Styresak 72/2024
Vedlegg 3

Trusselvurdering 2024

Det digitale trusselbildet mot spesialisthelsetjenesten

HELSE MIDT-NORGE HELSE NORD HELSE SØR-ØST HELSE VEST Norsk helsenett Helse- og KommuneCERT

Sammendrag

Trusselvurdering 2024

Et vellykket cyberangrep mot spesialisthelsetjenesten kan medføre store konsekvenser for spesialisthelsetjenestens evne til å utføre sine primæroppgaver. Dagens trusselbilde er komplisert og i konstant endring som følge av trusselaktørenes økte tilpasningsevne og utvikling av verktøy og metoder.

Vi vurderer at den mest alvorlige trusselen mot spesialisthelsetjenesten fortsatt er kriminelle aktører, og da særlig digital utpressing. Skadepotensialet av et slikt angrep kan være **meget høy**, og kan innebære både nedetid på tjenester, høye kostnader for opprydding og gjenopprettingstid. Evnen organisert kriminelle har til å gjennomføre cyberangrep er **høy**, og de investerer både tid og penger i å videreutvikle sine metoder. De gjennomfører sofistikerte angrep på tvers av sektorer. Målutvelgelsen er opportunistisk, samtidig er det tegn på en mer strategisk målutvelgelse basert på mengden verdifull informasjon. Organiserte kriminelle sin vilje til å utøve angrep mot spesialisthelsetjenesten er **meget høy**, og det er liten risiko for å bli identifisert og straffeforfulgt.

Statlige aktørers vilje til å utøve spionasje utgjør en betydelig trussel mot spesialisthelsetjenesten. Russland har mistet flere diplomater etter invasjonen av Ukraina, og deres tilgang til informasjon om norske interesser er svekket. Russlands vilje til å gjennomføre cyberspionasje mot spesialisthelsetjenesten vurderes til å være **høy**. Kinas vilje vurderes også til å være **høy**, med hensikt å styrke økonomi og posisjon i verdensbildet. Både Russland og Kina har **meget høy** evne til å gjennomføre cyberspionasje uten at dette oppdages. Skadepotensialet knyttet til cyberspionasje er **høyt**, og kan true nasjonale sikkerhetsinteresser.

Hacktivisters vilje til å ramme spesialisthelsetjenesten har gått ned fra i fjor, og vurderes i år til **medium**. Det er viktig å være bevisst på at viljen til hacktivistgrupper kan endre seg raskt med bakgrunn i skiftende geopolitisk situasjonsbilde, betente mediesaker eller andre saker som kan fange hacktivisters oppmerksomhet. Vi ser en klar sammenheng mellom mediesaker og hvordan det fremprovoserer prioriterte mål. Felles for disse er at jo mer oppmerksomhet sakene får i internasjonale og russiske medier, desto mer sannsynlig er det at hacktivister bruker sakene som et påskudd for å gjennomføre angrep. Vi vurderer det som **meget sannsynlig** at skadepotensialet for tjenestenektangrep til å være lavt og kortvarig. Sammenlignet med de andre aktørgruppene vurderes evnenivået til hacktivister som **lav**.

Det vurderes som **meget sannsynlig** at spesialisthelsetjenesten vil oppleve uønskede hendelser som følge av innsidevirksomhet, men at skadepotensialet vil kunne variere fra **ubetydelig** til **meget høyt**. Skadepotensialet fra en innsider vil variere basert på evne og vilje til å skade virksomheten. Dette avhenger av rettighetsnivå, teknisk kunnskap og myndighet.

For å motstå avanserte cyberangrep kreves det en helhetlig tilnærming til sikkerhetsarbeidet. Man må sikre at man har gode grunnleggende sikkerhetsbarrierer som stopper opportunistiske angrepsforsøk for å senke risiko for vellykkede angrep. Spesialisthelsetjenesten kan også tiltrekke oppmerksomhet fra svært avanserte statlige trusselaktører, som kan omgå grunnleggende sikkerhetsbarrierer. Dette betyr at spesialisthelsetjenesten må ha velutviklede metoder for å avdekke uønsket aktivitet og for å igangsette nødvendige tiltak.

Verden er inne i en periode med geopolitisk ustabilitet, blant annet som følge av krigen i Ukraina og Gaza. Dette påvirker samtlige trusselaktører og vil kunne endre prioritering om målutvelgelse raskt. Som følge av trusselbildet mot spesialisthelsetjenesten er det derfor avgjørende å jobbe i flere dimensjoner innenfor cybersikkerhetsområdet.

Innhold

Forsidebilde: Shutterstock | Grafisk design: Gnist Design

Hvordan lese rapporten

Sannsynlighetsord
I trusselvurderingskapitlet er vurderingene plassert på slutten av hvert delkapittel for tydelig å skille egne vurderinger fra informasjon hentet fra andres kilder. Kildereferanser er viktige for integritet, sporbarhet og annerkjennelse av andres arbeid. I denne rapporten brukes tall i parentes i teksten, for eksempel [99]. Referansene finner man igjen i kildelisten bakerst i rapporten. I våre vurderinger er det nødvendig at begrepsbruken er konsekvent. Derfor benyttes sannsynlighetsordene listet i tabellen til høyre.

Oversikt over trusselnivåer
Nivåene i tabellen til høyre brukes for å gjøre en overordnet totalvurdering av trusselaktørenes vilje og evne, og en grov vurdering av skadepotensial for spesialisthelsetjenesten. Skadepotensialet er avhengig av mange faktorer og er svært vanskelig å forutsi. Vi ønsker likevel å gi leseren en indikasjon på skadepotensialet av et angrep fra de ulike aktørene. Vurderingen av dette er basert på åpne kilder og er ikke knyttet til eget sårbarhetsnivå. Evnenivået er basert på aktørenes ressurser med hovedvekt på cyberkapabiliteter. Hensikten med tabellen er å kunne gi leser en god oversikt og gjøre det enklere å sammenligne aktørene. Det presiseres at teksten i vurderingene bør vektlegges mer enn tabellene.

Konfidensnivå
Rapporten er i hovedsak basert på pålitelige kilder og resultatene presenteres derfor generelt med et høyt konfidensnivå. Dersom enkelte av vurderingene er usikre eller basert på et tynt kildegrunnlag, er vurderingsordet markert med * for medium konfidensnivå eller ** for lavt konfidensnivå.

Avgrensninger
Tradisjonell etterretningsprossess ligger til grunn for utarbeidelsen av denne rapporten. Trusselvurderingen er utarbeidet for spesialisthelsetjenesten og er produsert ved å analysere, sammenstille og vurdere sentrale åpne rapporter og interne kilder. De nasjonale trussel- og risikovurderingene fra Politiets sikkerhetstjeneste (PST) [1], Etterretningstjenesten (ETJ) [2] og Nasjonal Sikkerhetsmyndighet (NSM) [3] er vektlagt tyngst.

Trusselvurderingen skal ta for seg de mest relevante typene trusselaktører og deres evne og vilje til negativt å påvirke spesialisthelsetjenestens verdier, primært gjennom digitale operasjoner og verktøy. Terrorisme i tradisjonell form er et eksempel på en trussel som ikke dekkes i vurderingen. Videre dekkes ikke utilsiktede hendelser, som for eksempel naturkatastrofer og strømbrudd. Kildegrunnlaget til denne vurderingen er basert på observerte og rapporterte hendelser. Dette er en avgrensning man må være oppmerksom på, da det er mye trusselaktivitet som aldri blir fanget opp.

Vurderingene er basert på informasjon innhentet frem til 22. april 2024 og må forstås deretter. Tidsperspektivet for vurderingene er ett år fra rapporten publiseres.

Sannsynlighetsord	Forklaring	Prosent
Meget sannsynlig	Det er meget god grunn til å forvente	>90%
Sannsynlig	Det er grunn til å forvente	60-90%
Mulig (like sannsynlig som usannsynlig)	Det er like sannsynlig som usannsynlig	40-60%
Lite sannsynlig	Det er lite grunn til å forvente	10-40%
Meget lite sannsynlig	Det er svært liten grunn til å forvente	<10%

Vilje	Evne	Skadepotensiale
Meget høy	Meget høy	Meget høyt
Høy	Høy	Høyt
Medium	Medium	Medium
Lav	Lav	Lavt
Meget lav	Meget lav	Meget lavt

Konfidensnivå	
Høy	(Ingen merknad, hele rapporten)
Medium	*
Lav	**

Foto: Luis Villasmil, Unsplash

Kapittel 1

Oversikt over trusselaktører som er mest relevant for spesialisthelsetjenesten

Trusselvurderingen skal beskrive trusselbildet mot spesialisthelsetjenesten fra relevante trusselaktører. For å beskrive trusselbildet mot spesialisthelsetjenesten på en helhetlig måte, er trusselaktørene gruppert etter en kombinasjon av organisering og intensjon.

Trusselvurderingen er delt inn etter denne grupperingen, men skillet mellom disse blir stadig mer utydelige. Dette skyldes økt samarbeid mellom aktørene. Det er utfordrende for virksomheter å attribuere hvilken aktør som står bak et angrep.

For eksempel kan det være flere aktører inne i et system under et cyberangrep, som gjerne bruker samme skadevare og har stort overlapp i metoder og verktøy. I tillegg er det flere som peker på ulike former for samarbeid og grader av knytninger mellom statlige aktører, organiserte kriminelle aktører og hacktivister [4] [5] [6] [7].

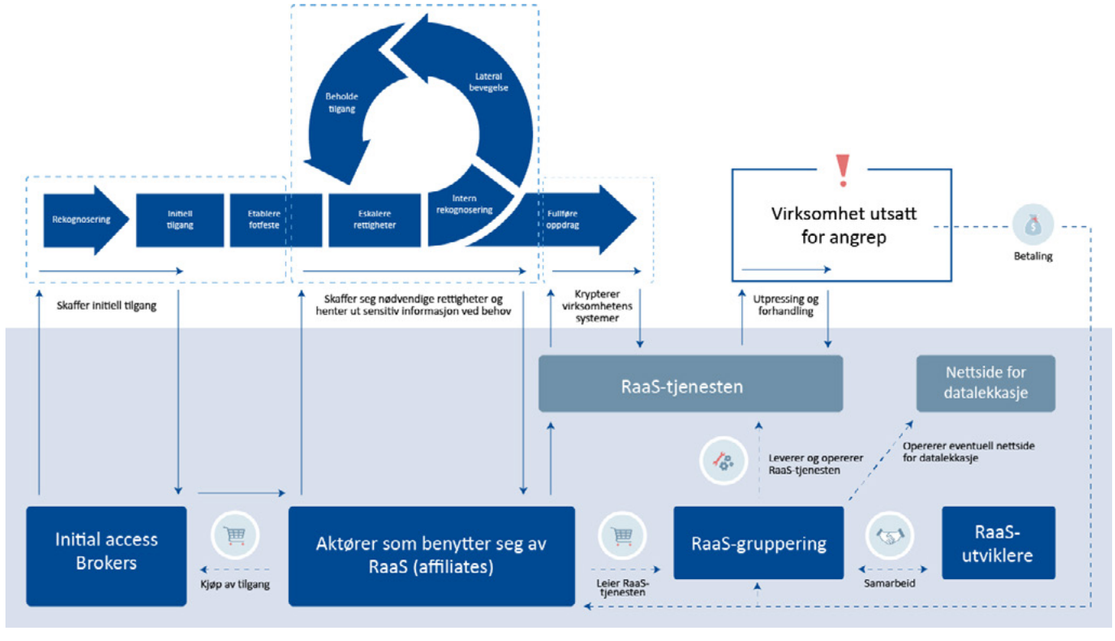
- **Organiserte kriminelle aktører**
  I denne rapport anses de som aktører som opererer ulovlig i cyberdomenet, og er hovedsakelig drevet av økonomisk vinning. Et eksempel på slike aktører er de som driver med digital utpressing.

- **Statlige aktører**
  Statlige aktører defineres her som andre staters etterretnings- og sikkerhetstjenester, inkludert aktører engasjert av disse. Statlige aktører utfører blant annet etterretningsoperasjoner i cyberdomenet.

- **Hacktivister**
  Hacktivister kan være enkeltpersoner eller grupper, og utfører digitale angrep for å formidle politiske eller ideologiske budskap.

- **Innsidere**
  Innsidere defineres som en person som har eller har hatt legitim tilgang til virksomhetenes systemer eller verdier, og som misbruker tilgangen for å skade virksomheten. Innsideaktivitet kan gjennomføres på egenhånd, eller på vegne av en statlig aktør, kriminelle, andre enkeltindivider eller for egen vinning. Fellesnevneren er at innsideren har kapasitet, intensjon og mulighet til å utføre uønskede handlinger.

Foto: Shutterstock



Figur 4: RaaS-økosystem, modellen er inspirert av Microsoft [22].

Kapittel 2

Organiserte kriminelle aktører

Aktørlandskapet knyttet til organiserte kriminelle aktører er et komplekst økosystem som består av flere undergrupper av aktører [8], og det er vanskeligere å skille grupperinger fra hverandre. Årets trusselvurdering vil derfor vurdere organiserte kriminelle aktører som helhet.

Felles for grupperingene innenfor organiserte kriminelle er at de primært drives av økonomisk vinning. Aktørenes økonomiske motivasjon er høy, og de er velorganiserte. De organiserte kriminelle aktørene samarbeider på tvers av landegrenser og innenfor økosystemet av kriminelle. Aktørene lærer av angrepene de gjennomfører, og forbedrer kontinuerlig sine verktøy, teknikker og modus operandi. Dette øker aktørenes kapabiliteter og robusthet, fordi de blant annet har mulighet til å spesialisere seg og effektivisere angrepene [9] [10].

Innenfor økosystemet av kriminelle finnes det ulike grupperinger. En viktig gruppering er Ransomware-as-a-Service (RaaS)-aktørene som stiller med skadevare som krypterer virksomhetens systemer, i tillegg til kommunikasjons- og betalingsløsninger. Tjenestene de tilbyr leies ut til andre aktører for en andel av fortjenesten i angrepet, ofte 10-20 % [11].

RaaS-modellen er utviklet som en forretningsmodell som gjør at RaaS-aktørene kan skalere raskt og øke inntjening. Samtidig kan de operere med lav risiko for å bli tatt, fordi aktørene bak RaaS eksponerer seg ikke i nettet til virksomheter.

Trusselaktørene som benytter RaaS kalles affiliates i RaaS-modellen (se figur på neste side). Det er affiliates som gjennomfører angrep hos virksomheter og kjører krypteringsskadevaren som de leier av en RaaS-aktør [11].

Organiserte kriminelle aktørers utvikling

Global statistikk viser at angrep mot helsesektoren har økt noe, sett opp mot fjoråret. Trusler knyttet til cyberspionasje og cyberkriminalitet anses mest fremtredende for helsesektoren [11] [12]. De fleste angrepene som er gjennomført av organiserte kriminelle er opportunistisk og finansielt motivert, men de siste to årene er det observert aktivitet som tyder på større grad av kartlegging og målrettethet [13] [14].

Organiserte kriminelle aktører peker i større grad ut virksomheter som mulig mål basert på sårbarheter eller endringer [15] [14] [16]. En stor del av organiserte kriminelle aktører utfører opportunistiske kampanjer. Disse refereres gjerne til som *"Big Game Hunting (BGH)"*. Hensikten er å oppnå tilgang til systemer eller finne sårbarheter som kan utnyttes. BGH benytter mer strategisk målutvelgelse av ofrene, og de går gjerne etter virksomheter som har sensitiv og verdifull informasjon [17] [14] [4] [18]. Disse aktørene velger sine ofre basert på deres mulighet til å betale løsepenger, og sannsynligheten for at de vil betale. Helseinstitusjoner trekkes frem som aktuelle ofre, blant annet som følge av at nedetid kan ha kritiske konsekvenser [18].

Organiserte kriminelle og den geopolitiske situasjonens påvirkning

Verden er inne i en periode med geopolitisk ustabilitet, blant annet som følge av krigen i Ukraina og Gaza. Dette påvirker ulike grupperinger innenfor organiserte kriminelle aktører. Etter invasjonen av Ukraina har spesielt russiskbaserte organiserte kriminelle opplevd forstyrrelser i sitt økosystem [19]. Endringer i den geopolitiske situasjonen kan være spesielt interessant for aktører som spesialiserer seg på videresalg av informasjon. Verdien av informasjon kan endre seg som følge av geopolitiske endringer [20], noe som kan påvirke målutvelgelsen til trusselaktørene. De endrer gjerne strategi og taktikk basert på situasjonen for å oppnå profitt.

Organiserte kriminelles aktørers vilje

Organiserte kriminelle aktører har primært økonomisk vinning som formål, og derfor er også deres angrep mindre målrettet. Motivasjonen for å utføre angrep på helsesektoren er hovedsakelig opportunistisk. Metodene aktørene benytter varierer, blant annet ved bruk av skadevare, phishing og sosial manipulasjon.

Enkelte aktører henter ut sensitiv informasjon fra virksomheter for å selge det videre, for eksempel i forbindelse med industrispionasje. Andre ganger kan målet være å få tak i påloggingsopplysninger, enten for direkte salg eller som et steg i å få tak i informasjon som kan selges [15] [20] [21] [22].

Gjennom det siste året har det vært en økning i salg av kompromitterte tilganger med 20 %, og det er stor spredning i geografi og sektorer som rammes [23]. Salg skjer hovedsakelig til andre organiserte kriminelle, samtidig som det i økende grad også selges til statlige aktører. Fremover forventes det at de organiserte kriminelle aktørene som selger kompromitterte tilganger og utvikler skadevaren, fortsetter å knytte tettere bånd [9] [21] [4].

En annen metode aktørene benytter, er å ta kontroll over informasjon eller systemer til en virksomhet og gjøre de utilgjengelig ved bruk av skadevare som krypterer systemene. Globalt har et større antall helseinstitusjoner og sykehus vært offer for utpressingsangrep, der løsepengesummen har vært av en betydelig størrelse i antall angrep med bruk av utpressingsskadevare [12] [11] [4].

Aktørene som benytter utpressingsskadevare som metode har også tatt i bruk det som omtales som dobbel utpressing. Her henter aktørene ut sensitiv informasjon fra offerets systemer, for eksempel helseopplysninger. Deretter krever aktøren løsepenger fra virksomheten for å ikke offentliggjøre eller videreselge disse opplysningene [11] [21].

Organiserte kriminelle aktørers evne
Fremgangsmåtene til aktørene er i kontinuerlig utvikling. I løpet av den siste perioden har man sett en økende trend i å benytte kunstig intelligens (KI). KI benyttes både for å gjennomføre mer sofistikert phishingangrep, og til å utvikle mer avansert skadevare [1] [28]. Aktørene spesialiserer seg også innenfor sektorer og systemer, og er ofte bare en del av et større bilde [15] [24] [25]. Aktørene lærer og utvikler metodene sine fra angrepene de gjennomfører. I tillegg samarbeider de med andre grupper innenfor økosystemet av organiserte kriminelle [21] [15].

Siden flere av aktørene ikke utfører fullverdige angrep selv, er det lavere risiko for å bli oppdaget og straffeforfulgt. Samtidig bidrar de sterkt til profesjonelle cyberangrep gjennom spesialiseringer, som for eksempel salg av tilganger som andre aktører benytter [8] [10].

Metoden som oftest benyttes av cyberkriminelle er utpressingsskadevare, og denne trenden er økende. Evnen og kapabilitetene til disse aktørene er under kontinuerlig utvikling, som følge av at ny teknologi og nye fremgangsmetoder blir tilgjengelige. Samtidig viser utviklingen en økning knyttet til utpressing istedenfor kryptering av virksomheters informasjon og data [4] [16].

Det forventes at sosial manipulering fremover blir mer sofistikert, der metoder som fakturasvindel og direktørbedrageri fortsetter [4]. Antall angrep mot bedrifter og organisasjoner ble redusert i 2023 sett opp imot 2022. Det gjennomsnittlige utbyttet økte derimot til nær det dobbelte. En av utfordringene med tallgrunnlaget på dette området er at det mest sannsynlig er store mørketall grunnet underrapportering [24]. Det er observert flere forsøk på direktørbedrageri innenfor helsesektoren, og dette er en trussel som forblir aktuell.

Vurdering:

Organiserte kriminelle aktører

Overordnet vurdering mot spesialisthelsetjenesten: Organiserte kriminelle aktører			
	Vilje	**Evne**	**Skadepotensiale**
Organiserte kriminelle aktører	Meget høy	Høy	Meget høyt

Vi vurderer at den mest alvorlige trusselen mot spesialisthelsetjenesten er organiserte kriminelle aktører. Organiserte kriminelle aktører er opportunistiske i sin målutvelgelse. Motivet er økonomisk vinning, og aktørenes vilje er **meget høy**. Dette er begrunnet i økt antall angrep globalt, inkludert mot helsesektoren. Aktørene har stor spredning i valg av mål og fremgangsmåter, både med hensyn til land og sektor, men det er fortsatt hovedsakelig opportunistisk utvelgelse. Samtidig er det økende samarbeid mellom aktørene og noe mer strategisk målutvelgelse basert på sensitiv og verdifull informasjon.

Aktørenes evne er **høy**, da de er profesjonelle og tilpasningsdyktige med høy motivasjon for inntjening. Profesjonaliteten fortsetter å øke, og vi ser at aktørene stadig forbedrer sine teknikker. Verktøyene aktørene benytter er blitt betydelig kraftigere og lettere tilgjengelig. Angrepsmetodene er sofistikerte, og trusselaktørene bruker god tid på å gjennomføre angrep. Videre bruker de avanserte metoder for å skjule sin aktivitet. Summen av dette har gjort at suksessraten på angrepene er høyere, noe som medfører økt sannsynlighet for kompromittering. Aktørene har også lav risiko for å bli straffeforfulgt.

Skadepotensialet som følge av angrep fra organiserte kriminelle er vurdert til **meget høyt**, basert på hendelser i sammenlignbare virksomheter globalt. Et angrep som tar ut kritiske systemer kan ramme elektiv og akutt pasientbehandling på kort og lang sikt, og medfører høye kostnader i gjenopprettelse. I tillegg kan kompromittering og publisering av person- og helseopplysninger kunne skade spesialisthelsetjenestens tillit hos befolkningen.

Det gjennomføres kontinuerlig forsøk på angrep mot spesialisthelsetjenesten, og vi vurderer det som **meget sannsynlig** at spesialisthelsetjenesten vil utsettes for cyberangrep gjennomført av organiserte kriminelle aktører. Aktørenes vilje er **høy**, og det er verdifull informasjon som kan omsettes til økonomisk vinning, både gjennom videresalg og utpressing. I tillegg vil nedetid på kritiske systemer kunne medføre alvorlige konsekvenser. Utvikling i den geopolitiske situasjonen vil også kunne påvirke målutvelgelse for organiserte kriminelle aktører, og spesialisthelsetjenesten vil kunne bli et mer attraktivt mål.

Foto: Shutterstock

Kapittel 3

Statlige trusselaktører

I trusselvurderingene fra etterretnings- og sikkerhetstjenestene (EOS-tjenestene) beskrives Russland som den største etterretningstrusselen mot Norge i 2024, og trusselen fra Kina er framhevet som økende [2]. Cyberoperasjoner er den foretrukne metoden brukt av fremmede etterretningstjenester for å gjennomføre spionasje, påvirkning og destruktive cyberangrep. Cyberoperasjoner er kostnadseffektiv og kan ramme et større antall mål med lav risiko for oppdagelse [26] [22] [1] [12] [3].

Spesialisthelsetjenesten forvalter betydelig mengde informasjon som har verdi for statlige trusselaktører, dette gjør oss utsatt for cyberangrep i årene fremover. EOS-tjenestene trekker frem Russland og Kina som de som står bak de mest avanserte operasjonene mot norske virksomheter. Russland og Kina har styrket det strategiske samarbeidet, der de har en sammenfallende interesse i å svekke Vesten [17] [27] [28] [22] [3].

3.1 Cyberspionasje

Cyberspionasje er spionasje eller etterretningsoperasjoner i cyberdomenet gjennomført av statlige trusselaktører. Enkelte land gjennomfører cyberspionasje av politiske grunner, for å oppnå økonomisk vinning eller for konkurransefortrinn. Utviklingen i cyberdomenet fører til at denne typen etterretningsvirksomhet kan gjennomføres i mye større skala enn tidligere. Cyberspionasje er i utgangspunktet tyveri av sensitiv informasjon, uten at motparten forstår at informasjonen er på avveie. Dette kan omfatte både selve informasjonen og systemene, hvor denne informasjonen ligger lagret, som er kompromittert. Derfor er det viktig for trusselaktøren at den tekniske gjennomføringen ikke medfører forstyrrelser på målet og at aktiviteten ikke blir oppdaget [14] [35] [26] [1].

Spesialisthelsetjenesten er en grunnleggende tjenestene i samfunnet og har en viktig beredskapsfunksjon for ivaretakelse av liv og helse. Dette gjør spesialisthelsetjenesten trusselutsatt på lik linje med andre deler av totalforsvaret og kritisk infrastruktur. Forskningsdata, informasjon om beredskap, og sensitiv informasjon som helse- og personopplysninger er noen av verdiene som statlige aktører ønsker tilgang til [36] [24] [14] [1] [22]. Spesialisthelsetjenesten har tette forbindelser med ulike forskningsinstitusjoner, og forskning er en viktig og integrert del av helsesektoren. Globalt er det rapportert om interesse for medisinsk forskning fra statlige trusselsaktører [11] [4] [29] [30].

Foto: Christopher Lindseth Moen, Sykehuspartner HF.

Russland

Norges medlemskap i NATO, strategiske plassering og grense til Russland påvirker den vedvarende høye etterretningstrusselen fra Russland. Russiske EOS-tjenester har behov for informasjon som styrker egen situasjonsforståelse i dagens sikkerhetspolitiske situasjon, og Norges evne til å håndtere kriser spesielt hvor russiske interesser er involvert [1]. Russlands avhengighet til Kina blir stadig større som en konsekvens av de vestlige sanksjonene i forbindelse med krigen i Ukraina. Landene samarbeider kommersielt og innen forskning i Arktis [2] [17].

Vilje

Russland har høy vilje til å gjennomføre cyberspionasje mot norske mål. Både sivile og militære EOS-tjenester i Russland har informasjonsbehov knyttet til Norge. Dette inkluderer et varig behov for informasjon om totalforsvaret og beredskapsapparatet, som spesialisthelsetjenesten er en del av. Kritisk infrastruktur er et mål for russisk etterretning fordi tilgangen kan benyttes til spionasjeformål, eller til forberedelse av destruktive angrep som kan utnyttes i en tilspisset situasjon [22]. Spesialisthelsetjenesten har store mengder med helse- og personopplysninger som kan brukes som et virkemiddel innenfor spionasje og kan ha høy verdi for utenlandsk etterretning. Helseopplysninger kan brukes til å presse eller utnytte myndighetspersoner eller personer med høyt rettighets-nivå i IKT-systemer
[1] [3] [28] [30] [21].

Evne

Russiske cyberaktører bruker hele spekteret av tilgjengelige kapasiteter i gjennomføringen av cyberspionasje. Russiske cyberaktører har kapasitet til å infiltrere nettverk, infrastruktur, skytjenester og kan etablere full og vedvarende tilgang til ønsket infrastruktur. Russiske etterretningstjenester er kjent for å benytte ulike former for samarbeid mellom hacktivister og organiserte kriminelle miljøer, hensikten er å skjule hvem som står bak angrepet [4] [5] [6] [7] [31] [27] [22].

Kina

Kinesiske etterretningstjenester utnytter hele spekteret av cyberdomenet i sine cyberoperasjoner og bruker alle tilgjengelige verktøy og digital infrastruktur for å skjule sin egen aktivitet. Kinesiske myndigheter gjennomfører cyberspionasje i utstrakt grad mot blant annet myndigheter, forsvar og helse. Kina fortsetter å utfordre det vestlige fellesskapet på flere måter, der de søker å kontrollere strategisk infrastruktur, ressurser og verdikjeder. Kina jobber aktivt mot nordområdene, for å sikre fremtidig ressursutvinning og strategisk posisjonering [17] [2] [27] [22] [11] [32] [22].

Vilje

Kina har rettet en betydelig andel av sine cyberoperasjoner mot Vesten, og samtlige av Norges EOS-tjenestene forventer en økning av aktiviteten i Norge årene som kommer [33] [21]. Flere kinesiske trusselaktører har gjennomført globale cyberspionasjeaksjoner i 2023 [22] [27] [30]. Den amerikanske cybersikkerhetstjenesten (HC3) bekrefter at flere kinesiske trusselaktører har gjennom årene gjennomført cyberspionasje mot helsesektoren i USA og Sør-Europa, der angrepene har vært rettet mot blant annet medisinsk teknisk utstyr og medisinsk forskingsdata [29] [1] [2].

Evne

Kinesiske etterretningsorganisasjoner har evne til å gjennomføre avanserte cyberspionasjeoperasjoner. De har kapasitet til å infiltrere nettverk, infrastruktur, skytjenester og etablere full og vedvarende tilgang til informasjon og styringssystem. Kina vil utgjøre en betydelig etterretningstrussel mot norske virksomheter i tiden fremover [4] [19] [22] [33] [32] [34] [43].

Kinas kontraetterretningslov gir en svært bred forståelse av «etterretningsaktivitet», og omfatter innhenting av informasjon av betydning for investeringer og produksjon i Kina. Enhver kinesisk borger, virksomhet og organisasjon plikter ifølge loven til å bistå Kinas etterretningstjeneste ved behov. For kinesiske kommersielle teknologiselskaper betyr dette i praksis at all teknologi og kunnskap fra kinesiske selskaper kan bli tilgjengeliggjort for kinesiske myndigheter [2] [1].

Kina søker å utnytte sårbarheter i internetteksponerte tjenester for å etablere fotfeste i informasjonssystemer. I 2023 har det videre blitt observert en økning av mer sofistikerte målrettede phishing-kampanjer fra kinesiske trussel aktører. I løpet av 2023 er det observert at kinesiske aktører i større grad har benyttet seg av sosiale medier for sosial manipulering og rekruttering av innsidere [22] [27] [32].

Iran

Iran fokuserer i hovedsak sine cyberspionasjeoperasjoner mot sine regionale naboer, men har også angrepet europeiske land og USA. Iranske statlige aktører bruker stadig mer sofistikerte metoder og utnytter teknologi som er lett tilgjengelig. Dette inkluderer blant annet å skjule infrastruktur for kommando og kontroll (C2) av skadevare i offentlige skymiljøer, og de utnytter nulldagssårbarheter raskere [22] [4] [27] [9] [35] [36].

Vilje

Iran har gjennomført cyberspionasje mot forsknings- og utdannings-sektoren i Norge. Politiets sikkerhetstjeneste (PST) forventer at iranske aktører vil ramme norske virksomheter i 2024. Iranske aktører vil i året som kommer drive cyberspionasje som del av sin etterretningsaktivitet mot Norge. Norske virksomheter, inkludert spesialisthelsetjenesten, kan være mål for cyberspionasje fra iranske aktører [22] [1] [2].

Evne

Iran har betydelige evner til å gjennomføre cyberspionasje. I 2023 har Iran styrket sine kapabiliteter, og utnytter nulldagssårbarheter raskere. De har også gjennomført operasjoner i skymiljøer, hvor formålet er tilgang til informasjon eller bruke skymiljøet som verktøy for å etablere fotfeste [22] [36] [4] [35].

Iranske statlige aktører bruker regelmessig tilpassede verktøy i sine operasjoner. Verktøyene gir aktøren evnen til å etablere tilstedeværelse og unngå oppdagelse. Utnyttelse av nulldagssårbarheter i programvare hjelper trusselaktører å holde seg et skritt foran den som er angrepet. Iranske statlige aktører bruker tilpassede verktøy som gjør det mulig å etablere tilstedeværelse og unngå oppdagelse [22] [27].

Nord-Korea

Nordkoreanske cyberoperasjoner har blitt mer sofistikerte enn tidligere år, og begynner å nærme seg nivået til aktører fra Russland og Kina [22] [36].

Vilje

Nord-Korea trekkes fremdeles frem som en aktør som vil utføre cyberspionasje mot norske mål i 2024. Nord-Korea bruker i utgangspunktet cyberoperasjoner for å gjennomføre industrispionasje for å styrke landets forsvarsevne og øke Nord-Koreas svake økonomi. Nordkoreanske cyberaktører har stjålet informasjon fra norske virksomheter som kan skade norske sikkerhetsinteresser [1] [37] [22] [2] [38].

Evne

Nord-Korea har kapasitet til å gjennomføre cyberspionasje og har gjennomført flere vellykkede angrep mot finansinstitusjoner, militære og politiske organer i Vesten. Nord-Korea benytter offentlig kjent og egenutviklede skadevarer i cyberangrep. De utnytter sårbarheter blant annet i internetteksponerte tjenester, skytjenester og det har blitt observert kampanjer hvor målet er å få tilgang til påloggings-informasjon [22] [36].

Vurdering:

Cyberspionasje

Overordnet vurdering av trusselen fra cyberspionasje mot spesialisthelsetjenesten			
Land	**Vilje**	**Evne**	**Skadepotensiale**
Russland	Høy	Meget høy	Høyt
Kina	Høy	Meget høy	Høyt
Iran	Medium	Høy	Høyt
Nord-Korea	Meget lav	Høy	Høyt

Det vurderes som **sannsynlig** at statlige aktører har evne og vilje til å gjennomføre cyberspionasje mot spesialisthelsetjenesten i 2024. Det vurderes som **meget sannsynlig** at Russland og Kina har **høy** vilje til å gjennomføre cyberspionasje mot spesialisthelsetjenestens verdier, men de har ulike målsetninger med angrepene. Russlands fokus vil dreie seg om tilgang til informasjon som styrker deres generelle situasjonsforståelse, men også forhold til NATO-landene.

Det vurderes som **meget sannsynlig** at Russland har **høy** vilje til å utøve spionasje mot spesialisthelsetjenestens verdier som omfatter beredskap og krisehåndteringsevne.

Kinas fokus er rettet mot spionasje for å styrke egen økonomi og posisjon i verdensbildet. Det vurderes derfor som **sannsynlig** at Kina har vilje til å gjennomføre spionasje mot forskningsmiljøer, også innen spesialisthelsetjenesten.

Cyberspionasje mot spesialisthelsetjenesten er skadepotensiale vurdert til **høyt**, det å bli utsatt for cyberspionasje vil nødvendigvis ikke påvirke vår evne til å levere helsetjenester i regionene. Imidlertid kan det true konfidensialiteten og i verstefall tilgjengeligheten til informasjonen spesialisthelsetjenesten forvalter, og derfor også sikkerheten. Cyberspionasje fra russiske aktører vil utgjøre den største trusselen fra statlige aktører mot spesialisthelsetjenesten.

Det vurderes som **meget sannsynlig** at statlige aktørers EOS-tjenester innehar kapabiliteter gode nok til å omgå et godt grunnleggende sikkerhetsnivå.

Det vurderes som **meget sannsynlig** at statlige aktører har evne til å omgå sikkerhetsmekanismer ved å utnytte ikke allment kjente sårbarheter, såkalte nulldagssårbarheter.

3.2 Destruktive cyberangrep

Destruktive cyberangrep er i denne vurderingen definert som digitale angrep med hensikt å ødelegge eller forandre informasjon, data eller programvare slik at de ikke kan benyttes uten vesentlig gjenoppretting [12] [21].

En rekke stater har evne til å gjennomføre destruktive cyberangrep mot kritisk infrastruktur, som spesialisthelsetjenesten er en del av. Samtidig er det globalt observert nedgang i destruktive cyberangrep fra statlige aktører [22] [2] [27]. Gjennom verdikjedeangrep vil spesialisthelsetjenesten kunne bli påvirket av destruktive cyberangrep ved at underleverandør blir angrepet. Det har blitt registrert målrettede angrep mot underleverandører som har forbindelse til konfliktområder som krigen i Ukraina og nå i senere tid i Midtøsten [1] [12].

Hvis fremmede staters vilje til å bruke destruktive cyberangrep mot kritisk infrastruktur i Norge endrer seg, kan destruktive cyberangrep ramme spesialisthelsetjenesten med alvorlige konsekvenser. Spesialisthelsetjenesten kan også påvirkes av destruktive cyberangrep mot andre deler av kritisk infrastruktur eller underleverandører, som kraftsektoren eller vannforsyning [22] [34]. Statlige trusselaktørers vilje og evner varierer, de bruker ofte lignende eller samme metoder når de distribuerer cyberangrep.

I utgangspunktet har helse et vern mot angrep gjennom Genèvekonvensjonene. Imidlertid har det blitt bekreftet i at russiske styrker har angrepet feltsykehus og ambulanser i Ukraina. I tillegg er det bekreftet av FN at Israel har angrepet på helseinstitusjoner i Gaza [39] [31]. Risikoen er at slike angrep kan skape en presedens som i større grad enn før legitimerer helse som mål i konflikter og krig. Denne utviklingen kan føre til at terskelen for å gjennomføre destruktive cyberangrep mot helse reduseres.

Russland

Vilje

Russiske statlige aktørers vilje til å gjennomføre destruktive angrep er i hovedsak for å støtte andre typer maktmidler. Viljen til å gjennomføre destruktive angrep mot norske mål er lav, og det observeres en generell nedgang globalt. Dette har sammenheng med økningen som skjedde i forbindelse med angrepet på Ukraina. Trusselen kan øke igjen i en skjerpet sikkerhetspolitisk situasjon eller militær konflikt [1] [2] [3] [22].

Evne

Russland har meget høy evne til å gjennomføre destruktive cyberangrep og har over tid praktisert slike angrep. I Russlands hybride krigføring mot Ukraina har russiske aktører gjennomført en rekke destruktive cyberangrep mot kritisk infrastruktur i landet. Russland er kjent for å bruke stedfortredere, som cyberkriminelle eller hacktivist-grupper, for å gjennomføre ulike typer cyberangrep [4] [40] [19] [22] [3] [27].

Kina

Vilje

Kinas vilje til å gjennomføre destruktive cyberangrep mot spesialisthelsetjenesten er uendret fra fjoråret. Imidlertid kan endring i kinesiske interesser påvirke viljen til å gjennomføre destruktive cyberangrep. [22] [27] [32].

Evne

Kina har evne til å gjennomføre destruktive cyberangrep. I 2023 oppdaget sikkerhetsmyndigheter i USA at kinesiske aktører hadde vært inne i flere datasystemer tilknyttet kritisk infrastruktur [33]. Amerikanske EOS-tjenester vurderte med stor sikkerhet at aktøren forhåndsposisjonerte seg på IT-nettverk for å forstyrre funksjoner i fremtiden. Aktørens valg av mål og atferdsmønster var ikke i samsvar med tradisjonell cyberspionasje eller etterretningsinnsamlingsoperasjoner [8] [22]. En viktig del av Kinas militære cyberstrategi er å kunne gjennomføre destruktive cyberangrep for å binde en nasjons ressurser til en intern krise som vil skifte fokus fra en konflikt mot Kina [33] [22] [27] [32].

Iran

Vilje

Iran fokuserer i hovedsak sine destruktive cyberangrep mot egen region, men har gjennomført angrep mot USA og land i Europa [35]. Iranske aktører har aktivt gjennomført slike angrep i mange år, blant annet mot Saudi Arabia og Israel [4]. Med angrepene mot mål i USA og Albania kan man se økt vilje til å gjennomføre slike angrep mot land som Iran oppfatter at jobber mot iranske interesser. Det er observert et skifte fra destruktive operasjoner til cyberspionasje fra Iran [22].

Evne

Iranske aktører har demonstrert betydelig evne i gjennomføring av destruktive cyberangrep, blant annet mot Saudi Arabia og Israel. Iran bruker også cyberdomenet aktivt mot stater som rammer eller jobber mot Iranske interesser. Iran har historisk fokusert sine operasjoner mot myndigheter, industri, infrastruktur og helse. Det siste året har Iran styrket sine kapabiliteter og har i større grad gjennomført operasjoner i skymiljøer i tillegg til å unytte nulldagssårbarheter raskere [27] [22] [35].

Nord-Korea

Vilje

Nord-Korea har i utgangspunktet økonomiske motiver i sine operasjoner, og dette har ikke endret seg. Nordkoreanske aktører har gjennomført målrettet angrep mot selskaper innenfor kryptovaluta, men benytter også utpressingsverktøy [22] [38].

Evne

Nord-Koreas fokus på økonomisk vinning har landet opparbeidet seg en betydelig kapasitet som kan benyttes til å gjennomføre destruktive cyberangrep. De benytter offentlig tilgjengelige, samt egenutviklede verktøy og skadevare. Nordkoreanske aktører utnytter sårbarheter i internetteksponerte tjenester, og det har blitt observert kampanjer der målsetningen er å få tilgang til påloggingsinformasjon for å benytte disse i senere destruktive cyberangrep [22] [36].

Vurdering:

Destruktive cyberangrep

Overordnet vurdering av trusselen fra destruktive cyberangrep i spesialisthelsetjenesten

Land	Vilje	Evne	Skadepotensiale
Russland	Lav	Meget høy	Meget høyt
Kina	Meget lav	Meget høy	Meget høyt
Iran	Meget lav	Høy	Meget høyt
Nord-Korea	Meget lav	Høy	Meget høyt

Destruktive cyberangrep har **meget høyt** skadepotensiale for spesialisthelsetjenesten, fordi systemer blir utilgjengelige, eller at sensitiv informasjon blir kompromittert. Trusselaktørene har **høy** til **meget høy** evne til å gjennomføre denne typen angrep.
På bakgrunn av EOS-tjenestene sine nasjonale vurderinger kan det ikke utelukkes forsøk på å etablere tilstedeværelse i vår kritiske infrastruktur for fremtidige destruktive cyberangrep. Det vurderes som **mulig** med **lav konfidens** at spesialisthelsetjenesten kan være utsatt for forsøk fra aktører som ønsker å posisjonere seg i operasjonell teknologi (OT) for senere å gjennomføre destruktive cyberangrep eller digital sabotasje.

Russland har **meget høy** evne til å gjennomføre destruktive cyberangrep, men viljen vurderes som **lav**, imidlertid kan trusselen stige i forbindelse med en skjerpet politisk eller militær konflikt. Viljen til å gjennomføre destruktive cyberangrep mot spesialisthelsetjenesten fra Kina, Iran og Nord-Korea, vurderes til **meget lav** og det er **meget lite sannsynlig** at aktørene gjennomfører angrep slik situasjonen er i dag.

Foto: Shutterstock

3.3 Påvirkningsoperasjoner

En påvirkningsoperasjon er en samordnet innsats for å påvirke en meningsdannelse hos enkeltpersoner eller grupper gjennom tilgjengelige verktøy, som sosiale medier, falske nyheter eller påvirkning av tjenester [41] [26]. Statlige aktører har i større grad brukt cyberdomenet til å spre sine narrative og fronte sine verdier til et større publikum. Det er rapportert mange eksempler på dette i den pågående krigen i Ukraina, hvor russiske aktører bruker sosiale medier for å spre sin versjon av krigen. Rapporter indikerer en lignende trend i kinesiske kampanjer, hvor de har tatt i bruk nye språk og sprer seg veldig raskt på sosiale medier.

Påvirkningsoperasjoner kan rettes mot hele samfunnet og fordi påvirkningsoperasjoner er fordekte, kan aktørene utnytte de fleste digitale plattformer og sosiale medier [2] [1] [42] [22]. Russland har demonstrert betydelige evner til å gjennomføre påvirkningsoperasjoner gjennom statlige ressurser, men de benytter ofte hacktivister og kontrollerte medier for å spre desinformasjon [3] [9] [27].

Kina anser påvirkningsoperasjoner som viktig del av sin propagandavirksomhet og gjennomføres ofte av private eller kinesiske mediefirmaer. Dette gjelder fra overvåkning internt i Kina, til regionale eller internasjonale kampanjer [22] [27] [30].

Vurdering:
Påvirkningsoperasjoner

Det vurderes som **lite sannsynlig** at spesialisthelsetjenesten vil bli utsatt for målrettede påvirkningsoperasjoner fra Russland og Kina. Aktørene har **meget høy** evne til å gjennomføre denne typen operasjoner. Viljen til å gjennomføre påvirkningsoperasjoner mot spesialisthelsetjenesten er **lav** med lav konfidens.

Dersom det er fordelaktig for russiske interesser å undergrave norsk helsevesen, kan dette også ramme spesialisthelsetjenesten. Videre kan Russland anse det fordelaktig å svekke tilliten til norske myndigheter, dersom den sikkerhetspolitiske situasjonen forverrer seg.
I en slik situasjon vurderes det som mulig at spesialisthelsetjenesten trekkes inn i en påvirkningsoperasjon.

Foto: Max Bender, Unsplash

Kapittel 4

Hacktivister

Hacktivister, eller cyber-aktivister, kan være enkeltindivider eller grupperinger hvis motivasjon er å formidle et holdningsmessig eller politisk budskap gjennom et digitalt angrep. Den typiske hacktivist-operasjonen benytter tjenestenektangrep (DDoS) eller kompromittering av en hjemmeside for å vise sin støtte til en sak. Eksempler på dette kan være motstand mot politisk betente emner eller pågående geopolitiske konflikter. Hovedmomenter i hacktivismeaktivitet det siste året har vært krigen mellom Ukraina og Russland og krigen i Gaza.

Etter en stabilisering i det pro-russiske hacktivistlandskapet det siste året, kom pro-palestinske hacktivistgrupper frem i lyset etter eskaleringen i konflikten på Vestbredden oktober 2023. Sammen med idealistiske hacktivistgrupper dukket det samtidig opp flere "*faketivister*" - statlige grupperinger som gjemmer seg bak hacktivist-merkelappen, som etterligner retorikken og mediebruken til eksisterende grupper for å passe inn i hacktivistlandskapet [4]. Det er gode indikasjoner på at både Russland og Iran, enten direkte eller indirekte, står bak flere "*faketivist*"-grupper [1].

Vilje
Hacktivister har utvist en lavere vilje til å angripe helsesektor det siste året. Norsk helsesektor har heller ikke nå vært et prioritert mål, og vi kan ikke se at helsesektor internasjonalt har vært spesielt prioritert over andre sektorer, der finans og transport har blitt rammet hardest.

Som året før, ser vi at flere grupper er mer opptatt av å bygge opp et varemerke og skape inntrykk av å ha en effekt, enn å ha en reell virkning [43]. Vi observerer at enkelte pro-russiske grupper har beveget seg bort fra å gjennomføre angrep, og hovedsakelig formidler propaganda fra det russiske statsapparatet. Dette kommer gjerne etter en endring i ledelsen i gruppen, og frafall av sentrale ressurser som hadde kompetansen til å gjennomføre angrepene [43]. De norske EOS-tjenestene forventer at hacktivister vil angripe Norge også det kommende året, dette har sammenheng Norges støtte til Ukraina og medlemskap i NATO [1] [2].

Evne
Hacktivisters evne til å utgjøre en trussel varierer kraftig. Enkelte grupper er ikke i stand til å utføre mer enn forstyrrende DDoS-angrep, mens andre har kapasiteten til å gjennomføre større koordinerte operasjoner og kompromittere utvalgte mål. Et eksempel på et slikt angrep er da den pro-palestinske gruppen AnonGhost kompromitterte en Israelsk app for varsling av angrep, og sendte ut falskt varsel om angrep med atomvåpen [44].

Under DDoS-angrep mot norske organisasjoner vil mange mål innføre geoblokkering eller vask av trafikken. Dette kan gjøre at trusselaktøren får inntrykk av å ha tatt ned målet, selv om det i realiteten er tilgjengelig for vanlige besøkende som opplever kun mindre forstyrrelser.

Få grupper har vist en evne til å ta ned større tjenester og nettsider, og de med kapabiliteten vet å utnytte den økonomisk. Flere grupper har begynt å tilby tjenestene sine til høystbydende og dermed gått bort fra den politiske overbevisningen gruppen ble grunnlagt på. Der gruppene liker å skryte av å ha tatt ned et mål, ser vi også at det gjennomføres et stort antall angrep der målet er tilstrekkelig beskyttet og opplever ingen nedetid [43].

Disse angrepene annonseres ikke av gruppene, noe som gir gruppens følgere et skjevt bilde av gruppens aktiviteter. At feilslåtte angrep ikke annonseres gjør det vanskeligere å vurdere gruppenes reelle evne til å gjennomføre angrep, da vi mangler det totale bildet.

Man har likevel det siste året sett en økning i evne hos enkelte grupperinger, der flere store vellykkede angrep har blitt gjennomført. Store organisasjoner må ofte godta trafikk fra hele verden og kan ikke beskytte seg med enkle midler, som geoblokkering. Med stor og langvarig nedetid og forstyrrelser i tjenester hos Microsoft og nedetid på nettsidene og mobil-appen til SAS, ser vi at noen kategorier av tjenester er sårbare for enkle virkemidler som utnyttes til det fulle av de mer kompetente hacktivistene [7].

Vurdering:
Hacktivister

Overordnet vurdering mot spesialisthelsetjenesten: **Hacktivister**			
	Vilje	**Evne**	**Skadepotensiale**
Hacktivister	Medium	Lav	Lavt

Hacktivisters vilje til å forsøke å ramme spesialisthelsetjenesten vurderes til **medium.** Det er viktig å være bevisst på at viljen til hacktivistgrupper kan endre seg raskt med bakgrunn i skiftende geopolitisk situasjonsbilde, betente mediesaker eller andre saker som kan fange hacktivisters oppmerksomhet. Vi ser en klar sammenheng mellom mediesaker og hvordan det fremprovoserer prioriterte mål. Felles for disse er at jo mer oppmerksomhet sakene får i internasjonale og russiske medier, desto mer sannsynlig er det at hacktivister bruker sakene som et påskudd for å gjennomføre angrep.

Vi vurderer det som **meget sannsynlig** at skadepotensialet av et tjenestenektangrep fra hacktivister vil være **lavt** og kortvarig. Det vurderes som **meget lite sannsynlig** at disse angrepene vil få konsekvenser for pasientbehandling.

Evnen til hacktivister er vurdert til å være **lav**, sammenlignet med andre trusselaktører omtalt i denne rapporten. Vi vurderer det som **sannsynlig** at enkelte hacktivistgrupper vil utvikle seg til å inneha en større organisatorisk kompetanse, og dermed øke evnen til å koordinere og gjennomføre større angrep.

Foto: Shutterstock

Kapittel 5

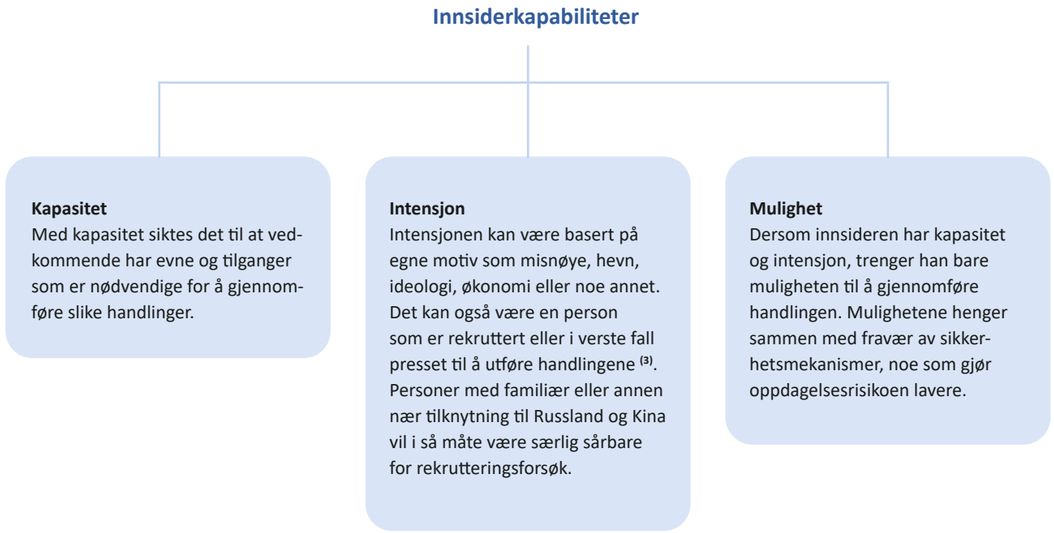
Innsidere

Denne aktørgruppen skiller seg ut fra de andre trusselaktørene som er vurdert i denne rapporten i den forstand at de har legitim tilgang til vår infrastruktur. Temaet er viktig å vite noe om for alle sektorer. Dette inkluderer også spesialisthelsetjenesten, som alene består av ca. 137 000 årsverk. Dette kapittelet skal derfor gi økt innsikt om temaet.

Samtlige av EOS-tjenestene melder om at det er forventet økt etterretningsaktivitet som følge av den nåværende sikkerhetspolitiske situasjonen. Russland vil utgjøre den største etterretningstrusselen i Norge, men også Kina vil utgjøre en betydelig og økende trussel. Cyberoperasjoner og rekruttering av innsidere vil være blant de mest sentrale metodene for statlige aktører i 2024, og det forventes at Russland og Kina vil være spesielt aktive i sine forsøk på å rekruttere kilder og innsidere [1] [2] [3].

En trend som fremheves er at bruk av innsidere vil få økt verdi mot virksomheter som har god digital sikkerhet. En trusselaktør som aksepterer økt risiko, har mer å vinne og mindre å tape på å utnytte menneskelige sårbarheter for å få tilgang til sensitiv informasjon. En trusselaktør vil sannsynlig velge minste motstands vei mot målet, og heller betale en ansatt for informasjon, enn å bruke avanserte verktøy for å bryte seg inn [40] [3] [45].

Det er et for lavt kunnskapsnivå i virksomheter om hva en innsider er, hvordan de opererer, samt trusselbildet rundt innsidevirksomhet. Dette gjør at oppdagelsesrisikoen er lavere, blant annet fordi det uten slik kunnskap vil bli vanskelig å gjennomføre tilstrekkelige sikkerhetstiltak [46].



Kapasitet, intensjon og mulighet
En innsider i denne rapporten er som ordet tilsier en person "på innsiden" av virksomheten, og som bruker sine legitime tilganger til å skade virksomheten eller for egen vinning. En innsider har i utgangspunktet kapasitet, intensjon og mulighet til å utføre uønskede handlinger mot virksomheten.

For eksempel kan en leder, forvalter eller annen person med utvidede tilganger enklere kunne hente ut sensitiv informasjon uten å vekke mistanke. Mulighetsrommet for en innsider vil også være større i systemer uten logging eller der det mangler tilgangsstyring.

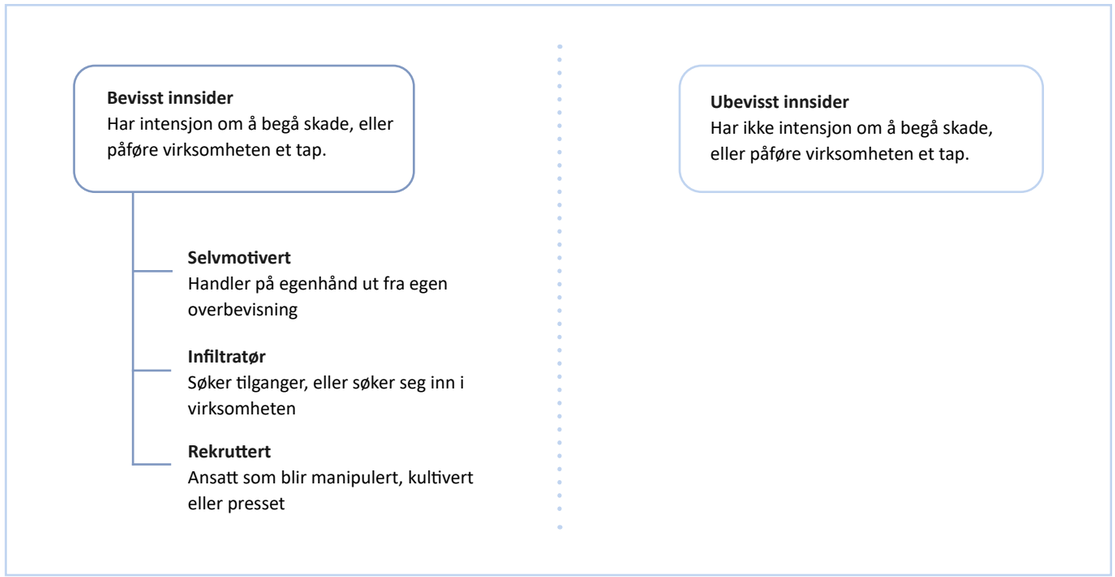
Kategorier av innsidere
Det kan med andre ord variere hva en innsider er, og det kan derfor være nyttig å kategorisere disse for å gjøre trusselen håndterbar.

Innsidere i en organisasjon kan variere fra de som ubevisst kan forårsake skade, til de som aktivt søker å skade virksomheten de jobber for. En ubevisst innsider mangler intensjonen om å skade, men kan blir brukt uten at vedkommende vet det selv. Muligheten til å gjøre skade henger da sammen med hvor bevist forhold innsideren har til informasjonssikkerhet, og sikkerhetskulturen i organisasjonen. En bevisst innsider er en person som har til hensikt å begå skadelige handlinger. Blant bevisste innsidere finner vi selvmotiverte innsidere, infiltratører og rekrutterte innsidere.

Selvmotivert innsider
En selvmotivert innsider har, som ordet antyder, motivert seg selv til å bli en innsider. Motivasjonen kan drives av personlige grunner, som for eksempel økonomisk gevinst eller ideologiske overbevisninger. Disse innsiderne kan også bli påvirket av desinformasjon som sprer seg i samfunnet, noe som kan endre deres oppfatninger og holdninger, og gjøre dem mer mottakelige for rekruttering.

Den generelle spredningen av desinformasjon i samfunnet kan endre enkeltpersoners oppfatninger, holdninger og handlinger gjennom feilaktig eller villedende informasjon (27) (1). Slik påvirkning kan også foregå på virksomhetsnivå, og ikke nødvendigvis direkte mot enkeltpersoner. Man kan forsøke å redusere lojaliteten til virksomheten gjennom tema som opptar enkelte grupper i virksomheten. For eksempel var det under massevaksineringen mot korona flere grupper som sto frem som mistroiske mot det offentlige helsevesenet (49).

Infiltratør
Infiltratører er en annen gruppe som i utgangspunktet ikke har kapasitet idet vedkommende blir rekruttert, men må posisjonere seg for å få dette. Dette kan for eksempel være en person som søker på en utlyst stilling, eller en ansatt som søker en annen stilling internt i virksomheten. Det kan også være en ansatt som søker utvidede tilganger slik at vedkommende kan få tilgang til informasjon, og derved nødvendig kapasitet.



Rekruttert innsider
Rekrutterte innsidere kan ha blitt manipulert, påvirket eller presset til å utføre innsidehandlinger av en ekstern aktør. Rekrutteringsprosessen foregår gjerne i fire faser: Kontaktetablering, vurdering av egnethet, kultivering/press og rekruttering. Tidligere foregikk slike rekrutteringsprosesser primært gjennom fysiske møter. Konferanser er fremdeles populære arenaer for kontaktetablering av mulige kilder. I dag bruker trusselaktører i økende grad sosiale medier og chatteapplikasjoner til rekruttering av kilder. I tillegg kan sosiale medier være en kilde til informasjon som kan brukes mot vedkommende (1) (22).

Dersom personen vurderes som egnet til å fungere som en innsider, er neste fase å kultivere et forhold til vedkommende. De kan tilby gaver eller andre fordeler, eller utøve press basert på informasjon eller svakheter de har oppdaget om personen. Til slutt kommer selve rekrutteringen, der vedkommende enten frivillig eller under tvang aksepterer å fungere som en innsider i virksomheten.

Vurdering:
Innsidere

EOS-tjenestene vurderer at rekruttering av innsidere spesielt fra Kina og Russland vil utgjøre en høy trussel for norske virksomheter. I tillegg er virksomheter innenfor helsesektoren definert som ett av hovedmålene til statlige trusselaktører. Vi ser også en trend der bruk av innsidere har økt verdi mot virksomheter som har god digital sikkerhet.

Vi vurderer derfor at sannsynligheten for at spesialisthelsetjenesten vil oppleve uønsket hendelse som følge av innsider er **meget sannsynlig**. Skadepotensialet til en innsider vil variere basert på evne og mulighet. Dette kommer an på blant annet rettighetsnivå til systemer, teknisk kunnskap og myndighet. Skadepotensialet vil derfor kunne variere fra **meget lavt** til **meget høyt**.

Foto: Shutterstock

Kapittel 6

Cybersikkerhetsutfordringer

Samfunnet blir stadig mer datadrevet, og med dette følger også nye sårbarheter. Informasjons- og kommunikasjonsteknologi har en viktig funksjon for å oppnå verdiskaping og beskytte verdiene mot sikkerhetstruende hendelser, som cyberoperasjoner. Derfor er tillitt til IKT-systemene avgjørende, og motstandsdyktighet mot digitale angrep vesentlig for spesialisthelsetjenesten. Truslene utvikler seg like raskt som gevinstene med teknologien vi benytter. Et mulighetsrom for spesialisthelsetjenesten vil også kunne gi et mulighetsrom for en trusselaktør.

I dagens trusselbilde handler derfor responsen mot trusler om prioritering og organisasjonens innsats. Dette innebærer at man må prioritere kjente og skadelige trusler samtidig som man må forberede seg på ukjente trusler.

Skytjenester
Bruk av skytjenester øker i omfang, noe som øker kompleksiteten og angrepsflaten. Skytjenester er gjerne tett integrert med interne IKT-systemer, der en slik hybrid tilnærming kan skape utilsiktet ekstern eksponering av interne tjenester. Samtidig gir skytjenester store muligheter for realisering av gevinster fra teknologiutvikling og digitalisering, samt at det kan bidra til bedre sikkerhet.

Bruk av skytjenester vil med andre ord kunne gi virksomheter større mulighetsrom og sikkerhetsmessige fordeler, men kan også føre til en sentralisering av verdier, og dermed bli et mer ettertraktet mål blant trusselaktører som er drevet av profitt og statlige aktører [8]. Virksomheter bør videre ha en bevist tilnærming til avhengigheter som skapes til leverandører og bygge kompetanse for å hente ut nødvendige sikkerhets-messige gevinster på kort og lang sikt.

Kunstig intelligens (KI)
Kunstig intelligens er systemer som utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data for å oppnå et spesifikt mål [50]. Virksomheter må ta i bruk kunstig intelligens på en trygg og ansvarlig måte, noe en trusselaktør ikke er bundet av. Dette skaper ujevne odds mellom oss og trusselaktørene, ved at de kan ta i bruk teknologien raskere.

Bruk av KI har potensiale til å transformere næring og samfunn, men er også sårbare for angrep og utnyttelse. En KI-modell kan produsere feil resultater basert på inngangsverdier, eller repetere biaser i datasett KI modellen har blitt trent på.

Utfordringene med KI for spesialisthelsetjenesten er flere, og tross at teknologien er forsket på lenge, er teknologien fortsatt umoden og man har lite erfaring med den over tid. En utfordring er at man ikke vet hvordan en KI-modell skal «glemme» eller avlæres.

KI vil øke våre evner til å oppdage trusler innen cyberdomenet vil det også i stor grad øke evnene til trusselaktørene til å gjennomføre cyberangrep uoppdaget. Ved bruk av KI kan trusselaktører automatisere deler av eller hele angrepsprosessen, rekognosering, målretting og utnyttelse. KI-styrte angrep kan tilpasse seg miljøet i målet som gjør dem vanskeligere å oppdage og motvirke [52] [51].

Trusselaktører fortsetter å utnytte bruk av KI til å utvikle sine metoder og verktøy, og vi ser allerede eksempler på bruk av KI i direktørbedrageri. Gjennom 2023 ser vi også at kunstig intelligens for alvor kom inn i det offentlige ordskiftet. Dette viser at kunstig intelligens kan understøtte flere kriminalitetsområder. Når cyberkriminelle tar i bruk nye verktøy kan andre raskt følge etter, noe som øker cyberkriminelle sine kapabiliteter hurtig [8]. Samtidig som kapabilitetene til de cyberkriminelle øker, vil KI også kunne bidra i eksponering av virksomheters svakheter for disse aktørene. Gjennom KI-støttet rekognosering og målretting vil en trusselaktør avdekke grunnleggende sikkerhetssvakheter hos et mål raskere.

En av konsekvensene av dette er at store datasett med sensitiv og verdifull informasjon vil sannsynlig bli mer ettertraktede mål for trusselaktører [25]. Datasett kan brukes til maskinlæring for å trekke ut sammenhenger som ellers er vanskelig tilgjengelig for ufaglærte. Slike databaser kan være offentlige helseregistre, folkeregistre eller registre over kritisk infrastruktur.

Løsninger basert på KI er på vei inn i pasientbehandlingen, men det fordrer en trygg og god ibruktagelse som ivaretar personvern og informasjonssikkerhet. Ettersom tilliten til KI vokser, vil avhengigheten til teknologien øke. Det er viktig å være bevisst på at bruk av kunstig intelligens kan endre arbeidsprosesser og behandlingsforløp.

Nulldagssårbarheter og raskere utnyttelse
Nulldagssårbarheter refererer til at det er en ukjent sårbarhet eller feil i programvare, som trusselaktørene gjerne oppdager før leverandøren [3]. Et sentralt utviklingstrekk innenfor cyberdomenet er utnyttelse av slike nulldagssårbarheter, og det er vanskelige å beskytte seg mot dette [8].

Nulldagssårbarheter er ofte krevende å avdekke, og det er gjerne kompetente trusselaktører som klarer å avdekke disse. Slike sårbarheter selges hovedsakelig kommersielt for store pengesummer. Nulldagssårbarheter vil sannsynligvis få økt verdi blant cyberkriminelle, og kunne øke skadepotensialet. Statlige aktører og organiserte kriminelle er kjent for å utnytte slike sårbarheter, og trenden med økende utnyttelse er forventet at fortsetter i tiden fremover [8, 14].

Sosial manipulering
Sosial manipulasjon er en tradisjonell måte å angripe virksomheter på, og teknologi er på mange måter en moderne måte utføre denne typen angrep gjennom. Likevel må det forventes at metodene vil fortsette å utvikle seg. Globalt ser man en begynnende trend der trusselaktører i større grad søker å bygge en form for tillitt hos sine mål først, før man forsøker å få vedkommende til å utføre en handling som muliggjør installering av skadevare. En informert, motivert og sikkerhetsbevisst ansatt vil fremdeles være et av de viktigste sikkerhetstiltakene mot fremtidens cybertrusler.

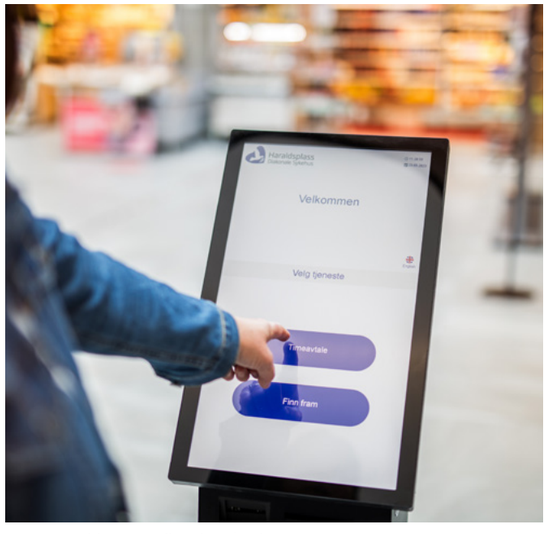


Foto: Ingvild Festervoll Melien / Helse Vest IKT

Referanseliste

1. **PST.** *Nasjonal trusselvurdering 2024.* Oslo : PST, 2024.

2. **Etterretningstjenesten.** *FOKUS 2024 Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Oslo : Etterrettningstjenesten, 2024.

3. **NSM.** *Risiko 2024 Nasjonal sikkerhet er et felles ansvar.* Oslo : NSM, 2024.

4. **Crowdstrike.** *Global Threat Report 2024.* s.l. : Crowdstrike, 2024.

5. **Recorded Future: Insikt Group.** *Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine.* s.l. : Recorded Future, 2023. CTA-RU-2023-0131.

6. **Recorded Future.** *Dark Covenant: Connections Between the Russian State and Criminal Actors.* s.l. : Recorded Future, 2021. CTA-RU-2021-0909.

7. **Mandiant Advantage.** *License to KillNet: Hacktivists Expand Targeting Beyond Eastern Europe.* s.l. : Mandiant Advantage, 2022. 22-00020786V2.

8. **Kripos.** *Cyberkriminialitet 2024.* s.l. : Kripos, 2024.

9. **Center for Cybersikkerhed CFCS.** *Trusselsvurdering Cybertruslen mod Danmark 2023.* s.l. : CFCS, 2023.

10. **Flare.** Bleeping Computer. *The Initial Access Broker Economy: A Deep Dive into Dark Web Hacking Forums.* [Internett] 07 09 2023. [Sitert: 01 04 2024.] https://www.bleepingcomputer.com/news/security/the-initial-access-broker-economy-a-deep-dive-into-dark-web-hacking-forums/.

11. **Check Point.** *2024 Cyber Security Report.* s.l. : Check Point Research, 2024.

12. **Center for cybersikkerhed.** *Cybertruslen mod sundhedssektoren.* s.l. : Center for cybersikkerhed, 2023.

13. **Politiet.** *Politiets trusselvurdering 2023.* Oslo : POD, 2023.

14. **HelseCERT,** *Intern Kilde.*

15. **Nordic Financial CERT.** *Cyber Threat Landscape for the Nordic Financial Sector.* s.l. : Nordic Financial CERT, 2024.

16. **Politiet.** *Politiets trusselvurdering 2024.* Oslo : POD, 2024.

17. **Justis- og beredskapsdepartementet.** *NOU 2023: 17 Nå er det alvor — Rustet for en usikker fremtid.* Oslo : Regjeringen.no, 5. juni 2023.

18. **Crowdstrike.com.** *Cyber Big Game Hunting.* [Internett] 22 Februar 2024. [Sitert: 23 04 2024.] https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/.

19. **Mandiant.** *M-TRENDS 2023 Mandiant Special Report.* s.l. : Manidant part of Google Cloud, 2023.

20. **CERT-EU.** *Threat Landscape Report 2023.* Brussel : EU, 2023.

21. **Spesialisthelsetjenesten.** *Trusselvurdering Det digitale trusselbildet mot spesialisthelsetjenesten.* s.l. : Sykehuspartner, 2023.

22. **Microsoft.** *Microsoft Digital Defense Report.* s.l. : Microsoft, 2023.

23. **Crowdstrike.** *2024 Global Threat Report.* s.l. : Crowdstrike, 2024.

24. **Den Norske Bank DNB.** *Finansiell trygghet i en usikker verden. Trusler og trender fra et DNB-Perspektiv 2024.* Oslo : DNB, 2024.

25. **European Union Agency for Cybersecurity.** *ENISA Threat Landscape 2022.* Brussel : EU, 2022.

26. **PST.** *Nasjonal trusselvurdering 2023.* Oslo : PST, 2023.

27. **Crowdstrike.** *2023 Global Threat Report.* s.l. : Crowdstrike, 2023.

28. **Mandiant Advantage.** *Country Snapshot: Norway (Q4 2023).* s.l. : Mandiant Advantage, 2024.

29. **Health Sector Cybersecurity Coordination Center.** HC3: Threat Profile August 16, 2023 TLP:CLEAR Report: 202308161700. s.l. : Health Sector Cybersecurity Coordination Center, 2023.

30. **Mandiant Advantage.** *Industry Snapshot: Healthcare (Q4 2023).* s.l. : Mandiant Advantage, 2024.

31. **Mandiant. Country Profile:** *Russia (2023).* s.l. : Mandiant Advantage, 2023.

32. **Mandiant. Country Profile:** *China (2023).* s.l. : Mandiant Advantage, 2023.

33. **CISA ASD NSA GCHQ CCCS ACSC.** *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* s.l. : CISA, 2024.

34. **CISA FBI NSA GCSB CCCS ACSC ASG.** *People`s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* s.l. : CISA, 2023.

35. **Mandiant Advantage.** *Country Snapshot: Iran (Q4 2023).* s.l. : Mandiant Advantage, 2023.

36. **Crowdstrike.** *2023 Cloud Risk Report.* s.l. : Crowdstrike, 2023.

37. **PST .** *"Indikatorer på ulovlige anskaffelser" (24. Aug. 2023) PST. <pst.no/alle-artikler/artikler/ulovlige-anskaffelser-og-indikatorer/>* . s.l. : PST, 2023.

38. **Mandiant Advantage.** *Country Snapshot: North Korea (Q4 2023).* s.l. : Mandiant Advantage, 2023.

39. **Marius Nyquist Pedersen, Tor Ole Vormdal, Marit Lind, Thor Engøy.** *FFI- Rapport Fremtidens sanitet effektiv ressurs i Forsvaret og totalforsvaret. Oslo : FFI, 2022.* 22/01114.

40. **NSM.** *NSM Nasjonalt digitalt risikobilde 2023.* s.l. : NSM, 2023.

41. **Bergh, Arild.** *Understanding Influence Operations in Social Media:. Journal of Information Warfare (2020)* 19.4: 110-131. 2020.

42. **FFI.** *Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv.* s.l. : FFI, 2023.

43. **HelseCERT.** *Intern kilde.*

44. **CyberMaterial.** *AnonGhost Hacks Red Alert App.* 2023.

45. **CISA Cybersecurity and Infrastructure Security Agency.** *Insider Threat Mitigation Guide.* s.l. : CISA, 2020.

46. **NSM.** *Temarapport Innsiderisiko.* Oslo : NSM, 2020.

47. **Mandiant Advantage.** *Country Snapshot: The Nordic Region Q4 2023.* s.l. : Mandiant Advantage, 2023.

48. **Palo Alto UNIT42.** *Incident Response Report 2024.*

49. **Politiet Kripos NC3.** *Temarapport: Generativ kunstig intelligens og cyberkriminalitet.* OSLO : Kripos, 2023.

50. **ØKOKRIM.** *okokrim.no. webområde for Økokrim.* [Internett] 3 4 2024. [Sitert: 3 April 2024.] https://www.okokrim.no/bedrageri.549300.no.html.

51. **National Cuber Security Centre & National Crime Agency.** *Ransomware, extortion and the cyber crime ecosystem: A white paper from the NCSC and the National Crime Agency (NCA).* s.l. : NCSC, 11 September 2023.

52. **Mandiant Advantage.** *Trust Me I`m a Professional: The Evolution and Commoditization of the Cyber Crime Ecosystem.* s.l. : Mandiant Advantage, 2021. 21-00012276.

53. **ESET Research.** *Threat Report.* s.l. : ESET, H2 2023.

54. **Check Point.** *Cyber Security Report.* s.l. : Check Point, 2023.

55. **ESET.** *Cybersecurity Trends 2023: Securing our hybrid lives.* s.l. : ESET, 2023.

56. **Mandiant Advantage.** *Industry Snapshot: Goverment (Q4 2023).* s.l. : Mandiant Advantage, 2023.

57. **Mandiant. Country Snapshot:** *China (Q4 2023).* s.l. : Mandiant Advantage, 2023. 24-10000016V1.

58. **Chainalysis.** *The 2023 Crypto Crime Report: Everything you need to know about cryptocurrency-based crime.* s.l. : Chainalysis, 2023.

59. **Ponemon Institute.** *2023 Cost of insider threats global report.* s.l. : DTEX, 2023.

60. **IBM.** *IBM X-Force Threat Intelligence Index 2024.* s.l. : IBM, 2024.

61. **Dawn Cappelli, Andrew P. Moore & Randall F. Trzeciak.** *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* s.l. : Addison-Wesley Professional, 2012. ISBN9780321812575.

62. **Poremba, Sue. Verizon.com.** *[Internett] [Sitert: 4 4 2024.] https://www.verizon.com/business/resources/articles/s/the-risk-of-insider-threat-actors/.*

63. **National Cyber Security Centre UK.** *The near-term impact of AI on the cyber on the cyber threat.* London : NCSC, 2024.

64. **Malwarebytes.com.** *Big-game hunting (BGH).* [Internett] https://www.malwarebytes.com/glossary/big-game-hunting-bgh.