Trusselvurdering 2025

Det digitale trusselbildet mot spesialisthelsetjenesten

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

Innhold

Innledning

Spesialisthelsetjenesten forvalter store verdier, blant annet personopplysninger, helseopplysninger og forskningsdata. Dette gjør at spesialisthelsetjenesten tiltrekker seg oppmerksomhet fra svært avanserte trusselaktører. Flere av helseforetakene er underlagt sikkerhetsloven, og understøtter den grunnleggende nasjonale funksjonen helseberedskap.

Helsevesenet er avhengig av informasjonsteknologi for å effektivt yte helsetjenester. Et vellykket cyberangrep mot spesialisthelsetjenesten kan medføre store konsekvenser for evnen til å yte helsetjenester og evnen til å ivareta helseberedskapen. Denne trusselvurderingen tar for seg de mest relevante digitale truslene mot spesialisthelsetjenesten, og hvordan disse kan påvirke spesialisthelsetjenestens verdier.

Etterretnings- og sikkerhetstjenestene (EOS-tjenestene) understreker at sikkerhetssituasjonen i Norge er mer krevende enn på lenge. Verden er inne i en periode med stor geopolitisk ustabilitet som skaper usikkerhet rundt det etablerte vestlige økonomiske og sikkerhetspolitiske samarbeidet. Dette kan føre til større endringer i maktbalansen i verden, noe som kan medføre at trusselaktørenes målutvelgelse raskt endres.

Totalforsvaret er den gjensidige støtten og samarbeidet mellom sivil og militær side i fred, krise og krig. Spesialisthelsetjenesten spiller en viktig rolle i dette samarbeidet. God kontroll på verdier og funksjoner med et særskilt beskyttelsesbehov er derfor avgjørende.

Longyearbyen sykehus. Foto: Helse Nord IKT

Hovedvurderinger

Trusselen mot spesialisthelsetjenesten fra **organisert cyberkriminalitet** er **meget høy**

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. Vi vurderer at spesialisthelsetjenesten er et ettertraktet og utsatt mål, og vi forventer økt oppmerksomhet fra utpressingsgrupper og deres samarbeidspartnere i kommende periode.

Trusselen mot spesialisthelsetjenesten fra **cyberspionasje** er **høy**

Teknologiutviklingen gjør at cyberspionasje og etterretningsvirksomhet kan gjennomføres mer effektivt, i et større omfang og med lavere risiko. Trusselbildet er komplekst og uoversiktlig, noe som gjør det vanskelig å skille cyberspionasje fra andre typer cyberangrep. Russland og Kina er de mest fremtredende truslene mot spesialisthelsetjenesten.

Trusselen mot spesialisthelsetjenesten fra **innsidevirksomhet** er **høy**

Spesialisthelsetjenesten er definert som ett av målene til statlige trusselaktører, og vi ser en økning i jobbsøkere fra høyrisikoland[1] i flere av våre helseforetak. Innsidevirksomhet må ses i sammenheng med trusselen fra cyberspionasje, og statlige aktørers intensjon om å benytte menneskelige kilder som virkemiddel.

Trusselen mot spesialisthelsetjenesten fra **destruktive cyberangrep og sabotasje** er **moderat**

Som følge av den spente sikkerhetspolitiske situasjonen i verden er det en økt trussel for destruktive cyberangrep og sabotasje. Russland og Kina har meget høy kapasitet til å gjennomføre destruktive cyberangrep og sabotasje mot spesialisthelsetjenesten. Spesialisthelsetjenesten kan rammes direkte som følge av målrettede angrep, eller indirekte som følge av angrep rettet mot kritiske samfunnsfunksjoner vi er avhengige av.

Trusselen mot spesialisthelsetjenesten fra **påvirkningsoperasjoner** er **lav**

Spesialisthelsetjenesten kan rammes av både målrettede påvirkningsoperasjoner og generelle påvirkningsoperasjoner mot det norske samfunnet. Trusselen kan endre seg raskt ved fremtidige helsekriser eller som følge av endringer i den geopolitiske situasjonen.

Trusselen mot spesialisthelsetjenesten fra **hacktivisme** er **lav**

Det er ikke observert hacktivisme-aktivitet mot spesialisthelsetjenesten det siste året, og denne typen trusselaktør har ikke vist nevneverdig interesse for norske virksomheter i 2024. Økte geopolitiske spenninger, mer bruk av hacktivisme som statlig virkemiddel og et mer dynamisk trusselbilde har tidligere vist at dette fort kan endre seg.

1 Høyrisikolandene som er nevnt i EOS-tjenestenes åpne trusselvurderinger.

Usikkerhet i det sikkerhets-politiske samarbeidet

Verden er inne i en periode med stor geopolitisk ustabilitet. Spenningen mellom Russland og Kina på den ene siden og Vesten på den andre siden har økt, og den norske Etterretningstjenesten anser at den vil fortsette å øke også i 2025 [1]. I tillegg viser USA at de ikke vil videreføre det stabile og forutsigbare frihandelsbaserte økonomiske samarbeidet som ble etablert etter andre verdenskrig, blant annet ved å innføre høye tollsatser. Dette skaper usikkerhet når det gjelder det etablerte vestlige økonomiske og sikkerhetspolitiske samarbeidet. Handelspolitikk er blitt et viktigere virkemiddel i det stormaktspolitiske spillet, også mellom allierte.

Norske myndigheter anbefaler å vurdere teknologi- og leverandørvalg i et strategisk perspektiv [2]. Nasjonal sikkerhetsmyndighet (NSM) har de siste fire årene advart mot konsentrasjonsrisikoen, det vil si risikoen for å bli avhengig av enkeltland eller enkeltleverandører, i anskaffelser [3, 4, 5, 6]. Dette kan oppstå ved flere eller store anskaffelser fra samme land eller leverandør. En slik avhengighet kan utnyttes til å utøve press og påvirkning [4].

Spesialisthelsetjenesten er svært avhengig av amerikanske tjenester og produkter, både i sky og lokalt. Det er derfor viktig å være oppmerksom på utviklingen i det sikkerhetspolitiske samarbeidet med allierte, og være bevisst på konsentrasjonsrisikoen. I tillegg er det regulatoriske samarbeidet med USA blitt mer uforutsigbart. Norske myndigheter anbefaler at virksomheter har en strategi for hva de skal gjøre dersom personopplysninger ikke lenger kan overføres til USA etter den samme avtalen [2]. Når teknologileverandør og leverandørkjede er utenfor nasjonal kontroll, er det særlig viktig å vurdere om det finnes alternativer.

Haukåsen radar. Foto: Christopher Lindseth Moen.

Begreper

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. Aktøren har kapasitet, intensjon og/eller planer om å gjennomføre et angrep.
Moderat	En generell trussel eksisterer. Aktøren 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.

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 %

Kildegrunnlaget til denne vurderingen er basert på observerte og rapporterte hendelser, og åpne rapporter og trusselvurderinger. Vurderingene er basert på informasjon innhentet frem til 22. april 2025 og må forstås deretter. Tidsperspektivet for vurderingene er ett år fra rapporten publiseres.

KAPITTEL 1

Trusselaktører

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

1.1 Organiserte kriminelle aktører

Organiserte kriminelle aktører består av flere undergrupper som 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. Organiserte kriminelle aktører er ofte mindre opptatt av hvem de rammer, fordi motivet er økonomisk. Den teknologiske utviklingen har bidratt til økt effektivitet og profesjonalitet i cyberangrep utført av disse aktørene.

1.2 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.

Statlige aktører kan også utføre destruktive angrep og forhåndsposisjonere seg i kritisk infrastruktur med henblikk på mulige fremtidige cyberoperasjoner. De bruker også påvirkningsoperasjoner som virkemiddel, gjerne i forbindelse med viktige demokratiske prosesser. Hensikten er å forsøke å destabilisere samfunn de oppfatter som fiendtlige.

De største statlige aktørene som er aktive mot Norge er Russland og Kina. EOS-tjenestene beskriver disse som en vedvarende cybertrussel i 2025 [1, 4, 7].

1.3 Hacktivister

Hacktivister kan være enkeltpersoner eller grupper som utfører digitale angrep for å formidle politiske eller ideologiske budskap. For en hacktivist er ofte 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.

Statlige eller andre mektige aktører kan utgi seg for å være hacktivister. Hensikten med å gjøre dette er å kunne nekte for innblanding i gitte situasjoner, eller for å kamuflere annen aktivitet, som kartlegging eller inntrengingsforsøk i systemer.

1.4 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 [8].

KAPITTEL 2

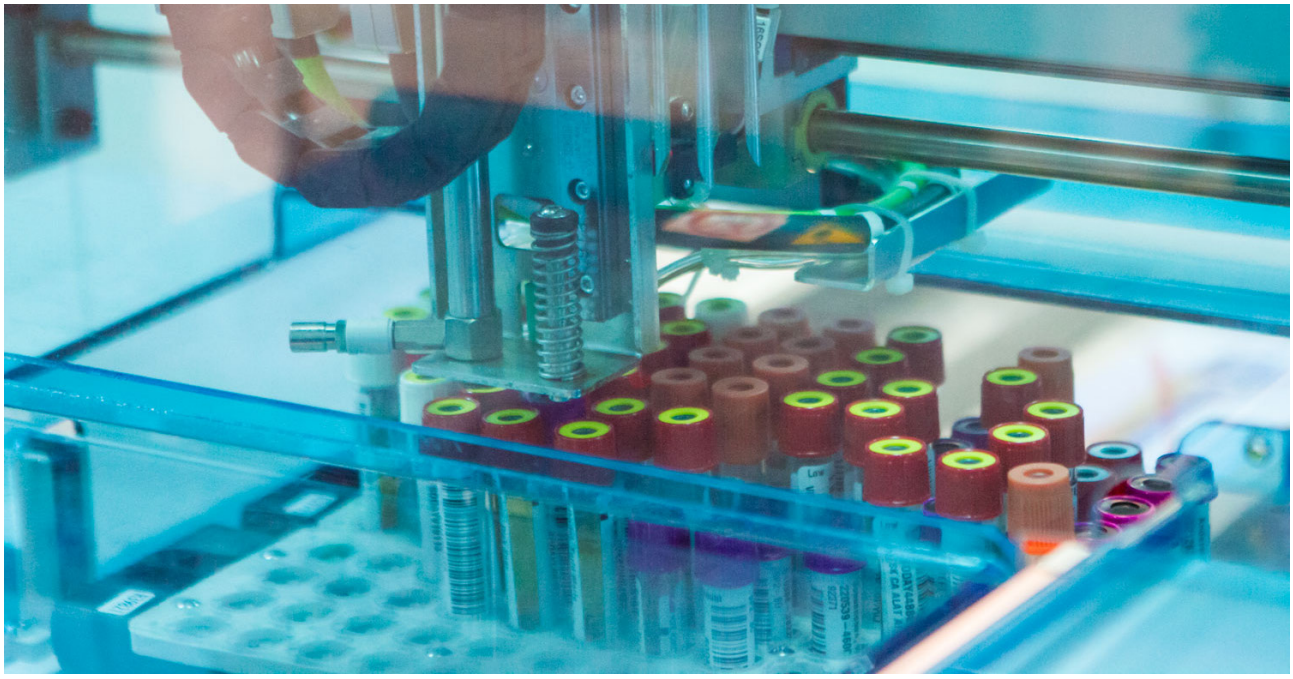
Motivasjon

Trusselaktører har ulik motivasjon for å utføre angrep mot spesialisthelsetjenesten, men samme trusselaktør kan ha mer enn ett motiv for å utføre et angrep.

Geopolitisk og sikkerhetspolitisk ustabilitet kan påvirke motivasjonen til alle typer trusselaktører. Den ustabile sikkerhetspolitiske situasjonen i verden smitter over på cyberdomenet [9]. Eksempler på dette er krigene i Ukraina og Gaza som har skapt nye aktører innen hacktivisme og økt eksisterende aktørers aktivitet [9]. Som følge av geopolitiske endringer kan verdien av informasjon endre seg [10]. Dette vil kunne påvirke både trusselaktørenes målutvelgelse og deres vilje til å gjennomføre angrep [10, 11].

Ønsket om å tilegne seg informasjon motiverer statlige aktører til å gjennomføre cyberangrep. Aktører kan være på jakt etter helsedata, forskningsdata, registerinformasjon og informasjon om enkeltmål. Stater kan bruke kunnskap om andre lands interne forhold til å understøtte sine egne målsetninger. Russland og Kina har styrket sitt strategiske samarbeid der de har sammenfallende interesse i å svekke Vesten, utfordre vestlige normer og styrke egen posisjon i verdenssamfunnet. Stater bruker gjerne cyberangrep som et virkemiddel for å oppnå strategiske fordeler, eller for å ivareta egne interesser [1, 4, 9, 12].

Økonomisk vinning er en drivkraft for flere typer trusselaktører. Organiserte kriminelle aktører utnytter sine data- og systemtilganger til å berike seg selv økonomisk [9], mens innsidere kan være drevet av personlig økonomisk vinning. Enkelte statlige aktører gjennomfører cyberoperasjoner for å fremme landets økonomiske interesser [9, 12], blant annet for å finansiere våpenprogrammer og militær opprustning [13].



Laboratorierør. Foto: Sykehuspartner HF

Statlige aktører gjennomfører cyberangrep og påvirkningsoperasjoner for å skape mistro til offentlige myndigheter og spre feilinformasjon. Formålet med slike angrep er å forsøke å endre oppfatningen til enkeltpersoner, grupper eller hele befolkningen i en retning som tjener trusselaktørens interesser [13]. For å oppnå dette vil statlige aktører benytte både nye og eksisterende konfliktlinjer i et forsøk på å polarisere og destabilisere samfunnet, svekke tillit og skape tvil om hva som egentlig er sant. Et annet formål kan være å fremstille den statlige aktøren på en mer positiv måte [13, 14, 15]. Et angrep mot spesialisthelsetjenesten kan ha til hensikt å svekke Norges evne til å håndtere for eksempel helsekriser [12].

Norges geografiske beliggenhet gjør oss til et attraktivt mål for statlige aktører med interesse for å posisjonere seg i Arktis. Flere stormakter viser stor interesse for å posisjonere seg i nordområdene. Russland søker å være den dominerende aktøren i Arktis [16]. Dette behovet blir stadig mer sentralt ettersom Arktis har fått økt strategisk betydning i en mer spent sikkerhetspolitisk situasjon [13]. Kina vil fortsette å prioritere sin langsiktige posisjonering i Arktis, og gradvis øke sin tilstedeværelse og etterretningsaktivitet. Kinesisk forskningsaktivitet på Svalbard kan for eksempel bidra til å normalisere kinesisk tilstedeværelse og legge til rette for etterretningsaktivitet [13].

Ideologisk overbevisning kan motivere både grupper og individer til å utføre cyberangrep. Hensikten kan være å skape offentlig oppmerksomhet om trusselaktørens dagsorden eller budskap [9]. Ideologisk overbevisning kan også være en motiverende faktor for at personer begår innsidevirksomhet.

Kilde: ©Rawpixel.com – stock.adobe.com

KAPITTEL 3

Aktuelle angrepsmetoder og sikkerhetstrusler

Det digitale trusselbildet for spesialisthelsetjenesten blir stadig mer komplekst, og trusselaktørene utvikler avanserte angrepsmetoder som utfordrer etablerte sikkerhetstiltak. Samtidig utgjør tilsynelatende enkle angrepsmetoder en betydelig risiko. Virkemiddelbruken kombinerer åpne, fordekte og skjulte metoder.

I hovedsak benytter angripere metoder i tre forskjellige kategorier for å bryte seg inn – omgåelse, utnyttelse og manipulasjon. I dette kapittelet løfter vi frem noen av de mest aktuelle metodene og truslene mot spesialisthelsetjenesten. Vi forventer at disse vil fortsette å skape utfordringer for spesialisthelsetjenesten i den kommende perioden.

3.1 Adversary-in-the-Middle-phishing

Phishing har i lang tid vært en aktuell sikkerhetstrussel, også mot spesialisthelsetjenesten. Multifaktorautentisering (MFA) har over tid blitt mer utbredt, noe som har gjort at phishing, som stjeler brukernavn og passord, har blitt mindre effektivt for en angriper. Som en respons har angripere de siste årene begynt å bruke Adversary-in-the-Middle-phishing (AitM) for å omgå flere typer MFA.

Spesialisthelsetjenestens sikkerhetsmiljøer har observert en kraftig økning i AitM mot helsesektoren. I tillegg til økt bruk av MFA kobler vi økningen til økt bruk av skytjenester, men vi ser at phishingresistente autentiseringsmetoder fungerer godt som et mottiltak.

AitM-phishing kan være vanskelig å oppdage når et angrep har vært gjennomført. Dette gjør det utfordrende for våre sikkerhetsmiljøer å oppdage en angriper som forsøker å holde seg skjult. For en vanlig bruker vil det være tilnærmet umulig å oppdage aktiviteten. En tålmodig angriper kan eksfiltrere sensitive e-poster, dokumenter og chattemeldinger fra en kompromittert konto over tid.

Det vanligste målet med AitM-phishing mot spesialisthelsetjenestene er tilgang til M365. Vi forventer at angripere følger godt med på hvilke tjenester som brukes mest, og tilpasser angrepsmetodikken. Dersom en aktør ønsker å gjennomføre målrettede angrep av denne typen, vil det som regel være lett å kartlegge hvilke tjenester en virksomhet benytter.

3.2 Eksterne lagringsmedier

Bruk av eksterne lagringsmedier, som USB-minnepinner og eksterne harddisker, er praktisk for lagring og overføring av data. Imidlertid utgjør de en vesentlig trussel som må tas på alvor. Bruk av lagringsmedier på tvers av IT-systemer øker sannsynligheten for spredning av skadevare og uautorisert tilgang til sensitive data. Risikoen forsterkes når slike medier benyttes på ikke-administrert utstyr eller i situasjoner hvor rutiner for sikker bruk mangler. I slike tilfeller kan det være utfordrende å spore dataflyten, noe som kan føre til misbruk av informasjon og gjøre det vanskelig å oppdage sikkerhetsbrudd.

Vi har over tid sett en økning i deteksjon av

skadevare på eksterne lagringsmedier, noe som understreker utfordringen med å benytte slike enheter. Mange av tilfellene er knyttet til bruk av uautoriserte enheter og svak sikring av tilkoblede systemer. Skadevare kan overføres automatisk fra lagringsmediet til tilknyttet utstyr, eller skjules i filer som tilsynelatende virker normale. Dette gjør det mulig for skadevare å spre seg videre når en enhet kobles til nye systemer. Utfordringer som manglende sporbarhet og økt risiko for uautorisert tilgang oppstår også når lagringsmedier mistes eller benyttes til å overføre filer mellom forskjellige typer maskinvare, som for eksempel mellom hjemmedatamaskiner og arbeidsmaskiner.

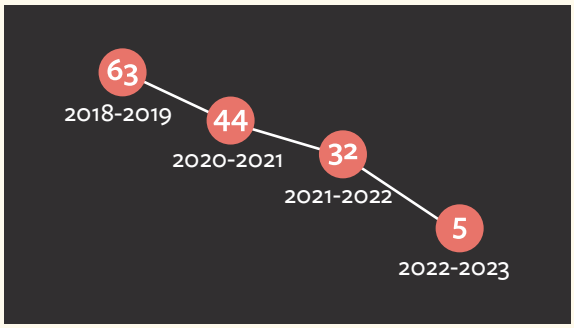
3.3 Utnyttelse av sårbarheter

Når trusselaktører benytter skadevarefrie teknikker, gjenbrukes programvare og systemadministrasjonsverktøy for å etterligne legitim aktivitet. Dette kan innebære gjenbruk av eksisterende programvare og utviklingsverktøy i virksomhetens systemer – living-off-the-land – eller å ta med seg programvare fra andre anerkjente leverandører. Skadevarefrie teknikker er utfordrende å detektere, og vil i liten grad stoppes automatisk av endepunktssikkerhetsløsninger – Endpoint Detection & Response (EDR).

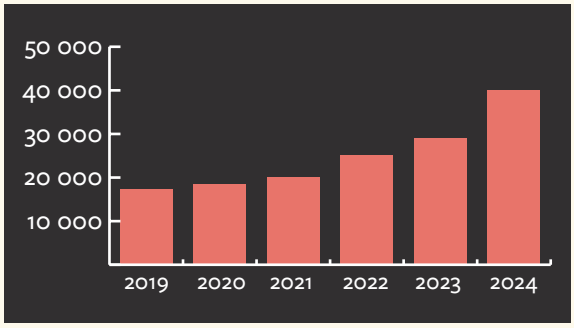
Trusselaktører har de siste årene tilpasset adferden i takt med økende bruk av EDR. Vi ser at det oftere benyttes skadevarefrie teknikker og utnyttelse av sårbarheter i edge-devices uten EDR – slik som brannmur, VPN og filsluser – for å unngå deteksjon [17, 18, 19, 20, 11]. I 2023 rettet en vesentlig andel av utnyttede sårbarheter seg mot spesialiserte enheter. I en kartlegging av hvordan angripere fikk tilgang til en virksomhets nettverk, skyldtes en tredjedel av tilfellene i 2023 utnyttelse av sårbarheter [18].

Analyser av utnyttede alvorlige sårbarheter viser at flertallet utnyttes innen én uke etter at de er blitt offentlig kjent. Antallet utnyttede sårbarheter, og andelen nulldagssårbarheter av alle alvorlige sårbarheter, øker. Av sårbarheter som ble observert utnyttet i 2023, er antallet nulldagssårbarheter for første gang større enn offentlig kjente sårbarheter (n-dagssårbarheter)[2] [17, 21, 19].

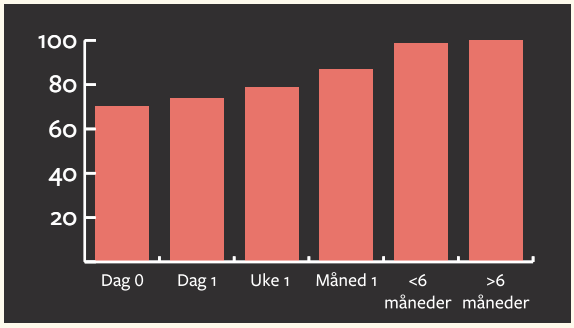
Fra 2021 til 2024 er antallet registrerte sårbarheter doblet [22]. Volumet av nye sårbarheter har medført kapasitetsproblemer i National Vulnerability Database (NVD), slik at et stort antall ikke er



Gjennomsnittlig tid (dager) til utnyttelse av alvorlige sårbarheter i 2023 - Mandiant [21].



Antall publiserte sårbarheter per år - NVD [22].



Prosent av alvorlige sårbarheter som er observert utnyttet i 2023 - Mandiant [21].

[2] Sårbarheten er offentlig kjent, og leverandør kan ha utarbeidet en oppdatering. En 0-dagssårbarhet blir til en 1-dagssårbarhet samme dag som den blir offentlig kjent.

analysert og kategorisert med hensyn til alvorlighet. Dette gjelder også utnyttede sårbarheter. NVD benyttes som datagrunnlag i de fleste sårbarhetsstyringsverktøy. Manglende vurdering og analyse av sårbarhetene påvirker dermed vår evne til å prioritere lukking av sårbarheter.

Når målrettet utnyttelse og masseutnyttelse av ukjente sårbarheter detekteres og eventuelle indikatorer blir kjent, kan vi i ettertid se at angrepene i noen tilfeller har foregått i flere måneder eller år [23, 24].

Edge-devices er særdeles attraktive mål. De er som oftest eksponert mot internett i nettverksperimeter, og støtter svært sjelden EDR. De har varierende loggkvalitet, og mangler ofte implementasjon av moderne herdingsteknikker for å forhindre utnyttelse av sårbarheter [17, 25, 11]. Sårbarheter i denne typen enheter krever typisk ikke brukerinteraksjon for vellykket utnyttelse. Mange høyt profilerte cyberoperasjoner viser at kompetente statlige trusselaktører som Kina og Russland, samt enkelte økonomisk motiverte trusselaktører, utvikler og benytter seg av denne typen sårbarheter for å oppnå fotfeste og persistens, samtidig som deteksjon omgås over lengre tid [14, 18, 17].

Kinesiske trusselaktører har vist kapasitet til, og intensjon om, langvarig investering i analyse for å finne nulldagssårbarheter og persistensteknikker i spesialiserte enheter [18, 11]. Sårbarheter avdekkes og utnyttelseskode utvikles ofte på tvers av privat sektor, statlig etterretning, militære enheter og akademia [26, 27, 28, 29]. En rekke produkter fra forskjellige leverandører har de siste årene blitt utnyttet i målrettede angrep [17]. I enkelte tilfeller er det observert at utnyttelseskode for samme nulldagssårbarhet benyttes av kinesiske trusselaktører fra ulike miljøer, mot forskjellige mål [30].

Edge-devices er ofte proprietære, og har gjerne tekniske tiltak for å forhindre tilgang og endring utover standardiserte grensesnitt. Disse tiltakene gjør effektiv digital etterforskning komplisert, og i noen tilfeller umulig. Grensesnittene gir i begrenset grad innsikt i systemets faktiske tilstand [18]. Etterforskning i forbindelse med hendelser i slike enheter har imidlertid avdekket vesentlige mangler med hensyn til sikker kodeutvikling, oppdatering av operativsystemer, applikasjoner og interne avhengigheter [18, 31, 32].

På bakgrunn av flere titalls angrepskampanjer mot edge-devices over flere år, publiserte NCSC-UK i 2025 retningslinjer for leverandører av spesialiserte enheter [33]. Retningslinjene inneholder konkrete minimumskrav for å redusere konsekvensen av sårbarheter og understøtte deteksjon og digital etterforskning.

3.4 Anskaffelser og leverandørkjeder

Spesialisthelsetjenesten er blitt stadig mer digitalisert de siste årene. Dette medfører lengre leverandørkjeder og et større antall leverandører, noe som øker angrepsflaten betraktelig. Det er utfordrende å ha god kontroll på alle leverandørene, og kjenne til deres sikkerhetsnivå og eventuelle politiske tilknytning [3]. Bytte av underleverandører kan være vanskelig å avdekke, men får store konsekvenser dersom det fører til at en trusselaktør får informasjon eller tilganger.

Angrep gjennom digitale leverandørkjeder kan utføres ved at angriper benytter tilgang hos leverandøren til å endre legitim programvare slik at den inneholder skadevare, som igjen distribueres til leverandørens kunder [9, 34]. En annen mulighet er at angriperen får direkte tilgang til kundenes systemer ved at leverandøren har legitim tilgang til et internt system for vedlikehold og support. Spesialisthelsetjenesten kan også påvirkes gjennom angrep på leverandørkjeden ved at tjenester eller systemer blir gjort utilgjengelige [35].

For statlige aktører kan det å være en del av leverandørkjedene være verdifullt. På denne måten kan de få tilgang til sensitiv informasjon, påvirke leverandørkjeder og gjennomføre fysisk eller digital sabotasje [16].

Aktørene kan oppnå tilgang til et ellers godt sikret mål ved å angripe en mindre sikker leverandør eller underleverandør [13]. Dette kan også være en fremgangsmåte for å treffe mange mål med ett og samme angrep [14]. Trusselaktører kan utnytte avhengigheter for å skape politisk press ved å true integriteten og tilgjengelighet i tjenesten [3, 16]. Angrep gjennom leverandørkjeden kan brukes for å skjule hvem som står bak, ettersom identifisering av aktøren kan kreve samarbeid på tvers av sektorer og landegrenser [13].

EOS-tjenestene advarer mot risikoen vi tar ved å gjøre oss avhengige av enkeltland og enkeltselskaper for leveranser til kritiske funksjoner [3]. Kina søker å etablere seg i kritiske leverandørkjeder gjennom subsidierte anskaffelser, og har en uttalt strategi om å kontrollere kritiske leverandørkjeder globalt [16]. En av strategiene de benytter for å oppnå dette, er å direkte eller indirekte subsidiere kinesiske teknologiselskaper slik at disse kan tilby teknologien sin til en pris som er vanskelig å konkurrere mot. På denne måten kan de vinne anbudskonkurranser, som ofte er basert på pris, og få innpass ved å utkonkurrere andre leverandører i kritiske leverandørkjeder [3].

3.5 Medisinsk-teknisk utstyr (MTU) og bygg-teknisk utstyr (BTU)

Moderne pasientbehandling er avhengig av medisinsk-teknisk utstyr, plassert i en kompleks bygningsmasse med til dels spesialisert bygg-teknisk utstyr. Med økt bruk av digitalt hjemmesykehus får vi en økning i bruk av MTU hjemme hos pasientene, noe som kan komplisere innføring av sikkerhetstiltak.

Spesialisthelsetjenesten forvalter i sum en svært kostbar og variert portefølje av nettverkstilkoblede enheter, som må kunne kommunisere med hverandre for å gi ønsket verdi. MTU og BTU kan ha en levetid på flere tiår, og noen er utdaterte sett i et IT-perspektiv. De er ofte ikke designet for et moderne nettverksmiljø eller for dagens trusselbilde.

MTU er omfattet av et strengt regulatorisk rammeverk og en streng godkjenningsprosess. Fra et cybersikkerhetsperspektiv gjør dette det utfordrende å oppdatere og vedlikeholde enhetene. Både MTU og BTU kan benytte innebygde nettverksoperativsystemer, og noen produsenter integrerer sine produkter med generelle operativsystemer. Sistnevnte kan i andre sammenhenger effektivt og raskt oppdateres ved hjelp av standardiserte løsninger. I MTU og BTU kan trusselaktører ofte dra nytte av et lengre tidsvindu for utnyttelse av sårbarheter, fordi oppdatering krever fornyet godkjenning og, i noen tilfeller, leverandørbistand.

I juli 2024 førte en feil hos IT-sikkerhetsleverandøren CrowdStrike til at 8,5 millioner Windows-PC-er over hele verden ble satt ut av drift [57]. Hendelsen påvirket blant annet helsetjenester i USA, Storbritannia, Canada, Tyskland og Israel, der flere sykehus måtte kansellere planlagte operasjoner [58]. Selv om hendelsen ikke var resultat av et cyberangrep, illustrerer den hvordan et leverandørkjedeangrep kan få store konsekvenser for mange virksomheter over hele verden.

Den generelle utviklingen innen cybersikkerhet er at stadig flere deteksjonskapabiliteter flyttes ned til endepunktet, i takt med at mer trafikk krypteres og beskyttes mot andre typer nettverksangrep. Endepunktssikkerhetsløsninger (EDR) støtter ikke innebygde nettverksoperativsystemer, og regulatoriske krav legger begrensninger på bruk i MTU-utstyr med generelle operativsystemer. Manglende tilstrekkelig synlighet i nettverkstrafikk og streng regulering av medisinsk utstyr svekker dermed deteksjonsevnen.

Å forhindre, oppdage og respondere på sikkerhetshendelser i MTU- og BTU-nettverk er utfordrende. Det krever en litt annen tilnærming, og legger enda større krav til sikkerhet i dybden. Jevnlig kartlegging av nettverket ved hjelp av spesialiserte produkter, mikrosegmentering og deteksjon i nettverket blir derfor viktigere tiltak for å oppnå god sikkerhet.

MTU og BTU likner på edge-devices i den forstand at det i mange tilfeller vil være særlig ressurskrevende, og til dels kreve inngående kjennskap til hvert enkelt produkt, å fastslå om en enhet er kompromittert. En angriper kan i denne typen miljø enklere oppnå persistens, uten å bli oppdaget. Et destruktivt angrep gjennomført mot relativt få MTU-enheter kan bli svært kostbart og kan raskt få konsekvenser for pasientbehandling.

3.6 Økonomisk svindel

Økonomisk svindel treffer alle virksomheter, og spesialisthelsetjenesten er ikke et unntak. Når spesialisthelsetjenesten blir rammet av svindel får det sjelden konsekvenser for liv og helse, men det kan like fullt påvirke oss gjennom tap av betydelige summer. Vi ser flere ulike typer svindel rettet mot virksomhetene våre. Felles for disse metodene er at de er en form for sosial manipulering. En angriper forsøker å lure en ansatt i virksomheten til å utføre en oppgave den ansatte har tillatelser og myndighet til.

I en årrekke har vi sett flere varianter av den klassiske direktørsvindelen, der noen utgir seg for å være en direktør som trenger hjelp. Det vanligste er å be om å få kjøpt gavekort eller å be om å få gjennomført banktransaksjoner. Disse er som regel enkle å identifisere, og på mindre beløp.

En annen variant vi har observert, er målrettet fakturasvindel. Her benytter svindleren seg av offentlig tilgjengelig informasjon om anbud. Svindleren vil først lure en anbudsvinner til å gi fra seg en ekte ubetalt faktura. På denne fakturaen vil svindleren redigere betalingsinformasjonen, før den sendes til offeret som lures til å betale. Metoden er effektiv ettersom fakturaen offeret mottar ser ut som en ekte faktura, med innkjøpsordre og riktig beløp, for varer og tjenester man har fått levert. Vi har sett denne metoden brukt i svindelforsøk i millionklassen mot spesialisthelsetjenesten.

CT-maskin. Foto: Sykehuspartner HF

KAPITTEL 4

Vurderinger

For å kunne beskytte sine verdier, må spesialisthelsetjenesten forstå hva trusselaktørene er ute etter og hvilke metoder de bruker for å nå sine mål. I dette kapittelet beskriver vi de fremgangsmåtene vi anser som mest sannsynlig at trusselaktørene vil bruke mot spesialisthelsetjenesten.

Det benyttes et bredt spekter av metoder og virkemidler for å utnytte potensielle sårbarheter. Når slike virkemidler kombineres, omtales det som sammensatt virkemiddelbruk.

Laboratorierør i stativ. Foto: Norsk helsenett SF

4.1 Organisert cyberkriminalitet

Aktivitet fra organiserte kriminelle er stadig i økning, også mot helsesektoren [36]. Spesialisthelsetjenesten opplever daglig forskjellige typer angrepsforsøk fra organiserte kriminelle, som svindelforsøk, forsøk på utnyttelse av sårbarheter i eksponert utstyr og forsøk på å få fotfeste på klientmaskiner.

Fremgangsmetoder som brukes av organiserte kriminelle varierer stort, og med et komplisert aktørlandskap kan det være utfordrende å utlede hva formålet med et angrep er dersom angrepet stoppes før angriper oppnår målet sitt. Flere av angrepene som observeres mot spesialisthelsetjenesten antas å komme fra «access brokers[3]», en aktørgruppe som har vært i stor vekst de siste årene [11]. Denne gruppen av angripere kobles tett til en av de største truslene mot spesialisthelsetjenesten – utpressingsaktører.

Utpressing i den digitale sfæren er knyttet til begrepet utpressingsangrep, det vil si hendelser der en angriper har fått tilgang til systemer og kan ha stjålet eller kryptert data og dermed gjort systemer utilgjengelige. Aktører som gjennomfører utpressingsangrep er ofte på jakt etter mål med høy verdi. Som følge av sin samfunnskritiske funksjon er spesialisthelsetjenesten et høyaktuelt mål for utpressingsaktører.

[3] En aktørgruppe som fokuserer på å få tilgang til bedrifters systemer og videreselge tilgange.

Ett av hovedmomentene i et utpressingsangrep er tyveri av data. En utpressingsaktør vil som regel presse et offer for penger mot å ikke publisere det som er stjålet. Dataene vil imidlertid kunne være verdifulle i seg selv. Dersom en angriper får ut e-poster eller filer fra arbeidsstasjoner, vet vi av erfaring at disse kan inneholde passord, nettverksskisser eller beskrivelser av interne forhold som kan benyttes ved et senere angrep.

En økende trend de siste årene er aktører som stjeler data og truer med å publisere dem uten at de også krypterer systemer [36]. Å ikke kryptere reduserer kompleksiteten i angrepet, og gjør at angriperen kan holde seg skjult lengre.

Utpressingsangrep blir sjelden utført av gruppen som påtar seg ansvaret. Angrepet kommer som regel fra en samarbeidspartner som står for kompromitteringen av systemet og bruken av skadevaren. En samarbeidspartner kan også jobbe for flere utpressingsgrupper, derfor er det vanskelig å identifisere hvem som egentlig står bak. Metoder som offentlig kobles til én gruppe brukes av flere, og den samme fremgangsmåten kan kobles til flere grupper.

Tidligere hendelser viser at det ikke er garantert at kritiske systemer kan gjenopprettes på kort tid selv om man betaler for dekrypteringsnøkler [37, 38]. Det er heller ikke gitt at angriperne holder det de lover, og at de sletter informasjonen som er stjålet. Når det er flere aktører involvert i en operasjon kan det oppstå konfliktflater mellom de involverte aktørene. En kompromittert virksomhet kan betale til en utpressingsgruppe, mens samarbeidspartneren som har gjennomført angrepet ikke får betalt og dermed ikke har et insentiv til å etterleve avtalen om å slette stjålne data.

Vurdering

Spesialisthelsetjenesten opplever daglig forsøk på angrep fra organiserte 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 derfor 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**.

Utpressingsangrepet *den 3. juni 2024 mot leverandøren av laboratorietjenester til National Health Services (NHS) illustrerer kompleksiteten i trusselbildet når det gjelder konsekvenser, motivasjon og intensjon. Trusselaktørens intensjon kan ha vært å ramme helsevesenet og å skape en helsekrise i London. Angrepet rammet IT-systemene til leverandøren, og førte til stopp i laboratorietjenesten som identifiserte blodtypen til pasientene. Sykehus måtte kansellere alle planlagte operasjoner, og traumemottak måtte flyttes til sykehus som ikke var rammet [55, 56].*

Angrepet ble utført av en russiskspråklig cyberkriminell gruppering som har spesialisert seg på utpressingsangrep. I tillegg til at de rammet laboratorietjenestene, stjal de store mengder pasientdata som senere ble publisert på det mørke nettet.

4.2 Cyberspionasje

Cyberspionasje utgjør en vedvarende trussel mot spesialisthelsetjenesten. Spesialisthelsetjenesten forvalter en betydelig mengde informasjon, fra sensitiv pasientinformasjon til store datasett, forskning og viktig digital infrastruktur for vår helseberedskap. Cyberspionasje utføres av ulike trusselaktører med ulike formål, fra industrispionasje til etterretningsoperasjoner.

Statlige trusselaktører bruker samme verktøy og teknikker som organiserte kriminelle. Fremmede etterretningstjenester bruker i større grad organiserte kriminelle aktører til å utføre deler av, eller hele, angrepet [39]. Dette har ført til at grensene mellom nasjonalstatsstøttede cyberangrep og kriminell aktivitet blir stadig mer uklare.

Trusselaktørene ønsker innsikt i hvordan organisasjoner, systemer og infrastruktur er bygd opp for å opprette bakdører. For å etablere tilgang bruker de ofte legitim påloggingsinformasjon som de urettmessig har skaffet seg, blant annet gjennom utilsiktede lekkasjer, sosial manipulering og innsidevirksomhet. Mange trusselaktører har avanserte metoder for å utføre cyberspionasje. De er meget effektive i å utnytte 0-dagssårbarheter mot mål av høy verdi. Vi forventer at trusselaktører vil benytte de samme metodene mot spesialisthelsetjenesten.

Spesialisthelsetjenesten som del av totalforsvaret har en viktig rolle i en militær konflikt, og vil derfor være interessant for russisk etterretning. Russland prioriterer kartlegging av kritisk infrastruktur og virksomheter som leverer tjenester som understøtter infrastrukturen. Hensikten med kartleggingen er å identifisere sårbarheter som kan utnyttes i form av sabotasje ved en militær konflikt [1]. Nordområdene er av særlig interesse for Russland, blant annet som følge av at Arktis har fått økt strategisk betydning i en mer spent sikkerhetspolitisk situasjon [7].

Kinesisk forskingsaktivitet på Svalbard kan være et virkemiddel for å normalisere Kinas tilstedeværelse slik at landet kan drive med etterretningsaktivitet. Kina bruker også cyberspionasje for å få tilgang til forskningsdata og teknologi for å fremme landets økonomiske interesser [13]. Kinesiske trusselaktører har gjennomført cyberspionasjekampanjer mot vestlig helsevesen over tid [40, 41].

Statlige aktører har gjennom flere år vist en betydelig interesse for forskningsinstitusjoner. Akademia er en arena hvor etterretningstjenester kan få tilgang til informasjon, menneskelig ressurser, teknologi, laboratorier og stordata [7]. Tilgang til medisinsk forskingsdata, helsedatabaser og genetisk data kan for eksempel brukes som et grunnlag for biologisk krigføring eller presisjonsmedisin [1].

Den største cyberspionasjetrusselen mot spesialisthelsetjenesten kommer fra etterretningsorganisasjoner i Kina og Russland. Begge disse landene har et strategisk behov for

Sommeren 2023 ble flere norske departementer utsatt for et avansert cyberangrep [60]. En angriper utnyttet flere nulldagssårbarheter i et system levert av en tredjepart, Ivanti Endpoint Mobile Manager, og fikk tilgang til e-postløsningen til 12 departementer [59]. Det er uvisst hva angriper har gjort med denne tilgangen. Det sofistikerte nivået på angrepet, kombinert med målet, sannsynliggjør at dette var et spionasjeangrep fra en fremmed stat.

å ha tilstedeværelse i nordområdene, noe som gjør regionen til et attraktivt etterretningsmål [7]. Russland bruker sin cyberspionasjekapasitet primært for å være forberedt på en militær konflikt med NATO, mens Kina har mer økonomiske og geopolitiske interesser.

Vurdering

Teknologiutviklingen gjør at cyberspionasje og etterretningsvirksomhet kan gjennomføres mer effektivt, i et større omfang og med lavere risiko. Trusselbildet er komplekst og uoversiktlig, noe som gjør det vanskelig å skille cyberspionasje fra andre typer cyberangrep. Statlige aktører gjennomfører cyberspionasjekampanjer mot vestlig helsevesen, og vi forventer at dette også vil treffe spesialisthelsetjenesten i Norge. Vi vurderer at trusselen fra cyberspionasje er **høy**.

Vi vurderer det som **sannsynlig** at spesialisthelsetjenesten vil utsettes for cyberspionasje fra aktører med direkte eller indirekte koblinger til russiske og kinesiske etterretningsorganisasjoner.

4.3 Innsidevirksomhet

Mennesker er den viktigste ressursen en virksomhet har, men de kan også utgjøre en trussel. Innsidevirksomhet kan få store konsekvenser for spesialisthelsetjenesten, særlig fordi helsesektoren er definert som ett av hovedmålene til statlige trusselaktører [13]. Konsekvensene av innsidevirksomhet kan være blant annet tap av informasjon, redusert kapasitet i helsetjenesten, økonomisk tap og omdømmetap. Det geopolitiske spenningsnivået, en større andel av personell med ulike former for tilknytning til andre land, og økt bruk av digitale kanaler er faktorer som gir økt risiko for innsidevirksomhet [4].

Innsidere i en organisasjon kan både være personer som ubevisst forårsaker skade, og personer som aktivt søker å skade virksomheten de jobber for [10]. 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. Slike handlinger henger ofte sammen med lav sikkerhetsmessig bevissthet hos den aktuelle personen, samt mangelfull sikkerhetsstyring og daglig sikkerhetsmessig ledelse i virksomheten [8, 10].

En bevisst innsider er en person som har til hensikt å begå skadelige handlinger som strider mot virksomhetens interesser [8]. En innsider kan være selvmotivert, en infiltratør eller en rekruttert innsider. 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 [8, 10].

Bruk av innsidere har økt verdi for trusselaktørene mot virksomheter som har god digital sikkerhet. I takt med at virksomhetene får på plass stadig mer sofistikerte fysiske og digitale sikkerhetstiltak for å beskytte sine verdier, vil rekruttering av innsidere

Kilde: ©Andrii Yalanskyi – stock.adobe.com

bli mer attraktivt for en trusselaktør [3, 42]. Trusselaktører kan forsøke å rekruttere innsidere eller plassere enkeltindivider på innsiden av en virksomhet. Innsideren kan utføre eller legge til rette for spionasje eller sabotasje fra innsiden av virksomheten [3].

Innsidevirksomhet kan være svært vanskelig å avdekke. Kina og Russland vil være spesielt aktive i å forsøke å rekruttere menneskelige kilder for å få tilgang til sensitiv og gradert informasjon [7]. Slike rekrutteringsforsøk blir i stadig større grad utført via digitale kanaler, for eksempel gjennom sosiale medier [7, 4]. Digital rekruttering er kostnadseffektivt, relativt enkelt å videreføre over tid, og innebærer lav risiko for å bli oppdaget [7]. Konfliktnivået i verden øker muligheten til å utnytte eller legge press på enkeltpersoner. Dette vil spesielt gjelde personer med tilknytning til krise- og krigsrammede områder, eller personer med tilknytning til høyrisikoland [4].

Spesialisthelsetjenesten har fått utpekt skjermingsverdige verdier som er underlagt sikkerhetsloven, og har derfor fått økt betydning for nasjonal sikkerhet [4]. Høyrisikoland vil forsøke å tilegne seg sensitiv kunnskap både i form av skjermingsverdig informasjon og sensitiv kunnskap som for eksempel helserelaterte forskningsdata. Den økningen noen helseforetak har sett i jobbsøkere fra høyrisikoland, kan være et ledd i å få plassert personell i stillinger der de har tilganger som en statlig aktør kan utnytte for å få tilgang til slik informasjon.

Vurdering

EOS-tjenestene peker på at innsiderisikoen er reell. Rekruttering av innsidere, spesielt fra Kina og Russland, utgjør en **høy** trussel mot spesialisthelsetjenesten. Innsidevirksomhet må ses i sammenheng med trusselen fra cyberspionasje, og statlige aktørers intensjon om å benytte menneskelige kilder som virkemiddel.

Spesialisthelsetjenesten er definert som ett av hovedmålene til statlige trusselaktører, og vi ser en økning i jobbsøkere fra høyrisikoland i flere av våre helseforetak. På bakgrunn av dette vurderer vi det som **meget sannsynlig** at spesialisthelsetjenesten vil bli utsatt for innsidevirksomhet.

4.4 Destruktive cyberangrep og sabotasje

Destruktive cyberangrep er digitale angrep som har til hensikt å ødelegge eller endre informasjon, programvare eller maskinvare for å skape alvorlige og omfattende konsekvenser for samfunnsviktige funksjoner. Destruktive cyberangrep og sabotasje kan indirekte ramme spesialisthelsetjenesten dersom andre deler av samfunnskritisk infrastruktur, som kraftsektoren eller vannforsyningen, blir angrepet. Konsekvensene av slike angrep kan også være betydelig skade på fysiske objekter eller personer [9].

Sammensatte virkemidler er konvensjonelle og irregulære virkemidler som en fremmed makt bruker i gråsonen mellom krig og fred. Virkemidlene som brukes er synkroniserte uønskede handlinger, hvor målet er å destabilisere samfunn for å oppnå politisk, økonomisk eller territoriell vinning. Cyberspionasje, påvirkningsoperasjoner, hacktivisme, leverandørkjedeangrep og destruktive cyberangrep er virkemidler som statlige aktører bruker i sin hybride krigføring [43].

Høyrisikoland har kapasitet til å gjennomføre destruktive cyberangrep mot spesialisthelsetjenesten. Hvorvidt aktøren gjennomfører et angrep eller ikke vil variere ut fra egeninteresse og strategiske målsetninger. Statlige aktører vil prøve å skjule sin tilknytning til et destruktivt cyberangrep ved å engasjere andre aktører. Som følge av økt forståelse for konsekvensene av destruktive cyberangrep, er bekymringen for slike angrep de siste årene blitt større i hele verden. Erfaringene fra Russlands

bruk av destruktive cyberangrep i krigen i Ukraina, viser tydelig intensjon og kapasitet til å lamme kritisk infrastruktur og kritiske samfunnsfunksjoner. Samtidig har Russlands risikovilje og Kinas bruk av sammensatte virkemidler økt [39, 9, 7].

Amerikanske sikkerhetsmyndigheter har gjort observasjoner av kinesiske trusselaktører som har forhåndsposisjonert seg i kritisk infrastruktur i USA. Angrepene ble vurdert til å være forhåndsposisjonering for å senere kunne gjennomføre destruktive cyberangrep [44]. Enkelte statlige aktører planlegger for destruktive og forstyrrende cyberangrep i sin militære strategi. Det er ikke avdekket forhåndsposisjonering i spesialisthelsetjenesten, men dette er en fremgangsmåte vi forventer at Kina og Russland vil forsøke å bruke.

Sabotasje er å skade eiendom, produksjonsmidler eller tekniske systemer med hensikt [45]. Hensikten kan være å ødelegge infrastruktur for å øke effekten av militære operasjoner eller påvirke politiske beslutninger. 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 [7]. Russiske etterretningstjenester har vist økt risikovilje, og bruker gjerne proxy-aktører for å gjennomføre angrep [1]. Dette gjør det vanskeligere å identifisere trusselaktørene, og operasjonene kan fornektes av de som virkelig står bak.

Målene for sabotasjeaksjonene har primært vært eiendom og logistikkinfrastruktur, men også annen ordinær sivil infrastruktur er blitt rammet. Det er ikke observert forsøk på sabotasjeaksjoner i Norge [7]. EOS-tjenestene har trukket fram kritisk infrastruktur, spesielt energiinfrastrukturen, som aktuelle mål for denne typen aksjoner [7]. Spesialisthelsetjenesten vil indirekte kunne bli påvirket av denne typen aksjoner, for eksempel ved tap av fiber eller kraft.

Vurdering

Som følge av den spente sikkerhetspolitiske situasjonen i verden er det en økt trussel for destruktive cyberangrep og sabotasje. Dette har sammenheng med økende vilje fra statlige aktører til å bruke sammensatte virkemidler.

Russland og Kina har meget høy kapasitet til å gjennomføre destruktive cyberangrep og sabotasje mot spesialisthelsetjenesten. Spesialisthelsetjenesten kan rammes direkte som følge av målrettede angrep, eller indirekte som følge av angrep rettet mot kritiske samfunnsfunksjoner vi er avhengige av. Vi vurderer at trusselen fra destruktive cyberangrep og sabotasje mot spesialisthelsetjenesten er **moderat**. Det er **mulig** at slike angrep vil kunne ramme spesialisthelsetjenesten i kommende periode.

4.5 Påvirkningsoperasjoner

Påvirkningsoperasjoner er koordinerte kampanjer som forsøker å påvirke handlinger eller holdninger i en gruppe ved bruk av manipulasjonsteknikker i forskjellige informasjonskanaler. Målet til en påvirkningsoperasjon kan være helt konkret og kortsiktig, som å få en bestemt kandidat valgt i en demokratisk prosess, eller abstrakt og langsiktig, som å destabilisere et samfunn.

En trusselaktør kan kombinere påvirkningsoperasjoner med andre metoder, omtalt som sammensatt virkemiddelbruk, for å øke effekten. Bruk av sammensatte virkemidler øker sannsynligheten for at operasjonen lykkes i Norge. Russland har tidligere kombinert påvirkningsoperasjoner med diplomatisk press for å påvirke politiske beslutninger i Norge [13].

Generativ kunstig intelligens (KI) er en teknologi som har fått stor betydning for påvirkningsoperasjoner [3, 11]. Generativ KI kan blant annet brukes til å øke kapabilitet og rekkevidde, unngå språkbarrierer og til å lage naturtro bilder, lydklipp og videoer. Det er observert tilsynelatende stor forskningsinteresse for

generert innhold fra Russland, Kina, og Iran.

Tillit til spesialisthelsetjenesten er svært viktig for å kunne håndtere fremtidige helsekriser [12]. Tillit til helsevesenet og myndighetene er en viktig faktor for om folk velger å følge myndighetenes pålegg og anbefalinger [46]. Et godt eksempel på dette er smitteverntiltakene som ble iverksatt mot Covid-19.

Påvirkningsoperasjoner kan ramme spesialisthelsetjenesten ved å målrettet bryte ned tilliten mellom befolkningen og spesialisthelsetjenesten, eller ved å gjennomføre en større operasjon med mål om å destabilisere det norske samfunnet. EOS-tjenestene forventer at Norge vil rammes av påvirkningsoperasjoner fra fremmede stater i kommende periode, spesielt fra Russland og Kina, der målsettingen er å endre opinionen i enkeltsaker [7].

Vurdering

Vi vurderer trusselen fra målrettede påvirkningsoperasjoner mot spesialisthelsetjenesten som lav, og det er lite sannsynlig at en slik operasjon vil gjennomføres. Trusselen og sannsynligheten kan endre seg raskt ved fremtidige helsekriser eller som følge av endringer i den geopolitiske situasjonen.

Spesialisthelsetjenesten kan rammes av generelle påvirkningsoperasjoner mot det norske samfunnet. Vi vurderer det som **mulig** at spesialisthelsetjenesten vil bli påvirket av en slik kampanje, men at trusselen er **lav**.

4.6 Hacktivisme

Hacktivist-grupper har som oftest lavere kapasitet enn andre trusselaktører, og benytter seg derfor ofte av mindre sofistikerte angrepsmetoder som tjenestenekt og digital vandalisme for å oppnå sine mål. Driverne for hacktivisme er fortsatt de pågående krigene mellom Ukraina og Russland, og mellom Israel og Hamas. Krigen mellom Israel og Hamas har fungert som en katalysator for økt hacktivisme mot Israel fra Iran og iranskstøttede grupperinger i regionen. Generelt sett er det etter 2022 en økning i frekvens, variasjon i målutvelgelsen og intensiteten til hacktivister [47, 48, 49].

Det siste tiåret har virksomheter som tilbyr tjenestenektbeskyttelse rapportert at størrelsen på angrep har økt eksponentielt [50, 51]. Antallet angrep øker særlig i EMEA (Europa, Midtøsten og Afrika) [48]. Enkelte hacktivist-grupper har allerede tilgang til infrastruktur som lar dem gjennomføre omfattende tjenestenektangrep.

Trusselaktører har den siste tiden i økende grad benyttet virtuelle maskiner hos skyleverandører for å utføre angrep, fordi å skape og opprettholde et botnet[4] ofte er ressurskrevende. Denne taktikken gir økt kapasitet og stabilitet, og reduserer effekten av mitigerende tiltak hos offeret ettersom trafikken kommer fra legitime skyleverandører. Trusselaktører benytter stjålne kredittkort for å betale for angrepskapasiteten, og kan samtidig omgå identitetssjekk hos leverandør. Dette erstatter i noen tilfeller både behovet for utvikling av egen skadevare

To sudanesiske medlemmer av hacktivist-gruppen Anonymous Sudan, kjent for tjenestenektangrep (DDoS) mot helsesektoren i Norden og tjenestenekt-angrepet på SAS (2023), ble i 2024 pågrepet og tiltalt av amerikanske myndigheter [47]. Til tross for at gruppens adferd i målutvelgelse, infrastruktur og sammenfallende propaganda indikerer nær knytning til russiske myndigheter, inneholdt tiltalen fra amerikanske myndigheter ingen direkte kobling.

[4] Botnet er en samling nettverkstilknyttede enheter som kan fjernstyres av en operatør (robot-nettverk), med eller uten eiers samtykke.

for å opprette et eget botnet, og for å leie kapasitet hos tilbydere av tjenestenektangrep.

Hacktivisme-aktivitet følger geopolitiske strategiske interesser oftere enn før. Dette gjenspeiles i målutvelgelse og budskap. Eksempelvis ble spesialisthelsetjenesten, som følge av Norges støtte til Ukraina, mål for flere tjenestenektangrep i 2023. Aktører som Russland og Iran benytter også hacktivisme som dekke i hybride operasjoner. Hacktivist-aktører har de siste årene utvist økt kompetanse på påvirkningsoperasjoner, der hacktivist-personaer[5], cyberangrep og en mer effektiv formidling av politiske budskap kombineres for økt effekt. Dette er metoder vi tradisjonelt forbinder med statlige aktører, og indikerer en sterkere knytning mellom statlige aktører og hacktivister.

Vurdering

Det er ikke observert hacktivisme-aktivitet mot spesialisthelsetjenesten det siste året, og denne typen trusselaktør har ikke vist nevneverdig interesse for norske virksomheter i 2024. Vi vurderer trusselen fra hacktivisme mot spesialisthelsetjenesten som **lav**, og at angrep er **lite sannsynlig**. Økte geopolitiske spenninger, mer bruk av hacktivisme som statlig virkemiddel og et mer dynamisk trusselbilde har imidlertid vist at dette fort kan endre seg.

Operasjonssal.Foto: Sykehuspartner HF

[5] En persona er en fiktiv profil av en type menneske, målgruppe eller liknende.

Referanser

[1] **Etterretningstjenesten**, «Fokus,» 2025.

[2] **B. O. Kjerstad og K. O. Tung**, «Skriftlig spørsmål fra Birgit Oline Kjerstad (SV) til digitaliserings- og forvaltningsministeren,» Stortinget, 26. februar 2025. [Internett]. https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=101777.

[3] **NSM**, «Risiko,» 2024.

[4] **NSM**, «Risiko,» 2025.

[5] **NSM**, «Risiko,» 2023.

[6] **NSM**, «Risiko,» 2022.

[7] **PST**, «Nasjonal trusselvurdering,» 2025.

[8] **NSM**, «Temarapport: Innsiderisiko,» 2020.

[9] **CFCS**, «Cybertruslen mod Danmark,» 2024.

[10] **Spesialisthelsetjenesten**, «Trusselvurdering 2024: Det digitale trusselbildet mot spesialisthelsetjenesten,» 2024.

[11] **CrowdStrike**, «Global Threat Report,» 2025.

[12] **Office of the Director of National Intelligence**, «Annual Threat Assessment of the U.S Intelligence Community,» 2024.

[13] **PST**, «Nasjonal trusselvurdering,» 2024.

[14] **CrowdStrike**, «Global Threat Report,» 2024.

[15] **F. Forskningsinstitutt**, Komponist, Kort forklart: Hva er påvirkningsoperasjoner. [Lydopptak]. 2022.

[16] **Etterretningstjenesten**, «Fokus,» 2024.

[17] **C. Condon, S. Fewer og C. Beek**, «2024 Attack Intelligence Report,» Rapid7, 2024.

[18] **Mandiant**, «M-Trends,» 2024.

[19] **S. Abbasi**, «2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is,» Qualys, 19. desember 2023. [Internett]. https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one.

[20] **CrowdStrike**, «Threat Hunting Report,» 2024.

[21] **C. Charrier og R. Weiner**, «How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends,» Mandiant, 15. oktober 2024. [Internett]. https://cloud.google.com/blog/topics/threat-intelligence/time-to-exploit-trends-2023.

[22] **CVE**, «Published CVE Records,» 2025. [Internett]. https://www.cve.org/about/Metrics.

[23] **F. Castelan, M. Thauer**, J. Glab, G. Roncone, T. Ahmed og J. Wilson, «Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575),» Mandiant, 24. oktober 2024. [Internett]. https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575.

[24] **D. Antoniuk**, «Belgium probes suspected Chinese hack of state security service,» The Record, 27 Februar 2025. [Internett]. https://therecord.media/belgium-investigation-alleged-china-cyber-espionage-vsse.

[25] **C. Livitt og J. Williams**, «A More Complete Exploit for Fortinet CVE-2022-42475,» Bishop Fox, 17. mai 2023. [Internett]. https://bishopfox.com/blog/exploit-cve-2022-42475.

[26] **D. Cary og A. Milenkoski**, «Unmasking I-Soon: The Leak That Revealed China's Cyber Operations,» SentinelOne, 21. februar 2024. [Internett]. https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/.

[27] **U.S. Department of Justice**, «China-Based Hacker Charged for Conspiring to Develop and Deploy Malware That Exploited Tens of Thousands of Firewalls Worldwide,» 10. desember 2024. [Internett]. https://www.justice.gov/opa/pr/china-based-hacker-charged-conspiring-develop-and-deploy-malware-exploited-tens-thousands.

[28] **World Watch team**, «The hidden network: How China unites state, corporate, and academic assets for cyber offensive campaigns,» Orange Cyberdefense, 22. oktober 2024. [Internett]. https://research.cert.orangecyberdefense.com/hidden-network/report.html.

[29] **U.S. Attorney's Office**, District of Columbia, «Chinese Nationals with Ties to the PRC Government and "APT27" Charged in a Computer Hacking Campaign for Profit, Targeting Numerous U.S. Companies, Institutions, and Municipalities,» 5. mars 2025. [Internett]. https://www.justice.gov/usao-dc/pr/chinese-nationals-ties-prc-government-and-apt27-charged-computer-hacking-campaign-profit.

[30] **R. McKerchar**, «Pacific Rim: Inside the Counter-Offensive,» Sophos, 31. oktober 2024. [Internett]. https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/.

[31] **Watchtowr**, «Pots and Pans, AKA and SSLVPN,» 19. november 2024. [Internett]. https://labs.watchtowr.com/pots-and-pans-aka-an-sslvpn-palo-alto-pan-os-cve-2024-0012-and-cve-2024-9474/.

[32] **Eclypsium**, «Flatlined: Analyzing Pulse Secure Firmware and Bypassing Integrity Checking,» 15. februar 2024. [Internett]. https://eclypsium.com/blog/flatlined-analyzing-pulse-secure-firmware-and-bypassing-integrity-checking/.

[33] **NCSC-UK**, «Guidance on digital forensics and protective monitoring specifications for producers of network devices and appliances,» 2025. [Internett]. https://www.ncsc.gov.uk/guidance/guidance-on-digital-forensics-protective-monitoring.

[34] **S. S. Poudel**, «XZ Utils Backdoor: Supply Chain Vulnerability (CVE-2024-3094),» Logpoint, [Internett]. https://www.logpoint.com/en/blog/emerging-threats/xz-utils-backdoor/. [Funnet 5. desember 2024].

[35] **L. Abrams**, «Tietoevry ransomware attack causes outages for Swedish firms, cities,» BleepingComputer, 21. januar 2024. [Internett]. https://www.bleepingcomputer.com/news/security/tietoevry-ransomware-attack-causes-outages-for-swedish-firms-cities/.

[36] **Kripos**, «Cyberkriminalitet,» 2025.

[37] **Semperis**, «Ransomware Risk Report,» 2024. [Internett]. https://www.semperis.com/wp-content/uploads/resources-pdfs/ransomware-report-2024.pdf.

[38] **M. S. McNamee**, «HSE cyber-attack: Irish health service still recovering months after hack,» 5. september 2021. [Internett]. https://www.bbc.com/news/world-europe-58413448.

[39] **Microsoft**, «Microsoft Digital Defense Report,» 2024.

[40] **Mandiant**, «Industry Snapshot: Healthcare,» 2025.

[41] **Mandiant**, «Region Snapshot: The Nordic Region,» 2025.

[42] **National Protective Security Authority**, «Insider Risk: What it is and why it matters,» 16. oktober 2024. [Internett]. https://www.npsa.gov.uk/insider-risk.

[43] **Forsvarsdepartementet**, «Forsvarskommisjonen av 2021— Forsvar for fred og frihet,» 2023. [Internett]. https://www.regjeringen.no/no/dokumenter/nou-2023-14/id2974821/?ch=10.

[44] **CISA ASD NSA GCHQ CCCS ACSC**, «PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,» CISA, 2024.

[45] **O. A. Engen**, «Store norske leksikon - Sabotasje,» 22. februar 2025. [Internett]. https://snl.no/sabotasje.

[46] **Folkehelseinstituttet**, «Tillit og vaksinasjon i Norge,» [Internett]. https://www.fhi.no/ss/korona/koronavirus/folkehelserapporten-temautgave-2021/del-1-9/tillit-og-vaksinasjon-i-norge. [Funnet 22. november 2024].

[47] **D. Zafra, A. Wahlstrom, J. Sadowski, J. Palatucci, D. Baumann og J. Nazario**, «Global Revival of Hacktivism Requires Increased Vigilance from Defenders,» Mandiant, 27. juni 2024. [Internett]. https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism.

[48] **Akamai**, «Fighting the Heat: EMEA's Rising DDoS Threats,» 2024.

[49] **Google**, «Tool of First Resort: Israel-Hamas War in Cyber,» 2024.

[50] **J. Salvador**, «Bigger and badder: how DDoS attack sizes have evolved over the last decade,» Cloudflare, 20. november 2024. [Internett]. https://blog.cloudflare.com/bigger-and-badder-how-ddos-attack-sizes-have-evolved-over-the-last-decade/.

[51] **M. Howard og M. Saltonstall**, «How to protect your site from DDoS attacks with the power of Google Cloud networking and network security,» Google Cloud, 8. oktober 2024. [Internett]. https://cloud.google.com/blog/products/identity-security/how-to-protect-your-site-from-ddos-attacks-with-cloud-networking.

[52] **U.S. Department of Justice**, «Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World,» 16. oktober 2024. [Internett]. https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals.

[53] **D. Zafra, K. Lunden og N. Brubaker**, «We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems,» Mandiant, 22. mars 2023. [Internett]. https://cloud.google.com/blog/topics/threat-intelligence/hacktivists-targeting-ot-systems/.

[54] **S. Vosoughi, D. Roy og S. Aral**, «The spread of true and false news online,» Science, pp. 1146-1151, 2018.

[55] **NHS England**, «Synnovis Ransomware Cyber-Attack,» 2024. [Internett]. https://www.england.nhs.uk/london/synnovis-ransomware-cyber-attack/.

[56] **NRK**, «Ber briter om blod etter dataangrep,» 2024. [Internett]. https://www.nrk.no/urix/blodgiverjakt-i-storbritannia-etter-cyberangrep-i-london-1.16919038.

[57] **S. M. Kerner**, «CrowdStrike outage explained: What caused it and what's next,» TechTarget, 29. oktober 2024. [Internett]. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

[58] **D. Cox**, «Hospitals Around the World Are Struggling After the Great IT Meltdown,» Wired, 19. juli 2024. [Internett]. https://www.wired.com/story/hospitals-crowdstrike-microsoft-it-outage-meltdown/.

[59] **M. Gundersen og S. H. Myrseth**, «PST: Henlegger dataangrep-saken mot departementene,» NRK, 20. oktober 2023. [Internett]. https://www.nrk.no/norge/dataangrepet-mot-departementene-er-henlagt-1.16600410.

[60] **Kommunal- og distriktsdepartementet**, «Departementer utsatt for dataangrep,» 24. juli 2023. [Internett]. https://www.regjeringen.no/no/aktuelt/presseinvitasjon/id2990098/.