Iran i februar 2026 [77].

Det ble også i 2025 oppdaget kinesiske aktører som hadde forhåndsposisjonert seg i kritisk infrastruktur i vestlige land, og de har også vist interesse for norske virksomheter [19, 12]. Intensjon er å kunne gjennomføre destruktive cyberangrep på et senere tidspunkt ved behov [12, 72, 78]. Flere land planlegger for å kunne benytte destruktive og forstyrrende cyberangrep som virkemidler i en konflikt. Vi forventer at statlige aktører forhåndsposisjonerer seg i europeisk infrastruktur [19, 12].

Irans regjering, og andre cyberaktører som sympatiserer med iranske interesser, har gjennomført angrep mot eller forhåndsposisjonering i land som har gitt støtte til Israel under krigen på Gaza [26]. Imidlertid er iranske trusselaktører i større grad opportunistiske i sine cyberangrep [19]. Det har vært rapportert at iranske trusselaktører har operert i Norge. Krigen i Iran har vist at datasentre er blitt strategiske mål i en militær konflikt [79, 80].

6.4.2 Sabotasje

Det har vært en økning i antall sabotasjeaksjoner mot europeisk infrastruktur de siste to årene. Angrepene er blitt sett i sammenheng med leveranser til krigen i Ukraina [19]. Russiske etterretningstjenester har vist økt risikovilje, og bruker gjerne proxy-aktører[13] for å gjennomføre angrep [2, 5, 19]. Dette gjør det vanskeligere å identifisere trusselaktørene, og operasjonene kan fornektes. Rekrutteringen skjer ofte på sosiale medier, og gjerningspersonene er i mange tilfeller ikke klar over at de arbeider for en russisk etterretningstjeneste [2]. Russland har derfor kun delvis kontroll over sabotørene. Angrepene har gjerne vært relativt enkle å utføre [2, 5, 19].

Etterretningsoperasjoner som kartlegging av fysisk og digital infrastruktur, er en trussel mot kritisk infrastruktur i nord. Dette kan innebære alle former for etterretningsaktivitet, inkludert innsidetrussel og rekruttering av personell [53]. Spesialisthelsetjenesten har flere lokasjoner i viktige knutepunkter mellom Norge, Finland og Sverige. Infrastruktur på tvers av landegrensene mellom Norge, Sverige og Finland er særlig utsatt for kartlegging og sabotasje fra russiske aktører [5, 19, 53].

Som del av totalforsvaret, og som leverandør av helsetjenester til forsvarspersonell og til NATO-allierte, må spesialisthelsetjenesten være forberedt på økt etterretningstrussel mot egen infrastruktur eller infrastruktur som understøtter vår virksomhet, særlig fra russisk side [19]. Nordområdene blir hyppigere besøkt av NATO-allierte, og det er en nasjonal styrking av Forsvaret nasjonalt når det gjelder materiell, men også gjennom økt tilstedeværelse og øvingsaktivitet i regionen.

I forbindelse med at det amerikanske hangarskipet USS Gerald Ford seilte i Nord-Norge, landet et amerikansk helikopter på UNN i Tromsø. Under landingen ble en kvinne observert da hun tok bilder av helikopteret. Denne typen interesse skaper bekymring for at statlige aktører driver kartlegging av aktivitet mot samfunnskritiske tjenester [81]. Spesialisthelsetjenesten leverer også tjenester på Svalbard, som det siste året har fått økt oppmerksomhet med tanke på den sikkerhetspolitiske situasjonen i Arktis.

Målene for sabotasjeaksjonene har primært vært eiendom og logistikkinfrastruktur, men også annen sivil infrastruktur er blitt rammet. Europeiske etterretnings- og sikkerhetstjenester har trukket fram kritisk infrastruktur, spesielt innen energi, som aktuelle mål for denne typen aksjoner [19, 5, 12, 2, 53].

Vurdering

Russland og Kina har meget høy kapasitet til å gjennomføre destruktive cyberangrep og sabotasje. Den sikkerhetspolitiske situasjonen i verden bidrar til at statlige aktører har økt vilje til å bruke slike sammensatte virkemidler. Spesialisthelsetjenesten kan rammes direkte som følge av målrettede angrep, eller indirekte som følge av angrep rettet mot kritisk infrastruktur som spesialisthelsetjenesten er avhengig av.

Trusselen fra destruktive cyberangrep og sabotasje mot spesialisthelsetjenesten er **moderat**, og det er **mulig** at slike angrep vil kunne ramme spesialisthelsetjenesten direkte eller indirekte i 2026.

[13]Proxy-aktører er personer eller grupperinger som handler på vegene av en fremmedstats, uten direkte eller formell tilknytting for å utføre oppdrag som spionasje eller sabotasje.

Illustrasjon: Sykehuspartner HF

6.5 Hacktivisme

Hacktivisme-angrep mot Norge økte kraftig i omfang etter Russlands eskalering av krigen mot Ukraina i februar 2022. I kjølvannet av invasjonen dukket det opp flere tilsynelatende uavhengige pro-russiske hacktivistgrupper som ville komme med sitt bidrag i kampen mot Ukraina og Vesten. De fleste gruppene benyttet tjenestenektangrep, mens noen få – ofte med knytning til russisk etterretning – benyttet såkalte hack-and-leak-taktikker[14] [82]. Russland har fått hackere til å lekke følsom informasjon for å sette personer eller organisasjoner i et dårlig lys [2]. Kompromittering eller lekkasje av helsedata vil kunne skade befolkningens tillit til spesialisthelsetjenesten.

Et norsk damanlegg ble angrepet 7. april 2025. Det ble oppdaget en uautorisert fjerntilgang til ventilenes styringssystem ved anlegget. Ventilen ble åpnet til hundre prosent, og tilgangen varte i underkant av fire timer. Angrepet ble gjennomført av en prorussisk hacktivistgruppe, og PST konkluderte med at det var en russisk statlig aktør som sto bak. Slike angrep illustrerer kapasitet og vilje til å ramme tjenester som styrer fysiske komponenter. Bekymringen er at slike angrep også kan ramme spesialisthelsetjenesten [12].

Det var et paradigmeskifte i trusselen fra hacktivistangrep i 2025. Flere pro-russiske hacktivistgrupper begynte å angripe internetteksponerte OT-systemer der de fikk tilgang til systemer og gjorde endringer som kunne få fysiske konsekvenser. For å demonstrere tilgangen sin, publiserte gruppene bilder og videoer av at de hadde logget inn på systemer og gjennomført endringer.

Spesialisthelsetjenesten har forskjellige typer OT-systemer, herunder byggteknisk utstyr (BTU) og medisinskteknisk utstyr (MTU). Disse har de samme svakhetene som OT-utstyr generelt: svake autentiseringsløsninger, kompliserte oppdateringsrutiner og komplekse godkjenningskrav. BTU og MTU utvider angrepsflaten vår betraktelig, også for angrep fra hacktivistgrupper.

Vi vurderer at hacktivistene som står bak disse angrepene opererer opportunistisk og angriper enkle mål, slik som dårlig sikrede internetteksponerte systemer. Konsekvensene av et vellykket angrep kan likevel være alvorlige, noe angrepet på dansk vannforsyning i desember 2024 og norsk damanlegg i 2025 demonstrerte [83, 84].

Når en gruppe angriper et OT-system utnytter de systemtilgangen til å gjøre så mye skade som mulig, for eksempel ved å endre verdier eller starte og stoppe prosesser [85]. Konsekvensene kan være at de åpner eller lukker ventiler i for eksempel damanlegg, fyringskjeler eller vannrør. Hacktivister viser med dette en større vilje til å gjennomføre operasjoner som får fysiske konsekvenser enn andre kategorier av trusselaktører.

Blant de pro-russiske hacktivistene ser vi få tegn til at spesifikke land prioriteres over andre annet enn i korte perioder. Målutvelgelsen begrunnes gjerne i en oppfattelse av at det er en generell anti-russisk holdning i Vesten. Etter mai 2025 blir det ofte hevdet av gruppene selv at angrep er hevn for en koordinert Europol-operasjon kalt Operation Eastwood [86]. Dette var en koordinert operasjon for å arrestere medlemmer av en hacktivistgruppe [87]. Selv om Norge ikke deltok i operasjonen, brukes den som begrunnelse for hacktivismeangrep mot norske mål.

Etter starten av USA og Israels krig mot Iran i februar 2026 økte pro-iranske hacktivistgrupper aktiviteten sin mot amerikanske og israelske mål. Flere pro-russiske grupper erklærte sin støtte til Iran, og økte fokus mot de samme landene.

Vurdering

Det har ikke vært hacktivistangrep rettet direkte mot spesialisthelsetjenesten i foregående periode. Vi har imidlertid sett økt aktivitet fra hacktivister mot kritisk infrastruktur i Norge og Europa, og vurderer trusselen fra hacktivisme mot spesialisthelsetjenesten som **moderat**. Med bakgrunn i den geopolitiske situasjonen vurderer vi at angrep er **mulig.**

[14]Kompromittering av virksomheter og påfølgende lekkasje av data.

REFERANSER

[1] Statsministerens kontor, «Nasjonal sikkerhetsstrategi,» 2025.

[2] Forsvarets Efterretningstjeneste, «UDSYN,» 2025.

[3] Helse- og omsorgsdepartementet, «Meld. St. 5 (2023-2024) En motstandsdyktig helseberedskap- Fra pandemi til krig i Europa,» 2023.

[4] Forsvarsdepartementet, «NOU 2023: 14 Forsvarskommisjonen av 2021- Forsvar for fred og frihet,» 2023.

[5] Etterretningstjenesten, «Fokus,» 2026.

[6] J. C. Bergaust, F. Skjei og S. R. Sellevåg, «Hva kan Norge lære av andre lands tilnærming til sammensatte trusler?- rapport til Forsvarskommisjonen,» FFI, 2022.

[7] Justis- og beredskapsdepartementet, «Meld. St. 9 (2024-2025) Totalberedskapsmeldingen- Forberedt på kriser og krig,» 2025.

[8] Justis- og beredskapsdepartementet, «NOU 2023: 17 Nå er det alvor- Rustet for en usikker fremtid,» 2023.

[9] Helse- og omsorgsdepartementet, «Meld. St. 9 (2023-2024) Nasjonal helse- og samhandlingsplan 2024-2027,» 2024.

[10] NSM, «Risiko,» 2025.

[11] NSM, «Risiko,» 2024.

[12] NSM, «Risiko,» 2026.

[13] Spesialisthelsetjenesten, «Trusselvurdering 2025- Det digitale trusselbildet mot spesialisthelsetjenesten,» 2025.

[14] H. Farrell og A. Newman, Underground Empire: How America Weaponized the World Economy, 2023.

[15] O. Lysne, M. A. Riegler, T. Cicic og H. Bryhni, «Microsoft-blokaden bør vekke Norge,» Dagens Næringsliv, 1. juni 2025. [Internett]. Available: https://www.dn.no/innlegg/teknologi/sikkerhetspolitikk/geopolitikk/microsoft-blokaden-bor-vekke-norge/2-1-1826417.

[16] C. Bessing, «Bill Gates om USAs bruk av teknologi mot Europa: – Inntil nylig var jeg sikker på at det ikke ville skje,» DIGI, 30. januar 2026. [Internett]. Available: https://www.digi.no/artikler/bill-gates-om-usas-bruk-av-teknologi-mot-europa-inntil-nylig-var-jeg-sikker-pa-at-det-ikke-ville-skje/567640.

[17] Microsoft, «Microsoft Digital Defense Report,» 2025.

[18] Kripos, «Cyberkriminalitet,» 2026.

[19] PST, «Nasjonal trusselvurdering,» 2026.

[20] NSM, «Temarapport- Innsiderisiko,» 2020.

[21] Spesialisthelsetjenesten, «Trusselvurdering 2024- Det digitale trusselbildet mot spesialisthelsetjenesten,» 2024.

[22] Helse- og omsorgsdepartementet, «Prop. 152 L (2024-2025) Endring i helselovgivningen,» 2025.

[23] PST, «Nasjonal trusselvurdering,» 2024.

[24] Anthropic, «Threat Intelligence Report: August 2025,» 2025.

[25] OpenAI, «Disrupting malicious uses of AI: an update,» 2025.

[26] CrowdStrike, «Global Threat Report,» 2026.

[27] CERT-UA, «UAC-0001 cyberattacks on the security and defense sector using the LAMEHUG software tool, which uses LLM (large language model) (CERT-UA#16039),» 17. juli 2025. [Internett]. Available: https://cert.gov.ua/article/6284730.

[28] Google Threat Intelligence Group, «GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use,» 12. februar 2026. [Internett]. Available: https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use/.

[29] Google Threat Intelligence Group, «GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools,» 5. november 2025. [Internett]. Available: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools.

[30] B. Singer, K. Lucas, L. Adiga, M. Jain, L. Bauer og V. Sekar, «Incalmo: An Autonomous LLM-assisted System for Red Teaming Multi-Host Networks,» 2025.

[31] Mandiant, «M-Trends,» 2025.

[32] Check Point, «Unveiling VoidLink – A Stealthy, Cloud-Native Linux Malware Framework,» 13. januar 2026. [Internett]. Available: https://research.checkpoint.com/2026/voidlink-the-cloud-native-malware-framework.

[33] Check Point, «VoidLink: Evidence That the Era of Advanced AI-Generated Malware Has Begun,» 20. januar 2026. [Internett]. Available: https://research.checkpoint.com/2026/voidlink-early-ai-generated-malware-framework/.

[34] DARPA, «AIxCC- AI Cyber Challenge,» [Internett]. Available: https://aicyberchallenge.com/. [Funnet april 2026].

[35] Anthropic, «Making frontier cybersecurity capabilities available to defenders,» 20. februar 2026. [Internett]. Available: https://www.anthropic.com/news/claude-code-security.

[36] Big Sleep team, «From Naptime to Big Sleep: Using Large Language Models To Catch Vulnerabilities In Real-World Code,» Google Project Zero, 1. november 2024. [Internett]. Available: https://projectzero.google/2024/10/from-naptime-to-big-sleep.html.

[37] OpenAI, «Introducing Aardvark: OpenAI's agentic security researcher,» 30. oktober 2025. [Internett]. Available: https://openai.com/index/introducing-aardvark/.

[38] S. Heelan, «On the Coming Industrialisation of Exploit Generation with LLMs,» 18. januar 2026. [Internett]. Available: https://sean.heelan.io/2026/01/18/on-the-coming-industrialisation-of-exploit-generation-with-llms/.
[39] Anthropic, «Assessing Claude Mythos Preview's cybersecurity capabilities,» 7. april 2026. [Internett]. Available: https://red.anthropic.com/2026/mythos-preview/.
[40] National Institute of Standards and Technology, «Module-Lattice-Based Digital Signature Standard,» 2024.
[41] National Institute of Standards and Technology, «Module-Lattice-Based Key-Encapsulation Mechanism Standard,» 2024.
[42] National Institute of Standards and Technology, «Stateless Hash-Based Digital Signature Standard,» 2024.
[43] H. Adkins og S. Schmieg, «Quantum frontiers may be closer than they appear,» Google, 25. mars 2026. [Internett]. Available: https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/.
[44] IonQ, «IonQ's Accelerated Roadmap: Turning Quantum Ambition into Reality,» 13. juni 2025. [Internett]. Available: https://www.ionq.com/blog/ionqs-accelerated-roadmap-turning-quantum-ambition-into-reality.
[45] IBM, «The future of computing is quantum-centric,» [Internett]. Available: https://www.ibm.com/roadmaps/quantum/. [Funnet 14. april 2026].
[46] Kripos, «Cyberkriminalitet,» 2025.
[47] Mandiant, «M-Trends,» 2026.
[48] CrowdStrike, «Global Threat Report,» 2025.
[49] AIVD and MIVD, «AIVD and MIVD identify new Russian cyber threat actor,» 2025.
[50] Cyber Safety Review Board, «Review of the Summer 2023 Microsoft Exchange Online Intrusion,» 2024.
[51] AVID, «Annual Report 2024,» 2025.
[52] D.-j. Mollema, «One Token to rule them all- obtaining Global Admin in every Entra ID tenant via Actor tokens,» 17. september 2025. [Internett]. Available: https://dirkjanm.io/obtaining-global-admin-in-every-entra-id-tenant-with-actor-tokens/.
[53] Telenor, «Digital sikkerhet,» 2025.
[54] Styrelsen for Samfundssikkerhed, «Cybertruslen mod Danmark,» 2025.
[55] C. Dupuis og Q. Laplanche, «Security that moves fast: Docker's response to Shai Hulud 2.0,» Docker, 2025. [Internett]. Available: https://www.docker.com/blog/security-that-moves-fast-dockers-response-to-shai-hulud-2-0/.
[56] O. P. B. Stokke, «Digert angrep: Shai-Hulud stjeler hemmelig¬hetene dine,» kode24, 2025. [Internett]. Available: https://www.kode24.no/artikkel/digert-angrep-shai-hulud-stjeler-hemmelighetene-dine/250162.
[57] Notepad++, «Notepad++ Hijacked by State-Sponsored Hackers,» 2. februar 2026. [Internett]. Available: https://notepad-plus-plus.org/news/hijacked-incident-info-update/.
[58] Google Threat Intelligence Group, «Hello 0-Days, My Old Friend: A 2024 Zero-Day Exploitation Analysis,» 29. april 2025. [Internett]. Available: https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends.
[59] Google Threat Intelligence Group, «Look What You Made Us Patch: 2025 Zero-Days in Review,» 5. mars 2026. [Internett]. Available: https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review.
[60] Mandiant, «How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends,» 15. oktober 2024. [Internett]. Available: https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023.
[61] GreyNoise, «Mass Internet Exploitation in 2024: A Rapidly Escalating Threat,» 2025.
[62] M. Meltzer, R. J. Mora, S. Koessel, S. Adair og T. Lancaster, «Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN,» Volexity, 10. januar 2024. [Internett]. Available: https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/.
[63] Health Sector Cybersecurity Coordination Center, «HC3: Sector Alert- ClickFix Attacks,» 2024.
[64] ESET, «Threat Report- H1 2025,» 2025.
[65] Mimecast, «The Global Threat Intel Report,» 2025.
[66] Proofpoint, «The Human Factor 2025- Vol. 2 Phishing and URL-Based Threats,» 2025.
[67] Proofpoint, «Around the World in 90 Days: State-Sponsored Actors Try ClickFix,» 17. april 2025. [Internett]. Available: https://www.proofpoint.com/us/blog/threat-insight/around-world-90-days-state-sponsored-actors-try-clickfix.
[68] CERT-UA, «Cyberattack UAC-0001 (APT28): PowerShell command in the clipboard as "entry point" (CERT-UA#11689),» 25. oktober 2024. [Internett]. Available: https://cert.gov.ua/article/6281123.
[69] N. Huq og D. Sanycho, «From LinkedIn to Tailored Attack in 30 Minutes- How AI Accelerates Target Profiling for Cybercrime,» Trend Micro, 23. februar 2026. [Internett]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/from-linkedin-to-tailored-attack-in-30-minutes-how-ai-accelerates-target-profiling-for-cybercrime.
[70] Sopra Steria, «State of Cyber Security,» 2026.

[71] D. V. Gioe og T. Manganello, «Smart new world: adapting human intelligence for the digital age,» Intelligence and National Security, 21. oktober 2025.
[72] CISA, «Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System,» 2025.
[73] Office of the Director of National Intelligence, «Annual Threat Assessment of the U.S. Intelligence Community,» 2025.
[74] NRK, «Truet iranere på TikTok fra norsk sykehus,» 12. mars 2026. [Internett]. Available: https://www.nrk.no/norge/truet-iranere-pa-tiktok-fra-norsk-sykehus-1.17797711.
[75] [PST, «Nordkoreanske IT-arbeidere er fordekt ansatt i norske bedrifter,» 2026.
[76] CERT Polska, «Energy Sector Incident Report- 29 December,» 2025.
[77] A. J. Vicens og C. Santhosh, «Iran-linked hackers claim responsibility for attack on US medical device maker Stryker,» Reuters, 11. mars 2026. [Internett]. Available: https://www.reuters.com/technology/stryker-shares-fall-after-report-suspected-iran-linked-cyberattack-2026-03-11/.
[78] Department of Homeland Security, «Homeland Threat Assessment,» 2025.
[79] Reuters, «Amazon's cloud business in Bahrain damaged in Iran strike, FT reports,» 1. april 2026. [Internett]. Available: https://www.reuters.com/world/middle-east/amazons-cloud-business-bahrain-damaged-iran-strike-ft-reports-2026-04-01/.
[80] I. Strümke, «Datasentre er som våpenfabrikker,» Aftenposten, 12. april 2026. [Internett]. Available: https://www.aftenposten.no/meninger/kommentar/i/Pdgy86/inga-strumke-datasentre-er-som-vaapenfabrikker.
[81] NRK, «Advarer etter at person tok bilder av militærhelikopter på sykehus,» 22. september 2025. [Internett]. Available: https://www.nrk.no/tromsogfinnmark/ansatte-ved-unn-blir-bedt-om-a-se-opp-for-mistenkelig-aktivitet_-_-vaer-arvaken-1.17580460.
[82] CISA, «Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure,» 2025.
[83] NRK, «PST mener prorussiske hackere stod bak sabotasje – henlegger likevel saken,» 3. oktober 2025. [Internett]. Available: https://www.nrk.no/vestland/pst-mener-prorussisk-hackergruppe-stod-bak-dam-sabotasje-pa-vestlandet-og-datainnbrudd-pa-ostlandet-1.17587446.
[84] J. Røstum, R. Aalstad og G. A. Johansen, «Hackere kan angripe drikkevannet ditt,» SINTEF, 4. august 2025. [Internett]. Available: https://www.sintef.no/siste-nytt/2025/hackere-kan-angripe-drikkevannet-ditt/.
[85] Helse- og kommuneCERT, «Tertialsbrief T3 2025,» 2025.
[86] Helse- og kommuneCERT, Intern kilde, 2025.
[87] Europol, «Global operation targets NoName057(16) pro-Russian cybercrime network,» [Internett]. Available: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network. [Funnet 10. april 2026].
[88] Justis- og beredskapsdepartementet, «Meld. St. 5 (2020-2021) Samfunnssikkerhet i en usikker verden,» 2020.
[89] Helse- og kommuneCERT, «Verdikjedeangrep,» [Internett]. Available: https://www.nhn.no/tjenester/helsecert/publikasjoner/verdikjedeangrep.
[90] Mandiant, «Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm,» 17. april 2024. [Internett]. Available: https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.
[91] Proofpoint, «The 2025 Study on Cyber Insecurity in Healthcare- The cost and impact on patient safety and care,» 2025.
[92] L. Aanes og J. Skjelsbæk, «DNB utsatt for sofistikert deepfake-angrep,» BankShift, 3. februar 2025. [Internett]. Available: https://www.bankshift.no/nyheter/dnb-utsatt-for-sofistikert-deepfake-angrep/375139.