2023 TRUSSELVURDERING

DET DIGITALE TRUSSELBILDET MOT SPESIALISTHELSETJENESTEN

Illustrasjonsfoto: Shutterstock

02.06.2023

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

Norsk helsenett
HelseCERT

FORORD

I Norge har vi gode muligheter for å få et godt innblikk i truslene vi står overfor gjennom åpenheten fra våre sikkerhets- og etterretningstjenester, og de årlige rapportene Risiko, Fokus og Nasjonal trusselvurdering. Denne rapporten er vår vurdering av relevante trusler for spesialisthelsetjenestens verdier og er basert på en sammenstilling av de nasjonale vurderingene, andre kilder og egne hendelser.

Årets rapport er en samlet, helhetlig vurdering av trusselbildet mot hele spesialisthelsetjenesten, og viser gevinstene av et sterkt, faglig sikkerhetssamarbeid på tvers av regionale grenser. Trusselaktørene opererer uavhengig av vår organisering og geografi, og gjennom en omforent forståelse av deres evne og vilje, så kan helseregionene bedre samarbeide og legge til rette for en felles innsats innenfor informasjonssikkerhetsområdet.

Ett av mange positive kjennetegn ved det norske helsevesenet og spesialisthelsetjenesten er den høye graden av digitalisering og bruken av ny teknologi. IKT gir bedre pasientbehandling med økt kvalitet og effektivitet. Samtidig behøver sektoren mer digitalisering og mer teknologi. Helsepersonellkommisjonens rapport fra februar i år fikk navnet *Tid for handling.* Tittelen understreker alvoret, og rapporten viser også hvordan en helhetlig, vellykket IKT-innsats er en forutsetning for å nå fremtidens behov.

Digitale systemer og arbeidsprosesser er vesentlig for dagens pasientbehandling, men samtidig introduserer denne digitaliseringen nye risikoer. Vellykkede digitale angrep mot spesialisthelsetjenesten kan få konsekvenser for helseforetakenes evne til å utføre sine primæroppgaver. Angrep kan blant annet påvirke pasientbehandlingen, økonomi, personvern og omdømme.

Trusselbildet endres også som følge av geopolitisk ustabilitet. Russlands invasjon av Ukraina endrer også trusselbildet mot spesialisthelsetjenesten i Norge. Destruktive angrep mot spesialisthelsetjenesten fra hacktivister var en av truslene som var vurdert i fjorårets rapport. Den 27. januar 2023 uttalte en pro-russisk hacktivistgruppe at de som hevn for det de kaller «support for the Nazis in Ukraine» ville gjennomføre destruktive cyberangrep mot datanettverk tilhørende sykehus i en rekke vestlige land, inkludert ti forskjellige helseforetak i Norge. Spesialisthelsetjenesten ble i den forbindelse utsatt for angrep, men angrepene ble håndtert effektivt og fikk derfor ikke reelle konsekvenser. Saken fikk medieoppmerksomhet, hvor det ble laget saker om at russiske hackere truet norske sykehus. Slike hendelser viser viktigheten av å være forberedt.

Årets rapport gir frempek på truslene vi mener er mest relevante i den kommende periode. Vurderingen er utarbeidet av Helse Nord IKT og Sykehuspartner HF, i samarbeid og med støtte fra HelseCERT og de øvrige helseregionene. Vi håper rapporten kommer til nytte.

Illustrasjonsfoto: Shutterstock

INNHOLDSFORTEGNELSE

01. HVORDAN LESE RAPPORTEN 6

02. ANGREPSVEKTORER 8

03. TRUSSELVURDERING 10

DEL 1 ORGANISERTE KRIMINELLE AKTØRER 12

DEL 2 STATLIGE AKTØRER 28

DEL 3 HACKTIVISTER 41

DEL 4 SELVMOTIVERTE INNSIDERE 44

04. TRENDER 47

05. AVSLUTNING 51

06. KILDER OG VEDLEGG 52

SAMMENDRAG

Spesialisthelsetjenesten tiltrekker seg oppmerksomhet fra ulike trusselaktører i det digitale rom. Disse aktørene ønsker å oppnå egne strategiske mål på bekostning av spesialisthelsetjenestens verdier. Vellykkede digitale angrep vil kunne få konsekvenser for helseforetakenes evne til å utføre sine primæroppgaver.

Vi vurderer at den mest alvorlige trusselen mot spesialisthelsetjenesten er organiserte kriminelle aktører som driver med digital utpressing. Bakgrunnen for dette er kombinasjonen av disse aktørenes vilje og evne til å utføre digitale utpressingsangrep mot spesialisthelsetjenesten og skadepotensialet et eventuelt vellykket angrep vil kunne medføre.

Disse aktørene har utviklet digital utpressing til en milliardindustri ved å hente ut sensitiv informasjon fra, og utilgjengeliggjøre, virksomheters systemer. Deretter krever aktørene løsepenger for å tilgjengeliggjøre systemene igjen og for å ikke publisere den sensitive informasjonen offentlig. Gjennomsnittskostnaden i 2022 for et digitalt utpressingsangrep mot helse globalt, var ca. 100 millioner kroner. Det finnes samtidig langt mer kostbare tilfeller på slike angrep mot helse, for eksempel angrepet mot det irske helsevesenet i 2021. Totalkostnaden ble i dette tilfellet estimert mellom 5 og 6 milliarder kroner.

Det er vår vurdering at et vellykket digitalt utpressingsangrep mot spesialisthelsetjenesten vil kunne ha **meget høyt** skadepotensiale. Dette er spesielt med hensyn til kryptering av, og nedetid på, kritiske systemer som kan ramme pasientbehandlingen, høye kostnader for opprydding og gjenoppretting, samt indirekte kostnader som følger av manuelle rutiner og konsulentbruk. Et

Illustrasjonsfoto: André Riise, Nettrakett

slikt angrep vil også kunne medføre kompromittering og publisering av sensitiv informasjon som for eksempel person- og helseopplysninger.

De digitale utpressingsaktørenes vilje mot spesialisthelsetjenesten vurderes som **meget høy.** Dette er basert på hva vi observerer, andre sentrale aktørers vurderinger og disse aktørenes høye aktivitetsnivå mot helsesektoren globalt. En undersøkelse viser at to tredjedeler av virksomheter innen helse globalt har vært utsatt for digital utpressing. Mot helse vurderes **meget sannsynlig** den mest sentrale driveren til digitale utpressingsaktører å være den høye kritikaliteten ved nedetid på IKT-systemer, gitt systemenes samfunnskritiske funksjon. Dette innebærer også at kliniske systemer kan være et mål. En annen sentral driver for digitale utpressingsaktører er at helsesektoren, i et globalt perspektiv, tradisjonelt sett har vært en sektor preget av stor angrepsflate. Videre vurderes det som **meget sannsynlig** at helse- og personopplysninger er de mest attraktive informasjonsmålene til digitale utpressingsaktører.

Evnen til digitale utpressingsaktører er vurdert **høy**. Disse aktørene er meget profesjonelle og tilpasningsdyktige og utvikler forretningsmodellene raskt for å kunne øke inntjening og redusere risiko. Digitale utpressingsaktører beskrives nærmere under kapittel 3, del 1, organiserte kriminelle aktører.

Statlige aktører vurderes å utgjøre en betydelig trussel for spionasje mot spesialisthelsetjenesten. Det vurderes som **meget sannsynlig** at Russland og Kina er de statlige aktørene med størst vilje til å utøve spionasje mot spesialisthelsetjenestens verdier. Samlet vurderes det som **meget sannsynlig** at fremmede staters sikkerhets- og etterretningstjenester har vilje til å drive spionasje mot spesialisthelsetjenestens forskningsmiljøer. Videre vurderes det som **sannsynlig** at statlige aktører vil forsøke å tilegne seg helseopplysninger fra regionene i kartleggings- og etterretningsøyemed. Det vurderes også som **sannsynlig** at Russland har vilje til å utøve spionasje mot spesialisthelsetjenestens verdier som omfatter beredskap og krisehåndteringsevne.

Russlands og Kinas evner til å utføre vellykkede spionasjeoperasjoner i det digitale rom er vurdert å være **meget høy.** Det vurderes som **meget sannsynlig** at statlige aktørers sikkerhets- og etterretningstjenester innehar kapabiliteter gode nok til å omgå et godt grunnleggende sikkerhetsnivå. Samtidig er det for disse aktørene en høyere kostnad og risiko forbundet med å benytte de mest avanserte metodene. Det vurderes derfor som **meget sannsynlig** at statlige aktører er villige til å bruke billige og enkle metoder mot spesialisthelsetjenesten, mens de mer avanserte og kostbare metodene vil benyttes i mindre grad og vurderes mer kritisk opp mot verdien av målet. Statlige aktørers vilje og evne til å gjennomføre spionasjeoperasjoner mot spesialisthelsetjenesten beskrives nærmere under kapittel 3, del 2, statlige aktører, spionasje.

Vi vurderer videre at Russland og Kina også innehar en **meget høy** evne til å utføre destruktive digitale angrep. Slike angrep vil kunne ha et **meget høyt** skadepotensiale da formålet er ødeleggelse. På bakgrunn av disse faktorene er det viktig å følge med på eventuell utvikling i statlige aktørers vilje til å gjennomføre destruktive digitale angrep. Kinas vilje er vurdert å være **meget lav**, mens Russlands vilje til å utføre destruktive digitale angrep mot spesialisthelsetjenesten er vurdert å være **lav** grunnet den spente geopolitiske situasjonen med bakgrunn i krigen i Ukraina. Statlige aktørers vilje og evne til å gjennomføre destruktive digitale angrep er beskrevet nærmere under kapittel 3, del 2, statlige aktører, destruktive angrep.

Det siste året har man observert angrep mot norsk helsesektor fra hacktivister med bakgrunn i Norges støtte til Ukraina. Pro-russiske hacktivister vurderes å ha **høy** vilje til å forsøke å ramme spesialisthelsetjenesten. Det vurderes som **sannsynlig** at spesialisthelsetjenesten vil bli direkte forsøkt rammet av et hacktivist angrep. Evnen til pro-russiske hacktivister er vurdert å være **lav** sammenlignet med de statlige- og organiserte kriminelle aktørene. Basert på sammenlignbare angrep vurderer vi at skadepotensialet av et tjenestenektangrep fra hacktivister **meget sannsynlig** vil være **lavt** og kortvarig for spesialisthelsetjenesten. Grunnet den **høye** viljen er det vesentlig å følge med på utvikling i evnenivået til pro-russiske hacktivistgrupper. Hacktivisters vilje og evne er beskrevet nærmere under kapitlet 3, del 3, hacktivister.

En selvmotivert innsider har en egen motivasjon for å utføre innsidevirksomhet som potensielt kan påføre virksomheten skade. Hovedbekymringen med selvmotiverte innsidere er personell med mulighet og evne til å påføre spesialisthelsetjenesten **meget høyt** skadepotensiale. Dette kan være personell med høyeste rettighetsnivå, teknisk kunnskap til å illegalt kunne skaffe seg høyeste rettighetsnivå eller lignende. Det vurderes som **meget lite sannsynlig** at spesialisthelsetjenesten vil bli utsatt for et angrep hvor en selvmotivert innsider benytter seg av muligheten til å utføre en handling med **meget høyt** skadepotensiale. Selvmotiverte innsidere er beskrevet nærmere i kapittel 3, del 4, selvmotiverte innsidere.

Til tross for at mange virksomheter jobber aktivt med sikkerhet og digital motstandsdyktighet, viser rapporter til at det som oftest er grunnleggende svakheter i sikkerhetstilstanden som muliggjør vellykkede angrep. Trusselbildet er i konstant endring, som følge av trusselaktørenes økte tilpasningsevne og utvikling av verktøy og metoder. For spesialisthelsetjenesten medfører dette at sikkerhetsmekanismene kontinuerlig må styrkes for å holde risikonivået stabilt.

01. Hvordan lese rapporten

Sannsynlighetsord | Oversikt over trusselnivåer | Konfidensnivå | Symbolbruk | Avgrensninger

Illustrasjonsfoto: Shutterstock, Daria Lukoiko

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 klammeparentes i teksten, for eksempel [99]. Referansene finner man igjen i kildelisten nederst 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 24. mars 2023 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	**

Symbolbruk

Viser hvor det legges frem hva andre mener

Viser hva som er våre egne vurderinger

Viser hva som er faktabokser, eksempler og dypdykk

02. Angrepsvektorer

Cyber attack lifecycle | Angrepsvektorer for initiell tilgang

Illustrasjonsfoto: Shutterstock

ANGREPSVEKTORER

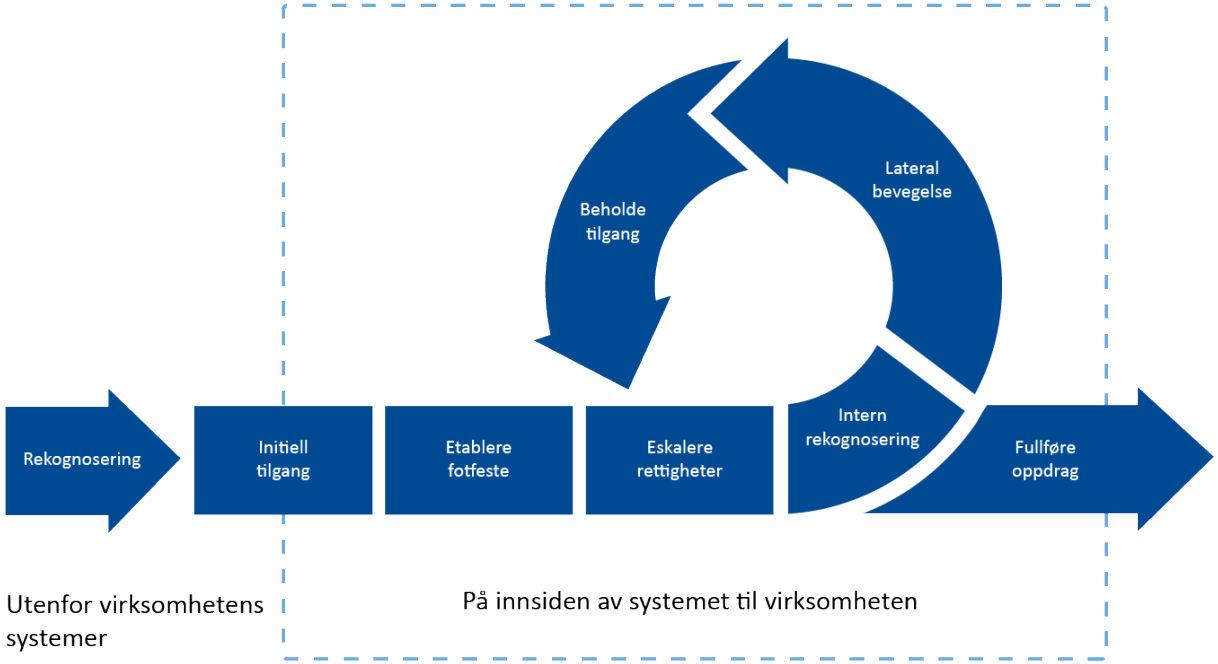
Cyber attack lifecycle

Modellen viser de ulike stegene som trusselaktører gjennomfører i et digitalt angrep. Man ser av modellen at det kun er en liten del av et digitalt angrep som handler om å skaffe initiell tilgang til virksomhetens system. Deretter må aktøren i ulik grad foreta operasjoner på innsiden av systemet for å kunne nå sitt endelige mål. I et sikkerhets perspektiv er det effektivt å rette sikkerhetstiltak mot å hindre aktørene i initiell tilgang og dette er derfor et viktig steg å fokusere på. Samtidig må man erkjenne at aktørene vil bryte gjennom den første barrieren og da er det også viktig med gode sikkerhetstiltak i dybden. Dette kan være gjennom arkitektur, overvåkning og deteksjon.

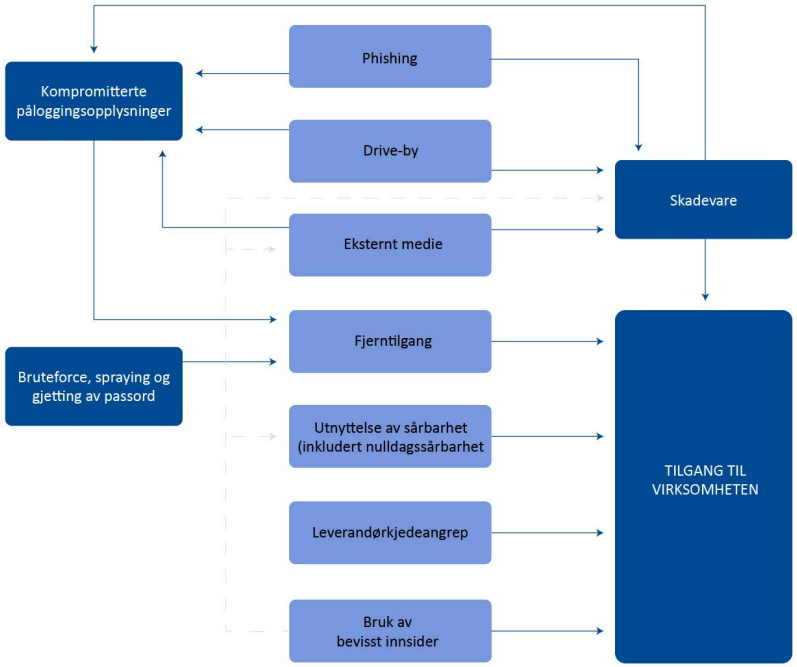
Angrepsvektorer for initiell tilgang

Modellen viser hva denne rapporten legger i *angrepsvektorer* for *initiell tilgang*. Selve angrepsvektorene er markert med grå farge. Pilene og de mørkeblå boksene viser sentrale sammenhenger. Angrepsvektorene forklares grundigere i vedlegg 1, angrepsvektorer. Modellen er sterkt inspirert av det danske cybersikkerhetssenteret (CFCS).

Figur 1: Cyber attack lifecycle [4].



Figur 2: Angrepsvektorer for initiell tilgang [5], [6].



03. Trusselvurdering

Oversikt over trusselaktørene som er vurdert

Illustrasjonsfoto: Norsk Helsenett

OVERSIKT OVER TRUSSELAKTØRENE SOM ER VURDERT

Denne rapporten beskriver de mest relevante kategoriene av trusselaktører for spesialisthelsetjenesten, og deres vilje og evne til å påvirke våre verdier. Det er flere ulike måter å dele inn trusselaktører på. Å gjøre en presis inndeling er blitt vanskeligere fordi skillet mellom aktørene er mindre tydelig enn tidligere [7], [8], [9]. For å beskrive trusselbildet mot spesialisthelsetjenesten på en helhetlig måte, er trusselaktørene gruppert etter en kombinasjon av organisering og intensjon. De fire kategoriene av trusselaktører som er vurdert å være mest relevant for spesialisthelsetjenesten er følgende:

Organiserte kriminelle aktører

I denne rapporten er dette organiserte aktører som opererer ulovlig i cyberdomenet med økonomisk vinning som primær motivasjon. Aktører som driver med digital utpressing er et eksempel på en organisert kriminell aktør.

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 enkeltindivider eller en gruppe personer hvis motivasjon er å formidle et holdningsmessig- eller politisk budskap gjennom et digitalt angrep [6].

Selvmotiverte innsidere

Selvmotiverte innsidere er personer som er gitt legitim tilgang til en virksomhets systemer, og som har en egen motivasjon for å utføre uønskede handlinger med denne tilgangen. Denne kategorien skiller seg ut fra de andre trusselaktørene ved å være intern. Det presiseres at denne aktøren ikke utfører handlinger på vegne av en trusselaktør.

Det er flere faktorer som kompliserer en god kategorisering av trusselaktører. For det første overlapper intensjonene mer, ved at det finnes statlige aktører med finansiell motivasjon og kriminelle aktører med politisk motivasjon. Det er også ofte vanskelig for virksomheter og myndigheter å identifisere hvilken aktør som står bak et angrep. For eksempel kan man ha flere aktører inne i et system under samme hendelse, som gjerne bruker samme skadevare og har stort overlapp i metoder og verktøy som benyttes i angrepet [9], [8], [7]. I tillegg er det flere rapporter som peker på ulike former for samarbeid og grader av knytninger mellom statlige aktører, organiserte kriminelle aktører og hacktivister [10], [7], [11]. Dette beskrives nærmere under kapittel 3, del 2, statlige aktører, spionasje.

03.

DEL 1

Organiserte kriminelle aktører

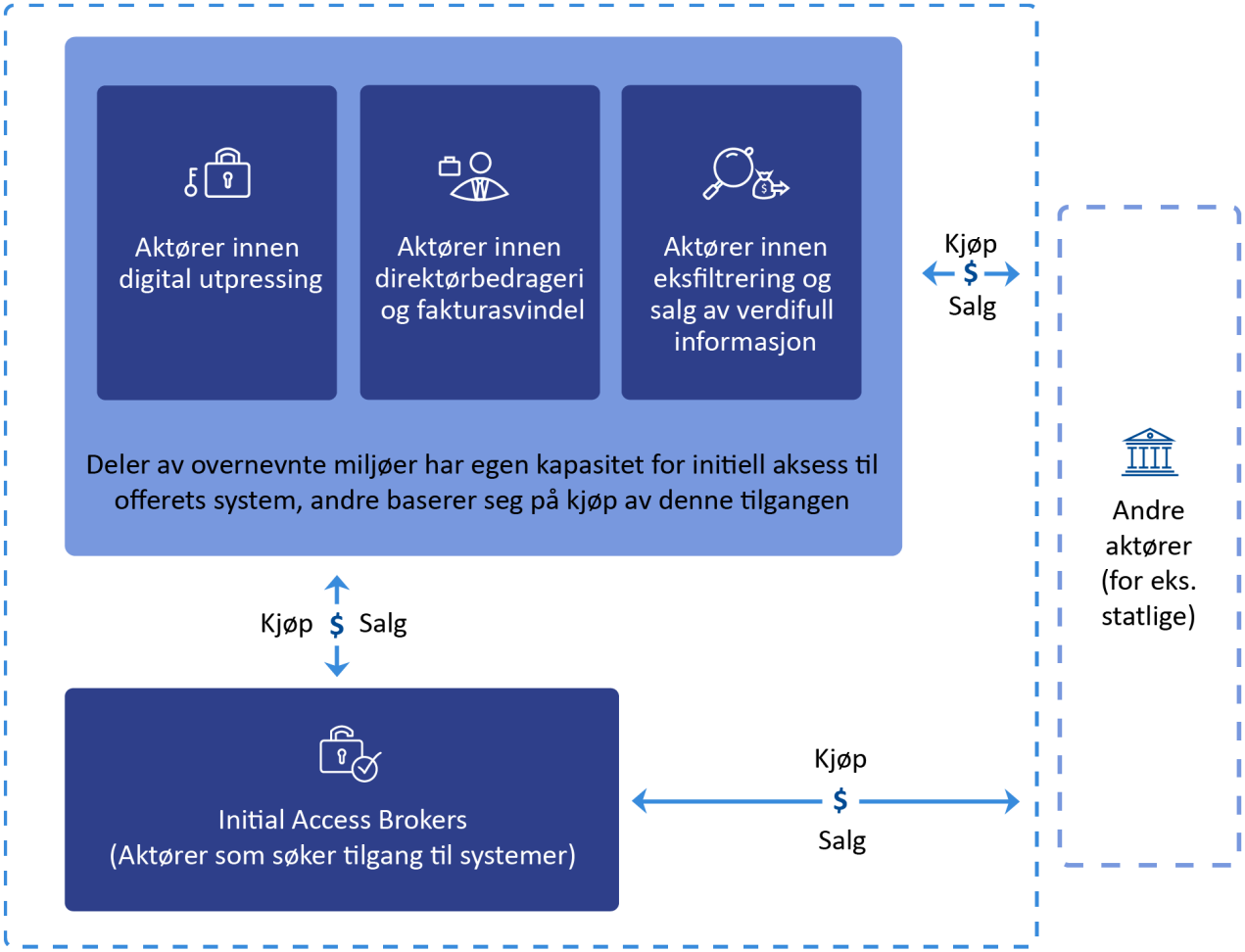
Kategorisering | Initial access brokers | Digital utpressing | Aktører innen videresalg av informasjon | Direktørberageri og fakturasvindel | Vurdering

Illustrasjonsfoto: Shutterstock, Pressmaster

KATEGORISERING AV AKTØRER INNEN ORGANISERT KRIMINALITET

Felles for organiserte kriminelle aktører i cyberdomenet er at deres primære motivasjon er økonomisk vinning. Samtidig er det også eksempler hvor disse organisasjonene har gjennomført operasjoner med andre motiver som politiske hensyn, hevn, ikke-økonomisk utpressing eller rendyrket vandalisme [12], [13]. Statistikk viser at 95 % av observerte dataangrep globalt er økonomisk motiverte [12].

Trusselbildet innen organisert kriminalitet i det digitale domenet er stort og komplekst. For å få oversikt er det derfor hensiktsmessig å dele aktørene inn i underkategorier etter hvordan de oppnår økonomisk vinning. Her beskrives kategoriene av organiserte kriminelle aktører som er vurdert å være mest relevant for spesialisthelsetjenesten.



Figur 3:
Kategorisering av aktører innen organisert kriminialitet basert på hvordan de oppnår økonomisk vinning.

Digitale utpressingsaktører

Digitale utpressingsaktører oppnår økonomisk vinning ved utpressing, primært mot virksomheter [14]. Denne aktørkategorien er såpass relevant for spesialisthelsetjenesten at økosystemet beskrives i større detalj i en egen figur under digital utpressing, evne. Disse aktørene benytter ulike former for utpressing, og metodene kan benyttes alene eller kombineres [14]. Utpressingsmetodene skilles fra hverandre i denne rapporten fordi metoden vil påvirke hvilke mål, altså hvilke verdier i spesialisthelsetjenesten, aktørene vil søke:

Utpressing (kryptering): Denne utpressingsmetoden innebærer at aktørene tar kontroll over og gjør systemene til en virksomhet utilgjengelige ved bruk av skadevare som krypterer systemet. Deretter krever angriperen løsepenger i bytte mot krypteringsnøkkel som kan gjøre systemene tilgjengelige igjen [14]

Utpressing (informasjonslekkasje): Metoden oppsto som et supplement til et digitalt utpressingsangrep (kryptering), med hensikt å legge ekstra press på ofrene, og ble derfor kalt dobbel utpressing. Metoden blir nå i økende grad brukt som en egen utpressingsmetode, og i denne rapporten kalles det derfor digital utpressing (informasjonslekkasje) [16]. 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 [17], [18], [9], [16].

Tredjeparts utpressing: Det finnes også eksempler på andre former for digital utpressing som for eksempel å kreve løsepenger fra en tredjepart, som pasienter eller kunder for ikke å offentliggjøre informasjonen deres. Denne formen for utpressing er langt mer sjelden enn de to overnevnte [17], [8], [19], [20].

Initial Access Brokers

Flere grupper av aktører spesialiserer seg på å skaffe tilgang til virksomheters systemer, for så å oppnå økonomisk vinning ved videresalg av disse tilgangene. Aktørene her er kjent som «Initial Access Brokers» og videresalget av tilgangene skjer som oftest til andre aktører innen digital utpressing. Initial Access Brokers omtales derfor ofte som en del av økosystemet knyttet til digital utpressing, men kan også selge tilganger til andre kriminelle eller statlige aktører [7], [17], [5].

Aktører spesialisert på videresalg av informasjon

Enkelte grupper av kriminelle aktører har som mål å hente ut sensitiv informasjon av virksomheters systemer for å oppnå økonomisk vinning ved videresalg. Dette kan være i forbindelse med industrispionasje eller i form av bruk til andre formål hos kriminelle eller statlige aktører [21].

Aktører som driver med direktørbedrageri og fakturasvindel

Andre grupper av kriminelle aktører er spesialisert på direktørbedrageri eller fakturasvindel. I direktørbedrageri utgir aktørene seg for å være en leder og kontakter medarbeidere i en virksomhet for å manipulere de til å overføre en større sum penger eller godkjenne utbetalinger. Fakturasvindel handler om å få personer med betalingsmyndighet til å godkjenne og betale falske fakturaer [22], [23].

Videre i dette delkapitlet beskrives hver av disse aktørkategoriene og deres vilje og evne.

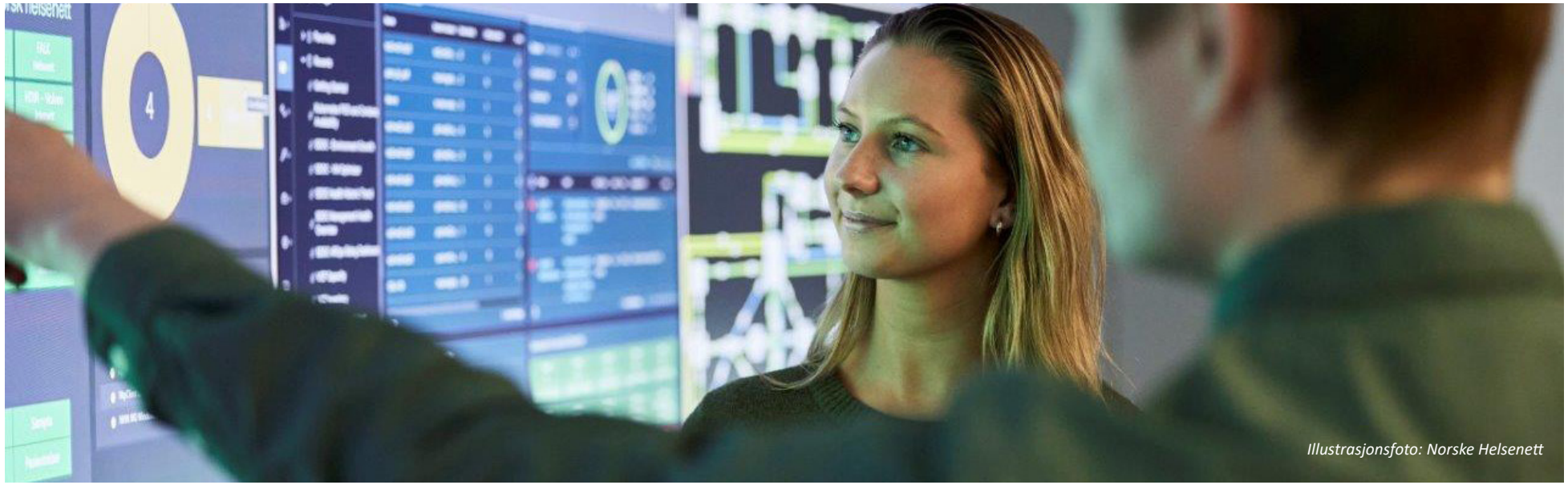
Illustrasjonsfoto: Norske Helsenett

INITIAL ACCESS BROKERS

Vilje
Det er digital utpressing og spesielt Ransomware-as-a-Service (RaaS)-modellen, beskrevet senere i kapitlet under digital utpressing - evne, som driver mesteparten av etterspørselen for Initial Access Brokers [5]. I 2022 er det observert en kraftig økning i etterspørselen for tjenestene til Initial Access Brokers [10]. Disse aktørene er ofte opportunistiske i målutvelgelsen, men kan også rette operasjonene mot en sektor, utvalgte nasjoner eller lignende [24]. Tilgang til digital infrastruktur er et mål for disse aktørene [25].

Aktørene er motivert av økonomisk vinning og det er derfor en fordel for Initial Access Brokers å kompromittere mål som vil gi god fortjeneste ved videresalg [17]. Spesialisthelsetjenesten ser stadig forsøk på kompromittering av aktører kjent som Initial Access Brokers [15].

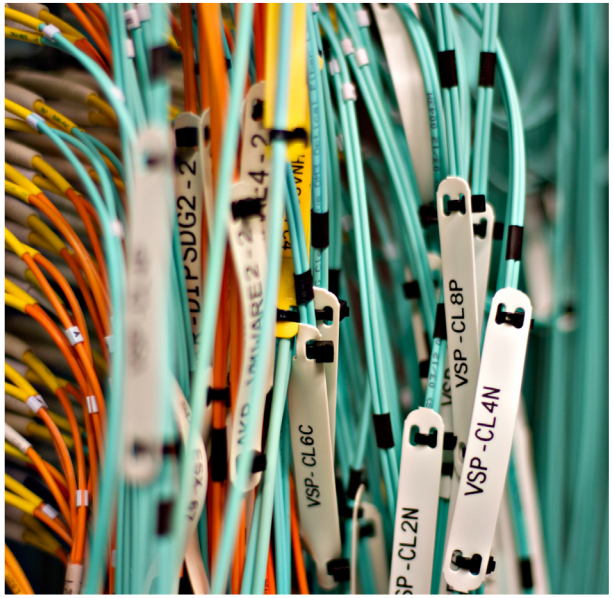
Evne
Tilgangene Initial Access Brokers videreselger varierer fra kompromitterte brukerkontoer til fullstendig kompromitterte systemer. Det betyr også at det varierer hvor langt ut i Cyber Attack Lifecycle, jf. kapittel 2, disse aktørene opererer [17]. Tilgangene selges både offentlig på undergrunns forumer og direkte til andre digitale utpressingsaktører [26]. Enkelte Initial Access Brokers tilbyr salg av kompromitterte tilganger sortert på geografisk område, yrkesgrupper og sektorer [24]. Angrepsvektorene som benyttes av Initial Access Brokers sammenfaller i stor grad med aktørene innen digital utpressing, og er dekket av neste delkapittel om digital utpressing.


Illustrasjonsfoto: Norske Helsenett

AKTØRER INNEN DIGITAL UTPRESSING

Norsk politi vurderer digital utpressing mot virksomheter som den største kriminalitetstrusselen mot digital infrastruktur [18]. Digital utpressing har stort skadepotensiale for virksomheter på flere områder. Et angrep kan medføre meget høye kostnader, spesielt knyttet til nedetid, gjenoppretting og opprydding [27], [18]. I 2022 kostet et gjennomsnittlig digitalt angrep mot helsesektoren globalt 10 millioner USD [32]. Digital utpressing kan også få konsekvenser for pasientbehandlingen [29]. En amerikansk undersøkelse av digitale utpressingsangrep mot helse viser at omtrent halvparten av angrepene påvirket pasientbehandlingen og at den gjennomsnittlige påvirkningen varte i 16 dager [31]. I tillegg kan sensitiv informasjon bli kompromittert og offentliggjort [24], [29], [31]. Den samme undersøkelsen viser at helseopplysninger ble offentligjort i hvert femte angrep [31].

Forretningsmodellen til digitale utpressingsaktører har vist seg å være svært effektiv. Aktørene har over tid hatt høy fortjeneste på sin virksomhet og har utviklet dette til en milliardindustri [32].



Illustrasjonsfoto: Sykehuspartner

Eksempel

Center Hospitalier Sud Francilie
I august 2022 ble et sykehus i Frankrike, Center Hospitalier Sud Francilien (CHSF), rammet av utpressings-skadevaren Lockbit. I angrepet ble alle systemene utilgjengeliggjort og sykehuset ble presset for 10 millioner USD. Utpressingen var både for å tilgjengeliggjøre systemene igjen og for at aktøren ikke skulle publisere sensitiv informasjon som var hentet ut i angrepet. CHSF betalte ikke, dermed ble operasjoner utsatt og pasienter ble sendt til andre sykehus. Til slutt publiserte trusselaktøren også informasjonen som var stjålet.

Digital utpressing - Vilje

Flere rapporter viser at helsesektoren er blant de mest utsatte sektorene globalt for digital utpressing [33], [24], [34]. Norsk politi vurderer det som sannsynlig at virksomheter med samfunnskritiske funksjoner rammes av digital utpressing [18]. Mot virksomheter generelt er aktørene fortsatt svært aktive, men basert på kildegrunnlaget til denne rapporten har det vært en reduksjon i antall angrep i 2022 sammenlignet med 2021 [24], [35], [36]. Dette stemmer også overens med hva NSM rapporterer nasjonalt [37].

De nasjonale åpne trusselvurderingene gir ikke spesifikke vurderinger mot helsesektoren. Det danske cybersikkerhetssenteret (CFCS), underlagt dansk etterretningstjeneste, gjør derimot vurderinger mot helsesektoren i Danmark som vi mener er sammenlignbare. I Danmark vurderes trusselen fra organisert kriminalitet som meget høy mot helsesektoren [29].

En annen rapport viser også at helsesektoren er høyt oppe på listen over hvilke sektorer som opplever mest aktivitet fra digitale utpressingsaktører i Norden [38].

For å gi en indikasjon på omfanget av digital utpressing mot helse er det trukket ut noen tall fra en større undersøkelse som inkluderer 5 600 virksomheter fra 31 land, 400 av disse innen helse. To tredjedeler av virksomhetene innen helse har vært utsatt for digital utpressing og rett i underkant av to tredjedeler av disse angrepene endte med kryptering av systemer. Gjennomsnittlig gjenopprettingstid etter angrepene var én uke [39].

Illustrasjonsfoto: Sykehuspartner

Spesifikke mål i spesialisthelsetjenesten
Noen digitale utpressingsaktører har en opportunistisk tilnærming til målutvelgelse. Andre aktører går målrettet etter virksomheter som de tror vil gi høy avkastning, for eksempel innen finans eller helse [29], [40], [5]. Forholdet mellom disse strategiene er vanskelig å tallfeste [30]. I tillegg vil ofte flere typer organiserte kriminelle aktører være inne i ulike faser av et angrep. Dette kan bety at en initiell kompromittering er opportunistisk, mens tilgangen deretter videreselges til en aktør som er målrettet i sin målutvelgelse [30].

Dette delkapitlet beskriver hvorfor organiserte kriminelle aktører spesielt forsøker å angripe spesialisthelsetjenesten. Dette innebærer hvilke spesifikke verdier spesialisthelsetjenesten innehar som tiltrekker seg aktørene, men også mer generelle verdier som kan være et mål for aktørene, og andre sentrale drivere. De fleste digitale utpressingsaktører vil kryptere offerets systemer og i tillegg hente ut sensitiv informasjon og true med å publisere denne [16]. Dette betyr at målene til digitale utpressingsaktører også i stor grad innebærer ulike former for sensitiv informasjon, i tillegg til tilgjengeligheten av systemet i seg selv.

Kritikalitet ved nedetid
Sykehus leverer 24/7-tjenester og utfører samfunnskritiske funksjoner. For særlig godt digitaliserte helsetjenester, som spesialisthelsetjenesten i Norge, så er det viktig å unngå unødvendig nedetid. Organiserte kriminelle aktører vil ikke ha skrupler mot å ta ned kritiske sykehussystemer for å oppnå høy profitt i digitale utpressingsangrep (kryptering) [20], [40]. Flere rapporter viser til at helsesektoren er ekstra utsatt for denne typen angrep fordi trusselaktørene vet at nedetid er kritisk for virksomhetene og at man derfor kan være mer mottakelig for å gi etter for utpressing [29], [40], [41], [42], [43].

Kliniske tjenester
Det er observert flere angrep av digitale utpressingsaktører som har medført konsekvenser for tilgjengeligheten til kliniske systemer og dermed også pasientbehandling [41], [30], [40].

Stor angrepsflate
Rapporter fremhever at helsesektoren globalt er et attraktivt mål for digitale utpressingsaktører grunnet sektorens tradisjonelt sett store angrepsflate. Med dette menes sektorens kompleksitet, distribuerte systemer og økende bruk av Internet of Medical Things. I tillegg er noen ganger medisinsk utstyr avhengig av operativsystemer som ikke lenger supporteres av leverandøren [29], [41], [42].

Personopplysninger
Personopplysninger er den hyppigst kompromitterte informasjonen i digitale angrep mot helsesektoren globalt [12]. Med personopplysninger menes enhver opplysning om en identifisert eller identifiserbar fysisk person [44]. Personopplysninger er et attraktivt mål for organiserte kriminelle aktører generelt, og kan også være verdifullt i digital utpressing (informasjonslekkasje) [41], [32], [42].

Helseopplysninger
En undersøkelse viser at helseopplysninger ble hentet ut i 46 % av dataangrep mot helsesektoren globalt [12]. Med helseopplysninger menes personopplysninger om en persons fysiske eller psykiske helse [44]. I forbindelse med utpressingsangrep (kryptering) har helseopplysningene en verdi i form av at det er kritisk at opplysningene er tilgjengelige. I tillegg har helseopplysninger en konfidensialitetsverdi i forbindelse med digital utpressing (informasjonslekkasje). Opplysningene kan også brukes i tredjepartsutpressing direkte mot pasientene [42], [45].

GDPR og helselovgivning
De digitale utpressingsaktørene er klar over de strenge kravene til behandling av person- og helseopplysninger og kan utnytte dette i digital utpressing (informasjonslekkasje) og forhandlinger om løsepenger [41], [42].

Forskning, utvikling og innovasjon
Forskningsinformasjon kan være spesielt attraktiv for videresalg, men kan også brukes i digital utpressing (informasjonslekkasje) [46], [29]. Sikkerhetsselskapet Mandiant trekker frem forskningsinformasjon som en sentral driver for trusselaktørers aktivitet mot helsesektoren globalt [42].

Faktaboks om Russlands krig mot Ukraina sin påvirkning på digitale utpressingsaktører

Digitale utpressingsaktører med tilhold i Øst-Europa har blitt påvirket i ulik grad av Russlands krig mot Ukraina. Noen utpressingsaktører har sverget troskap til Russland, mens andre har valgt en nøytral tilnærming og tydeliggjort at deres mål kun handler om økonomi. Flere av aktørene har tilpasset seg situasjonen og gjort større endringer i sin forretningsmodell som for eksempel å starte med RaaS. Andre aktører har i perioden med krig tilsynelatende lagt ned sin virksomhet [11]. Uavhengig av disse endringene fortsetter de russiskvennlige organiserte kriminelle aktørene å spille en viktig rolle for Russland. For noen innebærer dette en tydelig rolle hvor de deltar aktivt i angrep mot Ukraina og andre russiske mål for cyberoperasjoner, mens for andre aktører er det en mindre synlig kobling [11].

Eksempel Costa Rica

Våren 2022 ble myndighetene i Costa Rica nødt til å erklære unntakstilstand grunnet to digitale utpressingsangrep som rammet flere myndighetsorganer. Det første angrepet, i april, rammet blant annet det nasjonale skatte- og tollsystemet. Dette førte til at lønnsutbetalingsløsninger ble satt ut av spill, i tillegg kollapset landets eksport- og importlogistikk som følge av angrepet. Det neste angrepet, i mai, slo ut det nasjonale helsesystemet, som førte til at flere av landets sykehus knelte. Løsepengekravene varierte mellom 10 og 20 millioner USD. Summen ble ikke betalt, og de kriminelle aktørene publiserte derfor 50 % av informasjonen de hentet ut fra myndighetsorganene på internett, for å vise alvoret ved ikke å betale [24], [49].

Faktaboks om myndighetenes påvirkning av viljen til digitale utpressingsaktører

Flere land har uttalt at de ser på digital utpressing som en trussel mot kritisk infrastruktur og nasjonal sikkerhet. Vestlige myndigheter har derfor de senere årene trappet opp innsatsen og samarbeidet mot digitale utpressingsaktører [16]. En del av denne innsatsen er anbefalinger, påbud og krav til styring av sikkerheten hos virksomheter. Den andre delen er rettet mot trusselaktørene og innebærer etterforskning, sanksjoner, dusører og det er også gjennomført flere arrestasjoner [16].

I september 2021 oppdaterte amerikanske skattemyndigheter retningslinjer for betaling av løsepenger til digitale utpressingsaktører. Denne peker på juridisk risiko for virksomheter ved å betale ut løsepenger og viser også til forebyggende tiltak som må innføres for å redusere sannsynligheten for juridiske konsekvenser [47].

Utpressingsaktørene svarer denne innsatsen med mottiltak for å enten unngå eller vesentlig redusere myndighetenes kontroll, og for å vanskeliggjøre etterforskning og eventuell straffeforfølgelse. Dette innebærer organisering, anonymitetstjenester, kortere «levetid» for gruppene, bruk av kryptovaluta, bruk av metoder og verktøy som gjør etterforskning krevende [32], [16], [24]. Kripos viser til at lovgivningen og internasjonalt samarbeid fortsatt henger etter den raske digitale utviklingen, som gjør at aktørene opererer med lav oppdagelsesrisiko og enda mindre sjanse for å bli straffeforfulgt [48].

Illustrasjonsfoto: Shutterstock

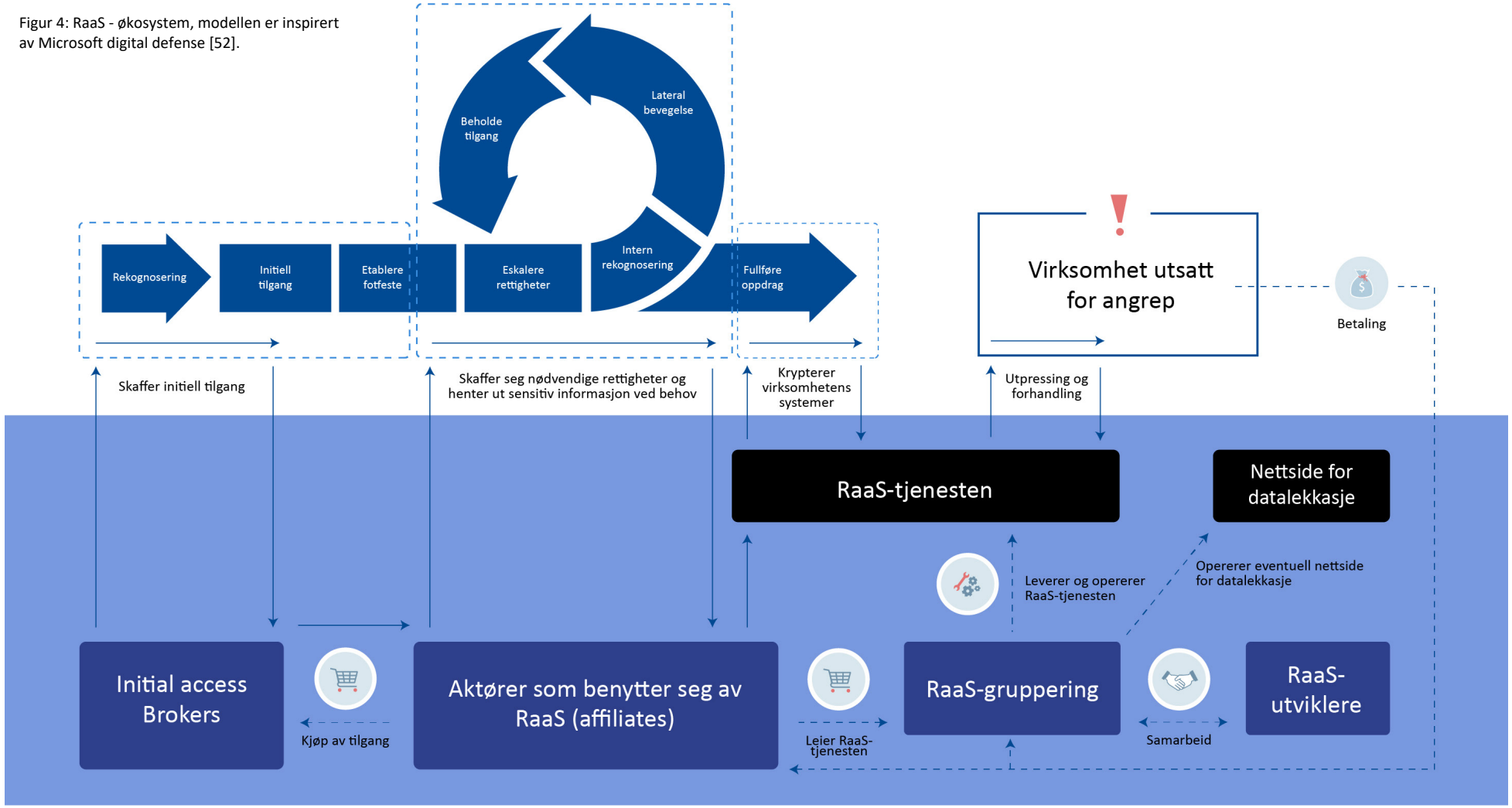
Digital utpressing - Evne

Økosystem innen digital utpressing, RaaS-modellen

Tidligere utførte ofte én aktør fullstendige angrep selvstendig. Dette forekommer fortsatt, men de siste årene har trenden vært at aktørene i større grad kjøper og selger tjenester seg imellom. Dette betyr at ulike aktører spesialiserer seg på en bestemt fase i et angrep og at flere aktører er involvert i hvert angrep [24], [16]. En forretningsmodell som er særlig relevant er Ransomware-as-a-Service (RaaS) og denne modellen og det tilknyttede økosystemet beskrives derfor i større detalj i figuren nedenfor.

Modellen her må sees på som en grov fremstilling av aktørenes samarbeid i RaaS-modellen. I realiteten er det mer flytende overganger og utfordrende å sette eksakte skiller. For eksempel vil det variere hvor dypt inn i systemet en Initial Access Broker har skaffet seg tilgang [24].

Figur 4: RaaS - økosystem, modellen er inspirert av Microsoft digital defense [52].



RaaS-aktør

I kjente angrep er det ofte navnet på RaaS-aktørene som blir referert til i media, eksempler på dette er LockBit, Conti og HIVE. RaaS-aktørene stiller med selve verktøyet eller skadevaren som krypterer virksomhetens systemer, samt kommunikasjons- og betalingsløsninger [24]. Utover dette varierer tjenestene de ulike RaaS-aktørene leverer.

De kan blant annet bidra i forhandlingene med virksomhetene som er angrepet, stille med utpressingsbrev, bidra med brukerstøtte til offeret og dekryptering dersom virksomheten betaler. De opererer gjerne også nettsider for lekkasje av sensitiv informasjon, såkalte «data leak sites», som benyttes dersom ofrene ikke betaler [16], [30]. Enkelte aktører har publisert informasjonen til over tusen ofre på sine nettsider [50]. I tillegg kan aktørene tilby tjenester innen overføring av kryptovaluta og hvitvasking [30].

Tjenestene leies ut til andre aktører for en andel av fortjenesten i angrepet. Merkenavn og pålitelighet er viktig for RaaS-aktørene. På denne måten skaper de forutsigbarhet hos sine ofre; virksomheter skal kjenne navnet deres og dermed være klar over hva som skjer dersom man velger å ikke betale. Samtidig skal de også skape nødvendig tillit, slik at ofrene vet at de får informasjonen og tilgjengeligheten på systemene tilbake dersom de velger å betale. Tilliten er også viktig mot aktørene som benytter seg av RaaS og andre aktører i økosystemet [32].

Trusselaktørene som benytter RaaS

Trusselaktørene som benytter RaaS blir ofte kalt affiliates i RaaS-modellen. Dette er gjerne mindre grupperinger av organiserte kriminelle aktører som benytter seg av en eller flere RaaS. Mange av disse aktørene kjøper den initielle tilgangen til systemer av Initial Access Brokers, mens andre skaffer tilgang selv [7], [17], [5]. Det er disse aktørene som utfører operasjonene i virksomhetens infrastruktur etter den initielle kompromitteringen, som for eksempel lateral bevegelse og eskalering av rettighetsnivå [24]. Som regel er det også denne aktøren som henter ut sensitiv data av systemene og om mulig også tar kontroll over virksomhetens backup-løsninger. Deretter kjører de selve krypteringsskadevaren, som de etter avtale leier av en RaaS-aktør [24].

RaaS-utviklere

RaaS-utviklere er profesjonelle personer eller grupperinger som utvikler og vedlikeholder verktøyene RaaS-aktørene leverer. Utviklerne kan være en del av RaaS-aktøren, eller en aktør som jobber mer selvstendig og tar betalt for tjenestene sine [24], [20].

Initial Access Brokers

Initial Access Brokers er tidligere beskrevet i denne rapporten, men er en viktig aktør i økosystemet for digital utpressing, siden det i mange tilfeller er de som skaffer den initielle tilgangen til virksomheten. Initial Access Brokers er lavest nede på næringskjeden av disse aktørene, da selve avkastningen fra angrepet som regel ikke deles med Initial Access Brokers [5].

Oppsummering RaaS

Det er RaaS-modellen som for tiden driver veksten i økosystemet for digitale utpressingsaktører [16]. For utleie av tjenesten tar RaaS-aktørene typisk betalt 10-20 % av fortjenesten i et angrep. RaaS-aktørene ønsker derfor at flest mulig aktører skal benytte deres tjenester [9].

Hovedårsakene til at RaaS er utviklet som forretningsmodell er at RaaS-aktørene kan skalere raskere og øke inntjening samtidig som de kan operere med lavere risiko for å bli tatt. Aktørene bak RaaS eksponerer seg ikke i nettet til virksomheter slik som Initial Access Brokers og trusselaktørene som benytter RaaS. I tillegg er det en tydelig trend at det er en lavere terskel for å entre dette økosystemet og aktører oppstår oftere og består kortere [36], [24], [32]. Økosystemet er preget av anonymitet og fortrolighet. Dersom én aktør som benytter en RaaS blir tatt, vil RaaS-aktørene fortsatt kunne drifte som normalt siden andre aktører fortsatt benytter deres tjenester [32], [24]. Disse faktorene kompliserer etterforskning og reduserer på den måten sannsynligheten for at aktørene blir tatt [24].

Illustrasjonsfoto: Shutterstock

Illustrasjonsfoto: Sykehuspartner

Digital utpressing - Evne fortsettelse

Modus operandi

De største aktørene innen digital utpressing fremstår som meget organiserte med stillingsannonser, lønn og ansattgoder tilsvarende ordinære virksomheter [16]. I lekkasjer fra aktøren Conti fremkommer det at de har hatt ulike avdelinger med dedikerte budsjetter, ledelse, og til og med egen HR-avdeling [13], [51], [17]. Den høye fortjenesten fra digital utpressing forsyner det kriminelle økosystemet med midler som muliggjør forskning og utvikling [52], [41], [19]. Som et eksempel på høy fortjeneste tjente en nyopprettet RaaS-aktør rundt 100 millioner USD gjennom utpressingsangrep mot totalt 1 300 virksomheter på litt over ett år [50]. Aktørene er tilpasningsdyktige og evner å endre teknologi, organisering, metoder og verktøy for å omgå sikringstiltak og unngå selv å bli tatt [53], [19], [32], [24].

Det har blitt observert en økning i digital utpressing (informasjonslekkasje), og denne formen for utpressing forekommer nå like ofte som kryptering [16]. Rapporter indikerer at digitale utpressingsaktører blir bedre til å finne sensitiv informasjon hos ofrene og at enkelte av aktørene dropper selve krypteringen og baserer forretningsmodellen sin på kun digital utpressing (informasjonslekkasje) [9], [24], [18].

Det siste året er det observert økt aktivitet mot backupløsninger for å vanskeliggjøre gjenoppretting etter angrep [54]. Det er også en trend at digitale utpressingsaktører, i større grad enn tidligere, utfører angrep uten å benytte skadevare. Dette kan være bruk av legitime verktøy og programmer som allerede er installert hos offeret [9], [10]. Fordelen til aktørene er at dette øker sannsynligheten for å unngå virksomheters sikkerhetsmekanismer og derav reduserer sannsynligheten for å bli oppdaget [9].

Angrepsvektorer

Mange av aktørene innen digital utpressing benytter seg av de samme angrepsmetodene og teknikkene, og utnytter de samme sårbarhetene [24]. Generelt ser man at verktøy og metoder som først var eksklusive senere blir offentlig tilgjengelig [9]. De tre mest brukte angrepsvektorene for digitale utpressingsaktører og Initial Access Brokers er phishing og spear phishing, utnyttelse av fjerntilgangsløsninger og utnyttelse av sårbarheter i internetteksponerte tjenester og servere [55], [24], [18], [33]. Aktørene har også benyttet leverandørkjedeangrep og i noen tilfeller har det vært observert forsøk på rekruttering av innsidere [20], [16], [13], [56], [57].

I rapporteringsperioden er det observert en økning i bruk av eksternt medie for å skaffe initiell tilgang. Konkret er det snakk om at skadevare leveres via USB-minnepinne i forbindelse med en større kampanje for å levere en skadevare kalt Rasperry Robin [9]. I Spesialisthelsetjenesten er det observert en økning i forsøk på å levere skadevare ved bruk av USB-minnepinne [15].

Utenfor konkrete angrepsvektorer for initiell tilgang spiller også utnyttelse av påloggingsopplysninger en sentral rolle i mange angrep, både i forbindelse med initiell tilgang og etter at fotfeste er etablert. Mange angrep inkluderer også en form for sosial manipulering eller menneskelig interaksjon [10], [16], [12], [55].

AKTØRER SPESIALISERT PÅ VIDERESALG AV INFORMASJON

Vilje
Det er blitt vanligere globalt at sensitiv informasjon hentes ut, også i angrep mot helsesektoren. Denne informasjonen brukes til digital utpressing, men kan også videreselges [20], [53], [18], [9], [24]. Politiet mener det er sannsynlig at bedrifter med roller i kritiske samfunnsfunksjoner i økende grad vil bli utsatt for angrep som innebærer tyveri av data [18].

Danske CFCS viser til at kriminelle aktører kan gå etter forskningsdata eller patenter i helsektoren for å videreselge informasjonen [29], [46]. Finansiell informasjon er også et attraktivt mål for kriminelle aktører [9]. Dette kan for eksempel være tjenester med betalingsløsninger for pasienter, lønnssystemer, faktura osv. Det finnes flere eksempler på at slik informasjon er hentet ut i angrep mot helsesektoren [29], [58].

I en stor mengde av vellykkede dataangrep globalt blir påloggingsopplysninger kompromittert. Dette kan være som et steg i et angrep, men kan også være et mål i seg selv [12], [19], [37]. Større mengder påloggingsopplysninger kan hentes ut og videreselges. Det er et velutviklet marked for kjøp og salg av slike opplysninger [10]. NSM har sett eksempler på at aktører nyttiggjør seg av påloggingsopplysninger i dataangrep flere år etter at kompromitteringen fant sted [37].

Helsesektoren behandler svært store mengder helse- og personopplysninger og dette pekes også på som en årsak til at helsesektoren er et mål for organiserte kriminelle aktører [41], [32], [42]. Slike opplysninger kan videreselges til aktører som bruker det til direktørbedrageri, målrettede phishingangrep eller annen svindel [37], [42], [45].

Evne
I kildegrunnlaget for denne rapporten er det vanskelig å finne informasjon som skiller evnene til disse aktørene fra andre organiserte kriminelle aktører, som for eksempel digitale utpressingsaktører [20], [53], [18], [9], [24].

Det er naturlig at det er store mørketall knyttet til disse aktørene da noe av formålet er å hente ut informasjon uten å bli oppdaget.

Illustrasjonsfoto: Sykehuspartner

AKTØRER SOM DRIVER MED DIREKTØRBEDRAGERI OG FAKTURASVINDEL

Vilje
Politiet peker på bedrageri som en økende trussel mot norske virksomheter og viser til at det sannsynligvis foreligger store mørketall. I tillegg viser politiet i denne forbindelsen til at bedrageri er en milliardindustri i Sverige [18], [27]. Bedrageriene varierer fra lite avanserte til svært sofistikerte utført av profesjonelle aktører som har kompromittert nettverk eller e-post kontoer i forkant [27]. Spesialisthelsetjenesten har tidligere opplevd forsøk på fakturasvindel og opplever også til stadighet lite avanserte forsøk på direktørbedrageri [15]. I direktørbedrageri og fakturasvindel vil personell som er involvert i fakturagodkjenning eller som har økonomisk fullmakt på vegne av virksomheten, være et mål for kriminelle aktører [22].

Et eksempel på fakturasvindel er hendelsen mot UiT Norges arktiske universitet i 2019, hvor de ble utsatt for fakturasvindel og tapte rundt 12 millioner kroner [59], [27]. Et annet eksempel er en norsk virksomhet som tapte flere hundre millioner kroner i et direktørbedrageri i 2016 [60]. Fakturasvindel og direktørbedrageri mot virksomheter og enkeltpersoner er tidligere rapportert som den mest innbringende, og dermed også største, kriminelle aktiviteten i det digitale domenet i USA [61].

Evne
Politiet viser til at disse aktørene er mer sofistikerte og målrettede i sine angrep enn tidligere; de bruker korrekt språk, selv om det i de fleste tilfellene er snakk om internasjonale aktører [18]. Faktura- og direktørbedrageri krever som regel at trusselaktøren i forkant har skaffet seg informasjon om nøkkelpersoner i en virksomhet [23]. Bedrageriene handler om sosial manipulering og kan gjøres ved hjelp av ulike angrepsvektorer, som for eksempel e-post eller telefon [16].

De senere årene har de mest sofistikerte angrepene av denne typen inkludert bruk av Business Email Compromise (BEC). BEC innebærer at angriper skaffer tilgang til en eller flere e-postkontoer i en virksomhet, og bruker denne til å gjennomføre phishing eller annen sosial manipulering, med den fordelen at e-posten tilsynelatende kommer fra en kollega [62], [24]. BEC er en effektiv metode som utvikles raskt og er, etter phishing, en av de mest brukte formene for sosial manipulering [12], [20].

Et sofistikert angrep beskrevet av amerikanske Federal Bureau of Investigation (FBI), begynner med at en trusselaktør kompromitterer e-posten til en daglig leder eller økonomidirektør hos en virksomhet. Deretter kaller aktøren inn en person, med betalings- eller overføringsmulighet, til et virtuelt møte. I møtet settes det gjerne inn et profilbilde av direktøren og trusselaktøren hevder at det er problemer med video og lyd og foreslår heller å bruke chat. Eventuelt kan stemmen til direktøren etterlignes ved bruk av deepfake-teknologi. Videre instruerer trusselaktøren personen til å gjøre en overføring til en konto trusselaktøren har kontroll over [61]. Økokrim vurderte i 2022 at det er meget sannsynlig at ny teknologi som deepfake vil bli benyttet i økt omfang i forsøk på direktørbedrageri [63].

Illustrasjonsfoto: Shutterstock

Illustrasjonsfoto: Shutterstock

VURDERING ORGANISERT KRIMINALITET

Organiserte kriminelle aktører
Overordnet vurdering mot spesialisthelsetjenesten

Aktører som driver med digital utpressing	Vilje	Evne	Skadepotensiale
	Meget høy	Høy	Meget høyt
Initial Access brokers	Vilje	Evne	Skadepotensiale
	Meget høy	Høy*	Høyt
Aktører som driver med kompromittering og videresalg av informasjon	Vilje	Evne	Skadepotensiale
	Høy*	Medium**	Høyt
Aktører som driver med faktura og direktørbedrageri	Vilje	Evne	Skadepotensiale
	Meget høy	Medium	Lavt*

Vurdering digital utpressing og Initial Access Brokers

Vi vurderer at den mest alvorlige trusselen mot spesialisthelsetjenesten er aktørene som driver med digital utpressing. Aktørenes vilje er vurdert å være **meget høy**. Dette er begrunnet i hva vi observerer, disse aktørenes høye aktivitetsnivå mot helsesektoren globalt og hvordan vi har vurdert viljen mot flere av verdiene i spesialisthelsetjenesten. Evnen til digitale utpressingsaktører er vurdert **høy.** Det må presiseres at evnen ikke er redusert fra fjorårets rapport, men at vi har gjort et bevisst valg på å bruke skalaen bedre. Disse aktørene er meget profesjonelle og tilpasningsdyktige og utvikler forretningsmodellene raskt for å kunne øke inntjening og redusere risiko. Skadepotensialet av digital utpressing er vurdert å kunne være **meget høyt**, basert på sammenlignbare hendelser globalt. Dette er spesielt med hensyn til kryptering av kritiske systemer som kan ramme pasientbehandling, høye kostnader ved nedetid, gjenoppretting og opprydding, samt kompromittering og publisering av sensitiv informasjon som for eksempel person- og helseopplysninger.

I et eventuelt digitalt utpressingsangrep mot spesialisthelsetjenesten vurderer vi det som **meget sannsynlig** at aktøren vil kryptere systemer for utpressing, **meget sannsynlig** at aktøren i tillegg til å kryptere systemer også vil hente ut sensitiv informasjon, **mulig** at aktørene kun vil hente ut sensitiv informasjon og til sist vurderes det som **lite sannsynlig** at målet vil være tredjeparts utpressing mot pasienter.

Vilje
Det vurderes som **meget sannsynlig** at virksomheter i spesialisthelsetjenesten vil være ansett som et attraktivt mål for aktører innen digital utpressing. Det vurderes som **meget sannsynlig** at spesialisthelsetjenesten vil bli utsatt for opportunistiske forsøk på digitale utpressingsangrep. Basert på verdiene vi besitter vurderes det som **sannsynlig** at spesialisthelsetjenesten vil bli utsatt for målrettede angrep fra digitale utpressingsaktører.

Mot helse vurderes **meget sannsynlig** den mest sentrale driveren til digitale utpressingsaktører å være den høye kritikaliteten ved nedetid på IKT-systemer, gitt systemenes samfunnskritiske funksjon. Dette innebærer også at kliniske systemer kan være et mål. En annen sentral driver for digitale utpressingsaktører er at helsesektoren, i et globalt perspektiv, tradisjonelt sett har vært en sektor preget av stor angrepsflate.

Det vurderes som **meget sannsynlig** at helseopplysninger og personopplysninger er de mest attraktive informasjonsmålene til digitale utpressingsaktører (informasjonslekkasje). Det vurderes som **sannsynlig** at forskning og innovasjon, påloggingsopplysninger og finansiell og økonomisk informasjon også vil være attraktive mål. Det vurderes som **mulig** at også intern og skjermingsverdig informasjon er attraktive mål for digitale utpressingsaktører.

Vi vurderer det som **sannsynlig** at en av våre leverandører vil rammes av et digitalt utpressingsangrep som kan ha skadepotensiale for spesialisthelsetjenesten.

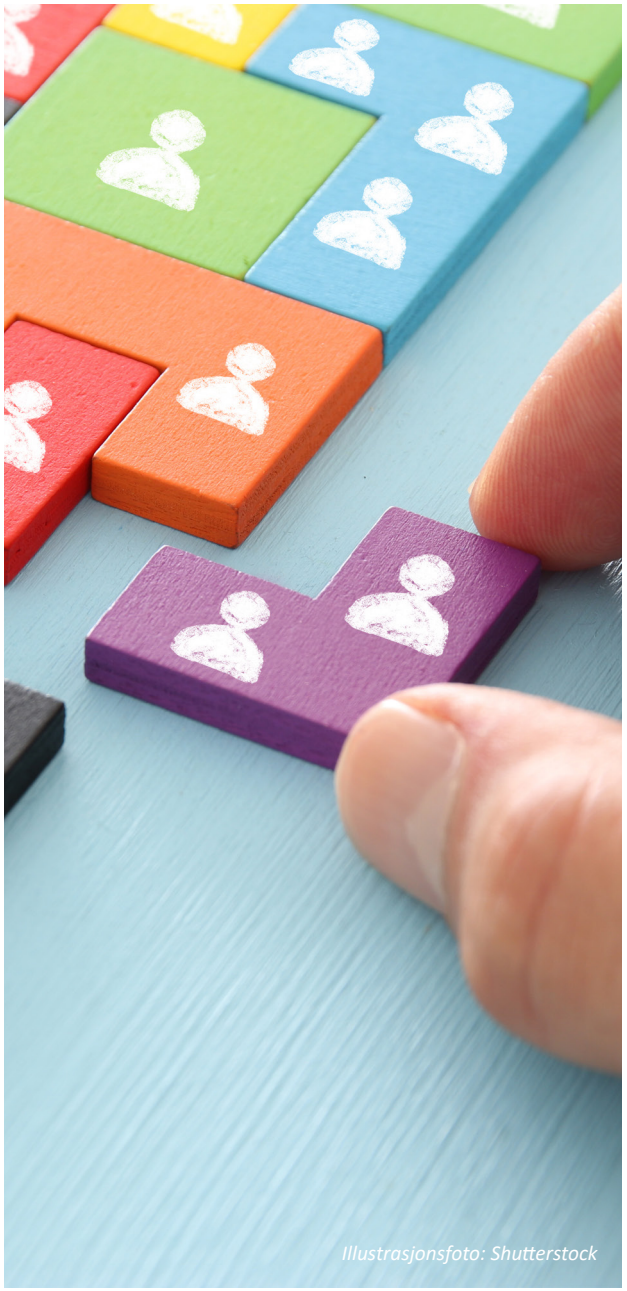
Evne
Enkelte av de mest aktive aktørene innen digital utpressing er ressurssterke, velorganiserte og tilpasningsdyktige, og har utviklet avanserte metoder og verktøy for å oppnå økonomisk vinning. Det vurderes som **sannsynlig** at økosystemet innen digital utpressing vil fortsette å utvikle sine kapabiliteter, sin organisering og tilpasse seg nye sikkerhetstiltak. Det vurderes som **sannsynlig** at digitale utpressingsaktører i større grad enn tidligere vil benytte seg av skadevarefrie angrep, for å unngå deteksjons- og sikkerhetsløsninger.

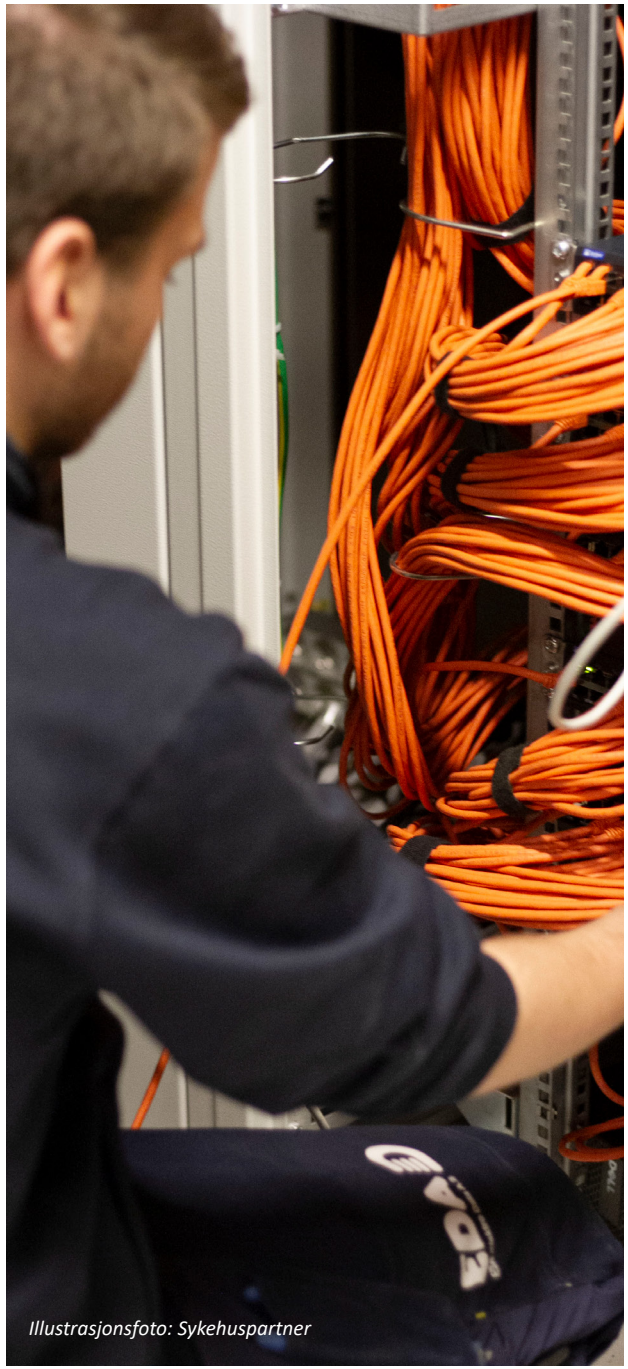
Vurdering av hvilke angrepsvektorer organiserte kriminelle aktører innen digital utpressing og Initial Access Brokers vil benytte seg av for å oppnå initiell tilgang til spesialisthelsetjenestens systemer:

Det vurderes også som **meget sannsynlig** at disse aktørene vil forsøke å kompromittere eller på andre måter utnytte påloggingsopplysninger i et eventuelt angrep.

Vi vurderer det som **sannsynlig** at kombinasjonen av vestlige myndigheters tiltak mot digitale utpressingsaktører og Russlands krig mot Ukraina er faktorer som har bidratt til at den generelle aktiviteten til digitale utpressingsaktører har stagnert i 2022.

Vurdering	Angrepsvektor for initiell tilgang
Meget sannsynlig	Phising og spear phising
Meget sannsynlig	Utnyttelse av fjerntilgang
Meget sannsynlig	Utnyttelse av sårbarheter i internetteksponerte tjenester og servere
Sannsynlig	Leverandørkjedeangrep (ikke målrettet)
Sannsynlig	Eksternt medie (for eksempel USB-minnepinne)
Meget lite sannsynlig	Innsidere
Meget lite sannsynlig	Leverandørkjedeangrep (målrettet)


Illustrasjonsfoto: Shutterstock



Illustrasjonsfoto: Sykehuspartner

Vurdering av aktører spesialisert på å hente ut informasjon for videresalg

Vurderingen av disse aktørene har et lavt til medium konfidensnivå. Det vurderes som **mulig** at organiserte kriminelle aktører vil utføre angrep mot spesialisthelsetjenesten med formål kompromittering og videresalg av informasjon som en metode for økonomisk vinning. Vi vurderer **sannsynlige** informasjonsmål å være forskning og innovasjon, samt finansiell og økonomisk informasjon. **Mulige** mål vurderes å være person- og helseopplysninger og påloggingsopplysninger.

Det foreligger lite informasjon om evnen til aktører som kompromitterer informasjon for videresalg og hvordan disse er organisert i forhold til økosystemet for digital utpressing. Det må forventes at det er større mørketall knyttet til disse aktørene, da hensikten er å hente ut informasjon uten å bli oppdaget. Det vurderes likevel som **sannsynlig** at det ligger mindre profitt i denne type aktivitet enn i digital utpressing. Dersom dette stemmer er det rimelig å anta at evnen er lavere og vil utvikle seg tregere enn evnen til aktørene innen digitial utpressing. Det vurderes som **sannsynlig** at angrepsvektorene vurdert i tabellen for digitale utpressingsaktører, er gjeldende for denne aktøren også, men med et sannsynlighetsnivå lavere på alle angrepsvektorene

Vurdering fakturasvindel og direktørbedrageri

Det vurderes som **meget sannsynlig** at virksomheter i spesialisthelsetjenesten vil bli forsøkt utsatt for fakturasvindel og direktørbedrageri. Personer involvert i fakturagodkjenning eller med økonomimyndighet vurderes **meget sannsynlig** å være attraktive mål for kriminelle aktører som driver med faktura- og direktørbedrageri.

Evnen til disse aktørene er vurdert som **medium**, det presiseres at dette gjelder cyberkapabiliteter. Disse aktørene er spesialisert på sosial manipulering og innen dette fagområdet har de en **meget høy** evne til å lykkes. Aktørene som driver med fakturasvindel og direktørbedrageri vil **meget sannsynlig** benytte seg av sosial manipulering i angrep mot spesialisthelsetjenesten. Enkelte av disse aktørene bruker også aktivt BEC som metode i sine operasjoner. Det vurderes som **mulig**, med medium konfidensnivå, at disse aktørene vil forsøke å kjøpe eller selv skaffe tilgang til spesialisthelsetjenestens IKT-systemer for å kunne ta i bruk BEC som en metode i sine operasjoner.

Det vurderes videre som **mulig** at det norske språket fortsatt fungerer som en sikkerhetsbarriere mot at fakturasvindel og direktørbedrageri vil lykkes. Vi vurderte i fjorårets rapport at det er **sannsynlig** at denne barrieren vil fortsette å viskes ut. Denne vurderingen står vi fortsatt ved og viser spesielt til utviklingen i teknologi og kunstig intelligens.

03.

DEL 2

Statlige aktører

Innledning | Spionasje | Destruktive angrep | Påvirkningsoperasjoner

Illustrasjonsfoto: Shutterstock, Andrei Kobylko

INNLEDNING/OVERORDNET

Statlige trusselaktører er grupper eller organisasjoner som opererer i samarbeid med eller på vegne av en stat. I denne rapporten er de omtalte statlige trusselaktørene i hovedsak andre nasjoners sikkerhets- og etterretningstjenester som søker å understøtte egen stats politiske og strategiske mål. Disse aktørene, ofte omtalt som Advanced Persistent Threat (APT), er ansett som de mest sofistikerte globalt og har vesentlige evner til å gjennomføre operasjoner i det digitale domenet. Et vesentlig poeng når det gjelder statlige aktører er at utvikling i den geopolitiske situasjonen vil påvirke staters informasjonsbehov og mål, og det har blitt observert økt etterretningsaktivitet når den geopolitiske spenningen har økt [2].

Fokuset i dette kapitlet er å vurdere de statlige aktørenes evne og vilje til å gjennomføre operasjoner innen spionasje, destruktive angrep og påvirkningsoperasjoner. Fellesnevneren er at det er mer kostnadseffektivt å gjennomføre denne aktiviteten i det digitale domenet, og nettverksoperasjoner utgjør derfor et viktig virkemiddel for statlige aktører [1]. De statlige aktørene vil benytte alle tilgjengelige digitale verktøy og metoder for å løse sine oppdrag, og vil på den måten dekke angrepsvektorene beskrevet i denne rapporten. Dette inkluderer blant annet alt fra enkle metoder, som phishing, til mer avansert utnyttelse av sårbarheter, og videre til svært avanserte leverandørkjedeangrep [10].

Spionasjeoperasjoner i cyberdomenet er angrep der aktøren søker ikke-legitim tilgang til sensitiv eller gradert informasjon eller intellektuell eiendom. Dette for å oppnå økonomisk vinning, konkurransefortrinn, eller av politiske grunner [64].

Destruktive angrep er i denne konteksten definert som digitale angrep med hensikt å ødelegge eller forandre informasjon, data eller programvare slik at de ikke kan benyttes uten vesentlig gjenoppretting [29].

Påvirkningsoperasjoner har en annen karakter enn de to foregående typene av operasjoner. Her handler det om å påvirke menneskers holdning, mening eller innstilling til myndigheter, nasjonale medier eller andre relevante problemstillinger. Slik aktivitet kan for eksempel oppnås gjennom informasjonskampanjer, falske nyheter eller generell misvisende informasjon [1].

De statlige aktørene som er beskrevet i denne rapporten samsvarer med aktørene de nasjonale sikkerhets- og etterretningstjenestene har beskrevet og vurdert i sine årlige trussel- og risikovurderinger for 2023. Aktørene er Russland, Kina, Iran og Nord-Korea [1], [2].

SPIONASJE

Generell Vilje

Statlige aktører som benytter nettverks-operasjoner gjennomfører dette i hovedsak med spionasje- og etterretning som formål [1], [10].

Person- og helseopplysninger har historisk sett vært attraktive mål globalt [42], og kan være interessant for statlige aktører fordi det kan brukes som et virkemiddel innenfor spionasje. Opplysningene kan for eksempel benyttes for å presse personer med betydelig myndighet eller høyt rettighets-nivå i IKT-systemene [3], [42].

Forskningsdata er også interessant for statlige aktører, og flere stater søker aktivt etter informasjon som kan bidra til at egen industri tar teknologiske steg raskere [2]. Norske universiteter og forskningsinstitu-sjoner vil ifølge PST bli forsøkt utnyttet for ulovlig kunnskapsoverføring, og Russland, Kina og Iran vil representere en særskilt utfordring [1].

Illustrasjonsfoto: Sykehuspartner

Generell Evne

De statlige aktørene beskrevet i denne rapporten, og da spesielt Kina og Russland, behersker alle angreps-vektorene beskrevet i figur 2, angrepsvektorer [65], [10], [24]. Selv om aktørene er sofistikerte, benytter de ofte enkle verktøy, som phishing eller spear phishing, i sine angrep for å levere avansert skadevare. Grunnen til dette er at metodene er kostnadseffektive og at risikoen for vellykket attribusjon er lav [24].

En av metodene statlige aktører kan benytte er inn-sidere. Russland og Kina har lang erfaring med å bruke innsidere, og benytter seg av utpressing, bestikkelser, infiltrasjon og sosial manipulering for å skaffe seg innsidere dersom målet er attraktivt nok [3]. Personer med tilgang til sensitiv og gradert informasjon vil være prioriterte mål for utenlandsk etterretning [1].

Russland

Russland har de siste årene vært en svært aktiv og vedvarende etterretningstrussel mot Norge [2]. Vårt medlemskap i NATO, tette samarbeid med USA og strategiske plassering med grense til Russland er blant årsakene [2]. I tillegg er også nordområdene av strategisk betydning for Russland. Russlands informasjonsbehov handler om tilgang til informasjon som styrker egen situasjonsforståelse i dagens sikkerhetspolitiske situasjon, og informasjon om teknologi, forskning, våre evner til å håndtere kriser og hvordan vi vil håndtere en eventuell tilspisset situasjon [1] .

Vilje

Russlands vilje til å gjennomføre digitale spionasjeoperasjoner er vedvarende høy mot norske mål, men flere kilder peker på at hovedaktiviteten fra russiske aktører har vært rettet mot Ukraina, som en del av Russlands hybride krigføring [2], [24], [10]. Denne krigføringen inkluderer også spionasje og eksfiltrering av sensitiv informasjon fra informasjonssystemer [10]. På utsiden av Ukraina har det blitt observert nettverksoperasjoner mot et hundretalls organisasjoner i over 40 land, inkludert Norge, der russiske aktører mistenkes å stå bak. Disse nettverksoperasjonene inkluderer spionasje, angrep utført av hacktivister og destruktive angrep [24].

Både sivile og militære etterretnings- og sikkerhetstjenester i Russland har informasjonsbehov knyttet til Norge. PST vurderer at Russland kommer til å være den største etterretningstrusselen mot Norge i 2023 og at Russland vil intensivere sin bruk at nettverksoperasjoner for etterretning og påvirkning. Dette grunnet vestens politiske og økonomiske sanksjoner, som blant annet har ført til utvisning av russiske diplomater i Norge og Europa, og dermed fjernet deler av Russlands evne til spionasje ved bruk av agenter under diplomatisk dekke [2], [1].

PST viser til at Russland har en interesse for å hente inn informasjon om totalforsvaret og det totale beredskapsapparatet [1], som spesalisthelsetjenesten er en del av. I tillegg vil også generell tilgang til kritisk infrastruktur være et verdifullt mål for russisk etterretning, siden denne tilgangen kan benyttes til spionasjeformål eller til forberedelse av destruktive angrep i en tilspisset situasjon [32]. Helsesektorens store mengder person- og helseopplysninger, egen forskning og samarbeid med forskningsmiljøer utenfor spesialisthelsetjenesten kan medføre at man er et mål for russisk etterretning [2], [29].

Evne

Russiske aktører har i lang tid vært ansett som en av de mest kapable trusselaktørene i det digitale trusselbildet [1], [32], [24]. I tillegg til kapasiteter innenfor cyberdomenet vil disse aktørene også kunne benytte andre metoder for informasjonsinnhenting for å nå sine mål. Aktørene har over tid vist at de evner å benytte et større antall metoder for å fullføre sine oppdrag. Disse metodene inkluderer blant annet phishing med og uten skadevare, verdikjedeangrep, utnyttelse av eksponerte sårbarheter og bruk av stjålne påloggingsopplysninger [24], [65]. Aktørene benytter ofte kjente verktøy for å utføre sine oppdrag, men har også evne til å utvikle egne verktøy for angrep [10], [24].

Som en følge av det endrede politiske klimaet og økt årvåkenhet i Norges befolkning forventes det at Russland vil øke bruken av fordekt innhenting, blant annet ved bruk av innsidere. Dette kan øke presset mot borgere i Norge med russisk bakgrunn eller borgere med knytninger til Russland [1].

Faktaboks om koblinger mellom statlige aktører, organiserte kriminelle aktører og hacktivister

Flere rapporter viser til at det er sterke indikasjoner på at statlige aktører har benyttet seg av organiserte kriminelle aktører og hacktivister for å nå sine mål [10], [7], [11], [1]. Det vises til eksempler hvor dette samarbeidet fremstår tydelig, mens i andre tilfeller kan det være mindre tydelig som for eksempel at timingen av et angrep stemmer overraskende bra med intensjonene til statlige aktører. Både hacktivister og organiserte kriminelle aktører kan benyttes i påvirkningsoperasjoner eller angrep med destruktive formål. Eventuelt kan de også benyttes for å dekke over en spionasjeoperasjon, ved for eksempel at de kommer inn mot slutten av operasjonen for å kjøre et digitalt utpressingsangrep for å lede oppmerksomheten bort fra det faktiske målet [10], [7], [11].

Enkelte aktører, som Russland og Kina, har over tid hatt policy om å utøve gråsoneaggresjon i cyberdomenet. Slike operasjoner ligger helt i ytterpunktet av den såkalte gråsonen; det vil si cyberoperasjoner som er helt opp til grensen for hva som er brudd på internasjonale konvensjoner og hva som kan utløse NATOs artikkel 5 [66]. I slike operasjoner kan både hacktivister og organiserte kriminelle aktører benyttes som verktøy. Statlige aktører vil da kunne oppnå sine mål uten at det direkte kan spores tilbake til dem.

Kina

Kina er ansett som en av de største aktørene innen spionasje i cyberdomenet. Målet med Kinas spionasjeaktiviteter er både politiske og økonomiske, med intensjoner om å øke landets teknologiske og økonomiske styrke [24]. Kinesiske myndigheter benytter nettverksoperasjoner i utstrakt grad og retter seg spesielt mot myndighetsnettverk, forsvar, forsvarsindustri, romforskning, helsesektoren, telekom og media [53]. Videre har kinesiske aktører vist interesse for informasjon av betydning for krigen i Ukraina og vestens respons [2].

Kina jobber aktivt med å posisjonere seg langsiktig i nordområdene, blant annet for å sikre fremtidig ressursutvinning. Norges overtakelse av formannskapet i Arktisk råd i mars 2023 kan gi økt kinesisk oppmerksomhet siden strategier og prosesser knyttet til nordområdene er blant de mest utsatte etterretningsmålene i norsk politikk. Kinas langsiktige mål om økt tilstedeværelse i nordområdene kan medføre økt etterretningsaktivitet [1], [2].

Vilje

Kina har i stor grad fokusert sin innsats mot organisasjoner i Asia i 2022, men de har likevel rettet en betydelig andel av sin nettverksoperasjoner mot organisasjoner i Norden, Europa og USA [67], [10]. Kinesiske nettverksoperasjoner er en vedvarende trussel mot myndigheter, forskningsinstitusjoner og virksomheter som er ledende innen fremvoksende teknologier [1].

Evne

Kina har betydelige kapasiteter og evner til å gjennomføre spionasjeoperasjoner og til å skaffe seg full og vedvarende tilgang til informasjon og infrastruktur [32], [67]. De vil derfor utgjøre en betydelig etterretningstrussel mot norske interesser [1].

Ifølge Kinas etterretningslov plikter enhver kinesisk borger, virksomhet og organisasjon å bistå Kinas etterretningstjeneste ved behov [68]. Dette medfører at statens evner til å gjennomføre spionasjeoperasjoner øker, både fordi innsideren kan gi informasjonen direkte og fordi innsideren kan bidra til å forenkle et digitalt angrep.
I senere tid har kinesiske aktører i mindre grad benyttet seg av tradisjonelle metoder som krever sosial manipulering, som phishing og innhenting av påloggingsopplysninger, og i større grad søkt å utnytte sårbarheter i internetteksponerte tjenester for å etablere fotfeste [10], [53].

De siste årene har det blitt observert at flere av de kinesiske aktørene benytter tilpassede verktøy som er like, som kan indikere at det kan være samarbeid mellom gruppene eller at utvikling og distribusjon av verktøy er sentralisert [69], [53]. Utvikling av verktøy for utnyttelse av sårbarheter krever høy kompetanse og god tilgang til ressurser. Dette gjelder særlig når aktørene søker å utnytte sårbarheter som ikke er allment kjent, såkalte nulldagssårbarheter [70].

Iran

Iran fokuserer i hovedsak på spionasje-kampanjer mot sine regionale naboer, men har de siste årene også gjennomført operasjoner mot europeiske land og USA [10], [32].

Vilje

I Norge har Iran i hovedsak søkt ikke-legitim tilgang til forskning [1], men har også gjennomført ondsinnet aktivitet mot norskiranere gjennom hacking av mobiltelefoner og datamaskiner [71].

Iran er blant aktørene som utfører nettverksoperasjoner i Norge, og PST forventer at Iran vil forsøke å ramme norske mål i 2023 [1]. Danske CFCS vurderer at Iran har kapasitet til å gjennomføre spionasjeoperasjoner, men at det er sannsynlig at Iran ikke har en generell vilje til å ramme danske mål [32].

Evne

Iran har betydelige evner til å gjennomføre spionasjeoperasjoner. De seneste årene har Iran styrket sine kapabiliteter for å gjennomføre operasjoner i det digitale domenet gjennom økt samarbeid med private kontraktører og tekniske universiteter [72].

Iranske aktører benytter ofte sosial manipulering, og utnyttelse av sårbarheter som metoder for å tilegne seg informasjon direkte eller som verktøy for å etablere fotfeste [72].

Nord-Korea

Nord-Korea sine prioriteringer i cyberdomenet reflekterer statens globale prioriteringer; bygge defensiv forsvarskapasitet, styrke landets svake økonomi og understøtte intern stabilitet på nøkkelområder [24].

Vilje

Nord-Korea trekkes frem av PST som en av aktørene man forventer vil utføre nettverksoperasjoner mot norske mål i 2023 [1]. Nord-Korea benytter ofte nettverksoperasjoner til andre formål enn spionasje. Nord-Korea har likevel de siste årene gjennomført spionasjeoperasjoner for å tilegne seg kunnskap rundt covid-vaksiner, men har det siste året gått tilbake til å gjennomføre industrispionasje, og velge ut regionale mål som er i tråd med landets strategiske interesser [73].

Evne

Nord-Korea har kapasitet og evne til å gjennomføre spionasjeoperasjoner og har gjennomført flere vellykkede angrep globalt [73], [24]. Nord-Korea benytter en rekke ulike verktøy og metoder i sine angrep, og er ansett som en avansert aktør i det digitale domenet [73].

Verktøyene Nord-Korea benytter i sine angrep er både offentlig kjente verktøy og skadevarer, men også egenutviklede skadevarer for å understøtte sine angrep. Nord-Korea utnytter også sårbarheter i internetteksponerte tjenester i sine angrep for å etablere fotfeste, og det har i tillegg blitt observert kampanjer hvor målsetningen er å få tilgang til påloggingsopplysninger for å benytte disse i senere angrep [73].

I tillegg til phishing har Nord-Korea også brukt sosiale medier for nettverksbygging, som LinkedIn, for å spre dokumenter eller linker til nettsteder med skadevare [24]. Nord-Korea søker også å få tilgang til informasjon av statens interesse gjennom å få eget personell ansatt i aktuelle virksomheter [73].

VURDERING SPIONASJE

Statlige aktører - Spionasje - Overordnet vurdering mot spesialisthelsetjenesten:			
Land	Vilje	Evne	Skadepotensiale
Russland	Høy	Meget Høy	Høyt
Kina	Høy	Meget Høy	Høyt
Iran	Lav	Høy*	Høyt
Nord-Korea	Meget Lav	Høy	Høyt

Vilje

Det vurderes som **meget sannsynlig** at Russland og Kina er de statlige aktørene med størst vilje til å utøve spionasje mot spesialisthelsetjenestens verdier, men at de har ulike målsetninger for å gjennomføre angrepene.

Russlands fokus vil dreie seg om tilgang til informasjon som styrker deres situasjonsforståelse generelt, men også rundt forholdet til NATO-landene. Det vurderes som **sannsynlig** at Russland har vilje til å utøve spionasje mot spesialisthelsetjenestens verdier som omfatter beredskap og krisehåndteringsevne. Kinas fokus er rettet mot industrispionasje og 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.

Samlet vurderes det som **meget sannsynlig** at fremmede staters sikkerhets- og etterretningstjenester har vilje til å drive spionasje mot spesialisthelsetjenestens forskningsmiljøer. Det vurderes videre som **sannsynlig** at statlige aktører vil forsøke å tilegne seg helseopplysninger fra regionene i kartleggings- og etterretningsøyemed, i den forbindelse vurderes også store mengder personopplysninger som et **mulig** mål for statlige aktører.

På bakgrunn av fremmede staters motivasjon knyttet til innflytelse i nordområdene, teknologi og økonomi, vurderes det som **mulig** at disse aktørene har interesse av økonomiske og finansielle verdier som blant annet innebærer strategiske investeringer, anskaffelser, avtaler og kontrakter.

Det vurderes som **mulig** at statlige aktører har en generell interesse for informasjon og informasjonssystemer i regionene. Dette innebærer også sikkerhetsrelaterte verdier, som for eksempel informasjon om sårbarheter som kan utnyttes for å få tilgang til IKT-systemene.

Det vurderes som **sannsynlig** at Russlands generelle vilje til spionasje vil påvirkes av utviklingen i krigen i Ukraina, der økt spenningsnivå og mindre samarbeid vil øke behovet for etterretning. På bakgrunn av dette vurderes det som **sannsynlig** at Russlands risikovillighet for å gjennomføre spionasje vil øke og det er **mulig** at sannsynligheten for spionasje mot spesialisthelsetjenesten også vil øke.

Evne

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

Det vurderes som **meget sannsynlig** at fremmede stater bruker kontraktører for å utføre deler av, eller fullverdige digitale operasjoner.

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

Dersom statlige aktører er villige til å benytte seg av innsidere mot spesialisthelsetjenestens verdier vil personell som er knyttet direkte til forskningsmiljøene **meget sannsynlig** være de mest attraktive målene. I tillegg vurderes det også som **sannsynlig** at personellgrupper med stor tilgang til informasjon, høye rettigheter i IKT-systemer, betydelig myndighet eller personer med god kjennskap til sårbarheter vil være utsatte mål.

Vurdering av hvilke angrepsvektorer statlige aktører vil benytte seg av for å oppnå initiell tilgang til spesialisthelsetjenestens systemer.

Vurdering	Angrepsvektor for initiell tilgang
Meget sannsynlig	Utnyttelse av sårbarheter i internett-eksponerte tjenester og servere
Meget sannsynlig	Utnyttelse av fjerntilgang
Meget sannsynlig	Phising og spear phising
Mulig	Leverandørkjedeangrep (ikke målrettet)
Lite sannsynlig	Innsidere
Lite sannsynlig	Eksternt medie
Meget lite sannsynlig	Leverandørkjedeangrep (målrettet)

DESTRUKTIVE ANGREP

Statsaktørene som gjennomfører destruktive angrep antas i denne rapporten å ha tilsvarende kapasitet som aktørene som gjennomfører spionasjeoperasjoner. Grunnen til denne antakelsen er at vi ikke har god nok innsikt til å skille de ulike interne gruppene hos aktørene fra hverandre i tilstrekkelig grad. Angrepsvektorer vil derfor ikke bli beskrevet eksplisitt i dette kapittelet, men vil bli beskrevet under avsnittet evne ved behov.

Illustrasjonsfoto: Sykehuspartner

Russland

Russland har siden 2007 benyttet destruktive digitale angrep som et virkemiddel i sin hybride krigføring, og spesielt rettet mot Ukraina i forbindelse med annekteringen av Krim-halvøya i 2014 og senest i forbindelse med krigen i Ukraina . Russland gjennomførte digitale angrep mot kritisk infrastruktur i Ukraina med såkalte wiper-skadevarer, som er en type skadevare ment for ødeleggelse og destruktive angrep. Hensikten med disse angrepene var varig skade eller bortfall av tilgjengelighet for å støtte den militære operasjonen på bakken. Disse angrepene var rettet mot kraftproduksjon, telekommunikasjon og annen kritisk infrastruktur [74], [24], [16].

Vilje

Russiske aktørers vilje til å gjennomføre destruktive angrep ser ut til å være sentrert mot krigen i Ukraina [75], og det ble observert minst 40 destruktive digitale angrep mot ukrainske mål i de første månedene av krigen [2]. Viljen til å angripe norske mål med destruktive angrep har av PST blitt vurdert til å være lite sannsynlig. Dette gjelder både i det fysiske og i det digitale domenet . Utvikling i den sikkerhetspolitiske situasjonen kan påvirke denne viljen [1]. Destruktive digitale angrep mot NATOs medlemsland kan i ytterste konsekvens utløse NATOs artikkel 5 og dermed bli ansett som angrep på forsvarsalliansen [76].

Helsesektoren er gitt et særlig rettslig vern i Genèvekonvensjonen og en operasjon i det digitale domenet kan, avhengig av omfang og konsekvens, være i strid med FN-paktens artikkel 2 (4) [77] . Dette vernet er ikke en garanti mot digitale angrep utført av statlige aktører, men kan alene eller i kombinasjon med NATOs artikkel 5, være begrensende faktorer for Russlands og andre stater vilje til å gjennomføre destruktive digitale angrep mot norsk spesialisthelsetjeneste.

Evne

Russland har, i likhet med spionasjeroperasjoner, meget høy evne til å gjennomføre destruktive operasjoner og har over tid praktisert slike angrep [32]. Rapporter peker også på russiske statlige aktørers knytning til enkelte hacktivistgrupper og organiserte kriminelle aktører [7], [10], [11]. Slike koblinger kan potensielt benyttes i destruktive operasjoner, og er allerede forklart nærmere i faktaboks under spionasje på side 31 [10].

Kina

Kina har i senere tid, ifølge denne rapportens kildegrunnlag, ikke benyttet destruktive digitale angrep som et virkemiddel i sine nettverksoperasjoner.

Vilje

Kina har de siste årene ikke vist vilje til å benytte destruktive digitale angrep som et verktøy for å understøtte egne mål i det digitale domenet, men det kan ikke utelukkes at Kina har gjennomført operasjoner for å skaffe seg tilgang til infrastruktur med hensikt om å kunne utnytte denne til destruktive angrep senere [20], [24].

Evne

En viktig del av Kinas militære cyberstrategi er å kunne gjennomføre destruktive digitale angrep mot fiendens datasystemer og annen kommunikasjon [78]. Som nevnt i kapittelet for spionasje finnes det indikasjoner på at utviklingen av verktøy i Kina er sentralt styrt [53], [69], og det er rimelig å anta at denne utviklingen også gjelder for destruktive verktøy.

Iran

Iran fokuserer sine destruktive angrep mot land i samme region, men har også gjennomført angrep mot USA og mot land i Europa [72].

Vilje

Irans vilje til å gjennomføre destruktive angrep har historisk sett vært rettet mot land i egen region, men har de siste årene også vist vilje til å angripe land i Europa og USA [80]. Iranske aktører har aktivt gjennomført slike angrep i mange år, blant annet mot Saudi Arabia og Israel [69]. 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

Eksempel

Sommeren 2022 gjennomførte Iran destruktive digitale angrep mot myndighetene i Albania. Angrepene har blitt satt i sammenheng med digitale destruktive angrep gjennomført mot iranske TV og radiostasjoner, som man mistenker ble gjennomført av regimemotstandere med base i Albania. Iran gjennomførte angrepene mot albanske myndigheter i forkant av en konferanse planlagt av en organisasjon som jobber mot det iranske regimet. Selv om konferansen ble avlyst, fortsatte iranske aktører å gjennomføre destruktive angrep mot albanske myndigheter [79]. Disse angrepene resulterte ikke i at Albania utløste NATOs artikkel 5.

Evne

Iran har, i likhet med spionasjeoperasjoner, betydelig evne til å gjennomføre destruktive operasjoner. I tillegg til å benytte lignende vektorer som ved spionasje, benytter iranske aktører også andre verktøy for å gjennomføre destruktive og disruptive angrep. Iran benytter skadevare brukt for utpressing i såkalte «Lock and leak» angrep [10] og mye tyder på at aktørene benytter seg av etablerte RaaS-plattformer fremfor å utvikle verktøy selv [72]. «Lock and leak» angrep er en samlebetegnelse for utpressingsangrep hvor man både krypterer systemer og henter ut og lekker sensitiv informasjon. Iranske aktører har hatt som målsetning å utilgjengeliggjøre systemer og lekke ofrenes data gjennom disse angrepene, ikke økonomisk vinning [69].

Nord-Korea

Den største forskjellen fra Russland, Kina og Iran, er at en av prioriteringene til statlige aktører i Nord-Korea i stor grad er økonomisk vinning. Som eksempel har Nord-koreanske aktører både gjennomført målrettet angrep mot selskaper innenfor kryptovaluta, og benyttet ransomware-verktøy for å styrke egen økonomi. For Nord-Korea er dette en milliardindustri [24], [73]. Angrep hvor formålet er økonomisk vinning som får destruktive konsekvenser faller ikke inn under definisjonen vi har brukt for destruktive angrep. Denne delen av Nord-Koreas aktivitet faller ikke inn under dette delkapitlet, men er godt dekket av kapitlet om organiserte kriminelle aktører.

Vilje

Nord-Korea har benyttet destruktive angrep som en del av sine påvirkningsoperasjoner. Et av de mest omtalte av disse angrepene ble gjennomført i forbindelse med Sony Pictures' komedie «The Interview» høsten 2014. Angriperne stjal og lekket store mengder data, firmaets infrastruktur ble utilgjengeliggjorte ved hjelp av wiper-skadevare og det ble framsatt trusler om digitale angrep mot kinoer som skulle vise filmen. Sony valgte å kansellere kinovisninger av filmen [81], [82]. Selv om hendelsen begynner å bli gammel viser den en vilje fra Nord-Korea til å benytte alle tilgjengelige verktøy for å oppnå egne målsetninger.

Evne

Nord-Korea har betydelig kapasitet og evne til å gjennomføre destruktive angrep. Nord-Korea benytter en rekke verktøy og metoder for å gjennomføre sine oppdrag, både kjente tilgjengelige verktøy, men også avanserte selvutviklede verktøy [73], [24].

VURDERING DESTRUKTIVE ANGREP

Statlige aktører - Destruktive angrep - Overordnet vurdering mot 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

Det vurderes som **meget sannsynlig** at statlige aktører har betydelig kapasitet til å kunne gjennomføre destruktive digitale angrep mot spesialisthelsetjenestens IKT-systemer. Det er derfor ekstra viktig å følge med på endring i vilje til å gjennomføre destruktive digitale angrep.

Det vurderes som **lite sannsynlig** at Russland har vilje til å gjennomføre destruktive angrep mot spesialisthelsetjenesten. Denne viljen kan påvirkes av utviklingen i Ukrainakrigen.

Et destruktivt angrep vil kunne medføre **meget høyt** skadepotensiale for spesialisthelsetjenesten.

Det vurderes som **meget lite sannsynlig** at Kina, Iran og Nord-Korea har vilje til å gjennomføre destruktive angrep mot spesialisthelsetjenesten.

Det vurderes som **sannsynlig** at et eventuelt krypteringsangrep fra Nord-Korea vil ha økonomisk vinning som målsetning og derfor ikke vil bli klassifisert som et destruktivt angrep.

Det vurderes som **lite sannsynlig** at leverandører, samarbeidspartnere eller andre avhengigheter kan rammes av et destruktivt angrep. Et slikt angrep kan eventuelt medføre konsekvenser for spesialisthelsetjenestens verdier.

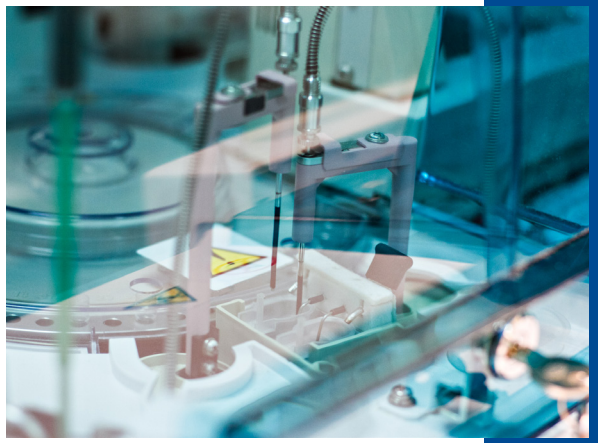
Det vurderes som **sannsynlig** at dersom spesialisthelsetjenesten blir utsatt for et destruktivt angrep av en statlig aktør, vil dette være utført som gråsoneaggresjon. I den forbindelse vurderes det som **mulig** at hacktivister eller organiserte kriminelle aktører vil benyttes som verktøy for at angrepet ikke skal kobles til statlige aktører og derav også vanskeliggjøre respons fra myndighetene.

Illustrasjonsfoto: Sykehuspartner

PÅVIRKNINGSOPERASJONER

I motsetning til foregående kapitler vil ikke denne rapporten beskrive egne vurderinger om andre staters vilje og evne til å påvirke spesialisthelsetjenesten. En av grunnene til dette er at påvirkningsoperasjoner ikke har som målsetning å påvirke vår digitale infrastruktur, men å påvirke mennesker og samfunn. Norge har fagmiljøer i NSM, PST og ETJ som er naturlige analysemiljøer for å vurdere denne typen angrep. Spesialisthelsetjenesten forholder seg til disse etatenes vurderinger om dette temaet. I dette kapittelet beskrives de to største aktørene, Russland og Kina, som de nasjonale fagmiljøene trekker frem i sine rapporter.

Spesialisthelsetjenesten er en betydelig sektor i staten og det er derfor viktig at påvirkningsoperasjoner også belyses i denne rapporten. Påvirkningsoperasjoner kan rettes mot sektoren som helhet, men også mot enkeltindivider. Det er derfor viktig å spre kunnskap om temaet og dermed bidra til å forebygge mot slike operasjoner.



Illustrasjonsfoto: Sykehuspartner

Russland

Russland har i mange år vist vilje og evne til å gjennomføre påvirkningsoperasjoner i vestlige land. I 2022 har Russland gjennomført påvirkningsoperasjoner primært med formål om å påvirke vestens oppfatning av krigen i Ukraina [75]. Det forventes at denne aktiviteten vedvarer og at Russland vil forsøke å påvirke norske beslutningstakere og befolkningen i Norge i saker som har stor betydning for Russland. Dette kan være å splitte vestlig samhold om støtte til Ukraina eller økonomiske sanksjoner [1], [2].

Vilje

Påvirkningsoperasjoner er en integrert del av Russlands doktrine for informasjonskrigføring. Dette inkluderer blant annet bruk av nyhetsbyråer for å spre desinformasjon, spre desinformasjon til utvalgte målgrupper, eller å teppebombe medier med ulike teorier, halvsannheter og usannheter for å skape tvil om sannhet eller svekke tillit til myndigheter [2]. Det siste året har Russland gjennomført påvirkningsoperasjoner med høy frekvens av moderat størrelse og har rettet denne aktiviteten mot Ukraina, NATO-land og andre land som gir støtte til Ukraina [75]. PST påpeker at fremmede etterretningstjenester, inkludert Russland, vil forsøke å påvirke beslutningstakere og den norske befolkningen i 2023 [1]. I Norge er spørsmål knyttet til forsvars- og sikkerhetspolitikk spesielt utsatt for russisk påvirkningsaktivitet [2], og PST påpeker at fremmede etterretningsoffiserer vil arbeide målrettet for å påvirke utfallet av enkeltsaker gjennom påvirkning av personer som har politisk innflytelse [1]. Russiske myndigheter har historisk sett ikke vist vilje til å gjennomføre påvirkningsoperasjoner mot spesialisthelsetjenesten, men utviklingen av krigen i Ukraina, og vår involvering, kan påvirke dette.

Evne

Russland har betydelige evner til å gjennomføre påvirkningsoperasjoner med egne ressurser men kan i tillegg til å benytte nyhetsbyråer, også benytte hacktivister, eller utgi seg for å være hacktivister, for å spre desinformasjon [32], [10]. Som en konsekvens av krigen i Ukraina vurderer ETJ at Russlands evne til å påvirke vesten som sterkt svekket [2].

Kina

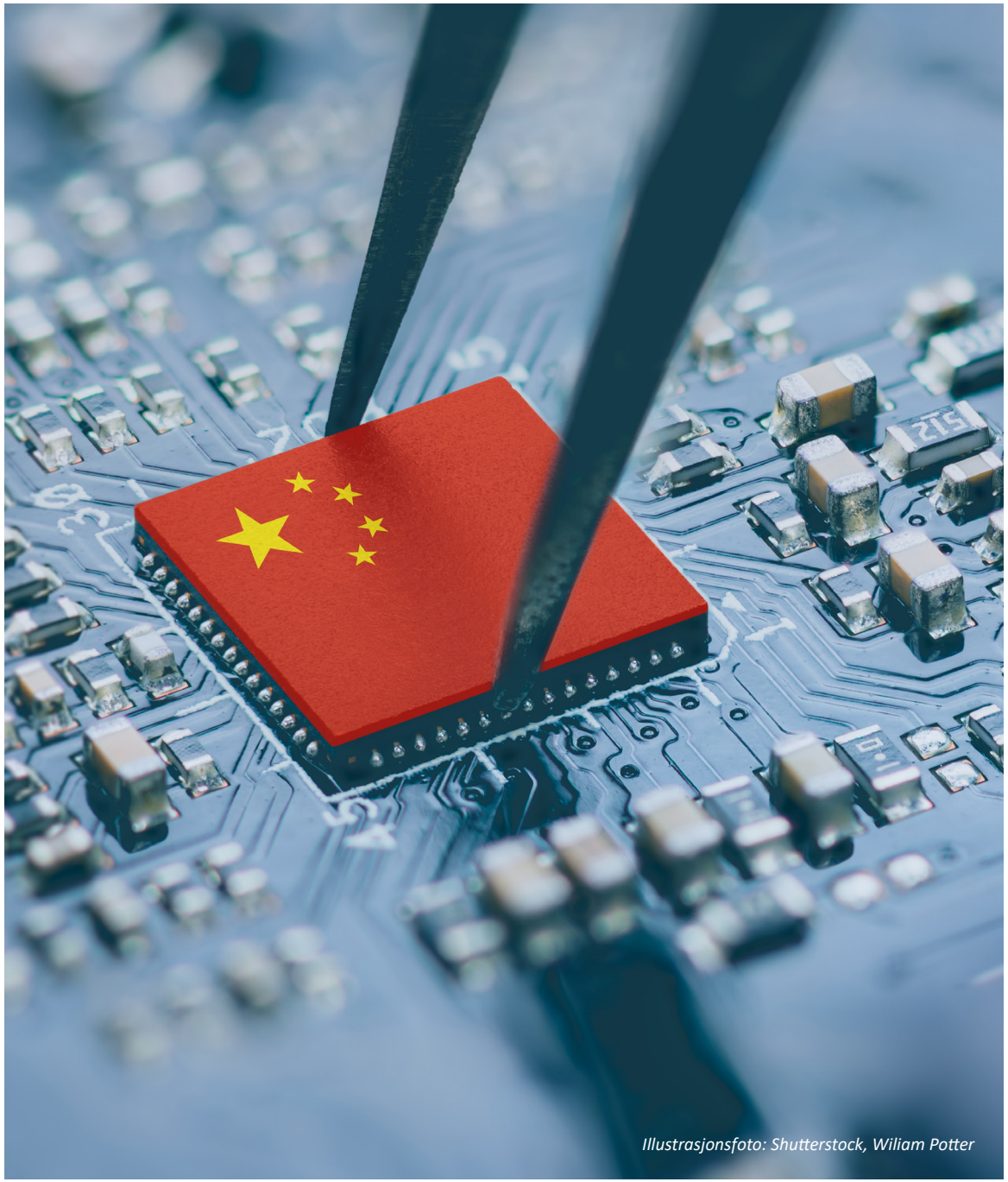
Kina har de siste årene gjennomført påvirkningsoperasjoner mot flere europeiske land. I 2022 har påvirkningsoperasjonene i stor grad omhandlet narrativ om Taiwan, men Kina har også gjennomført operasjoner for å påvirke narrativet rundt sabotasjen av gasslinjene fra Russland til Europa [70].

Vilje

Kina har vært svært aktive for å forsterke pro-kinesiske holdninger globalt og har gjennomført operasjoner med høy frekvens, men med begrenset effekt. De har også forsøkt å påvirke enkeltsaker som sabotasjen av gasslinjene til Europa fra Russland [70]. Flere land i Europa har de siste årene blitt utsatt for press og trusler fra Kina med formål å endre eller påvirke disse landenes beslutninger [1]. Det forventes at kinesiske myndigheter vil forsøke å påvirke norske beslutningstakere og Norges befolkning, og utøve press mot personer som åpent kritiserer Kinas kjerneinteresser [1].

Evne

Kina har betydelige evner til å gjennomføre påvirkningsoperasjoner [70].



Illustrasjonsfoto: Shutterstock, Wiliam Potter

03.

DEL 3

Hacktivister

Vilje | Evne | Vurdering

Illustrasjonsfoto: Shutterstock

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 hacktivistoperasjonen benytter tjenestenektangrep eller kompromittering av en hjemmeside for å vise sin støtte til en sak, slik som motstand mot politisk betente emner, koranbrenning eller pågående geopolitiske konflikter [15].

Hacktivistlandskapet endret seg drastisk i tiden etter Russlands invasjon av Ukraina 24. februar 2022. Store grupper som spesialiserer seg på tjenestenektangrep ble opprettet, og flere av disse opererer som en privat forlenget gren av statsapparatet og speiler statens internasjonale relasjoner [11], [83]. Gruppene som ble opprettet etter invasjonen kan deles inn i to kategorier, pro- og anti-Russland. I denne rapporten er det tatt et bevisst standpunkt om å ikke nevne spesifikke hacktivistgrupper med navn, for å ikke gi grupperingene unødvendig oppmerksomhet. Dette kapittelet vil diskutere den «nye» bølgen hacktivister som en generell kategori, med fokus på de pro-russiske gruppene.

Vilje

Det siste året har man observert angrep mot norsk helsesektor fra hacktivister med bakgrunn i Norges støtte til Ukraina [84]. Den norske helsesektoren har ikke vært et prioritert mål etter invasjonen, men ble angrepet direkte som en del av en større angrepskampanje rettet mot helsesektorene i flere NATO-land i januar 2023. Angrepene i denne kampanjen var rettet mot flere NATO-land som ga støtte til Ukraina, og utelukkende mot helserelatert infrastruktur. Til tross for at angrepene hadde liten til ingen effekt, ble de fremstilt som en suksess på PR-kanalene hacktivistgruppene administrerer.

Angrepene har også blitt omtalt av vestlige medier. Dette spiller rett inn i et mønster for gruppene - det er oppmerksomhet og PR som er det primære målet [85]. Norsk helsesektor har ikke opplevd angrep fra øvrige hacktivistgrupper det siste året [15].

De pro-russiske gruppene fungerer også som samlingspunkt for likesinnede, og gruppene publiserer nyheter, ber om donasjoner og sprer pro-russisk desinformasjon. Det blir dermed feil å se på disse gruppene som rene tjenestenekt-grupper, da de bidrar kraftig til å spre en konkret narrativ om konflikten til en stor gruppe tilhørere [11], [15], [86].

De norske etterretnings- og sikkerhetstjenestene har ikke fokusert på trusselen fra pro-russiske hacktivistgrupper i sine åpne rapporter, men danske CFCS oppgraderte i januar 2023 sin vurdering fra middel til høy som en direkte konsekvens av hacktivist-angrepet motivert av Danmarks støtte til Ukraina. De vurderer også at stor mediedekning kan bidra til økt oppmerksomhet og flere angrep fra slike grupper [85].

Under krigen i Ukraina har russiske statlige aktører utført en rekke cyberoperasjoner. Dette har pågått siden før invasjonen av Krim-halvøya i 2014. Operasjonene inkluderer destruktive angrep og datalekkasjer, og det er funnet klare koblinger mellom russiske statlige aktører og pro-russiske hacktivister. Dette samarbeidet er beskrevet i større detalj under statlige aktører, side 31 [83]. Uavhengig av denne koblingen har hacktivistgruppene en klar vilje til å angripe Norge og norsk kritisk infrastruktur, herunder helsesektoren [15].

Evne

Angrep utført av hacktivistgrupper mot helsesektoren i Norge og andre sammenlignbare land har vært lite sofistikerte og har i Norge hatt liten konsekvens. Gruppene opererer med lavere budsjetter enn andre aktører, som organiserte kriminelle og statlige aktører, og ber jevnlig følgerne sine om donasjoner [15].

I kontrast har enkelte grupper en stor evne til å organisere og gjennomføre angrep, og engasjerer en stor følgerskare som blir med på angrepene [15], [87].

Grovt sett kan metodene hacktivister bruker deles opp i fire kategorier:

- Tjenestenektangrep
- Kompromittering og manipulering av nettsider for å publisere et budskap
- Kompromittere og publisere sensitiv informasjon
- Politisk motivert digital utpressing

[16]

Pro-russiske hacktivistgrupper benytter seg i størst grad av tjenestenektangrep, da dette krever lav teknisk innsikt, men kan gi mye mediedekning og oppmerksomhet [15], [88].

Det er også tilfeller av kompromitteringer og datalekkasjer fra hacktivistgrupper motivert av konflikten i Ukraina. Disse forekommer langt sjeldnere enn tjenestenektangrep, og i noen tilfeller har man klare indikasjoner på at selve kompromitteringen ble gjort av en statlig aktør mens informasjonen ble publisert av en hacktivistgruppe [15], [11], [83].

VURDERING HACKTIVISTER

Hacktivister - Overordnet vurdering mot spesialisthelsetjenesten:		
Vilje	Evne	Skadepotensiale
Høy	Lav	Lavt

Den tradisjonelle hacktivisten vurderes til å ha **meget lav** vilje til å ramme spesialisthelsetjenesten, og er ikke vurdert ytterligere. Videre vurderinger retter seg mot den nye bølgen hacktivister, spesifikt pro-russiske hacktivister motivert av krigen i Ukraina.

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. Det vurderes som **sannsynlig** at leverandører og tjenester spesialisthelsetjenesten benytter kan bli utsatt for et tjenestenektangrep.

Vilje

Pro-russiske hacktivister vurderes til å ha **høy** vilje til å forsøke å ramme spesialisthelsetjenesten. Det vurderes som **sannsynlig** at spesialisthelsetjenesten vil bli direkte forsøkt rammet av et hacktivistangrep.

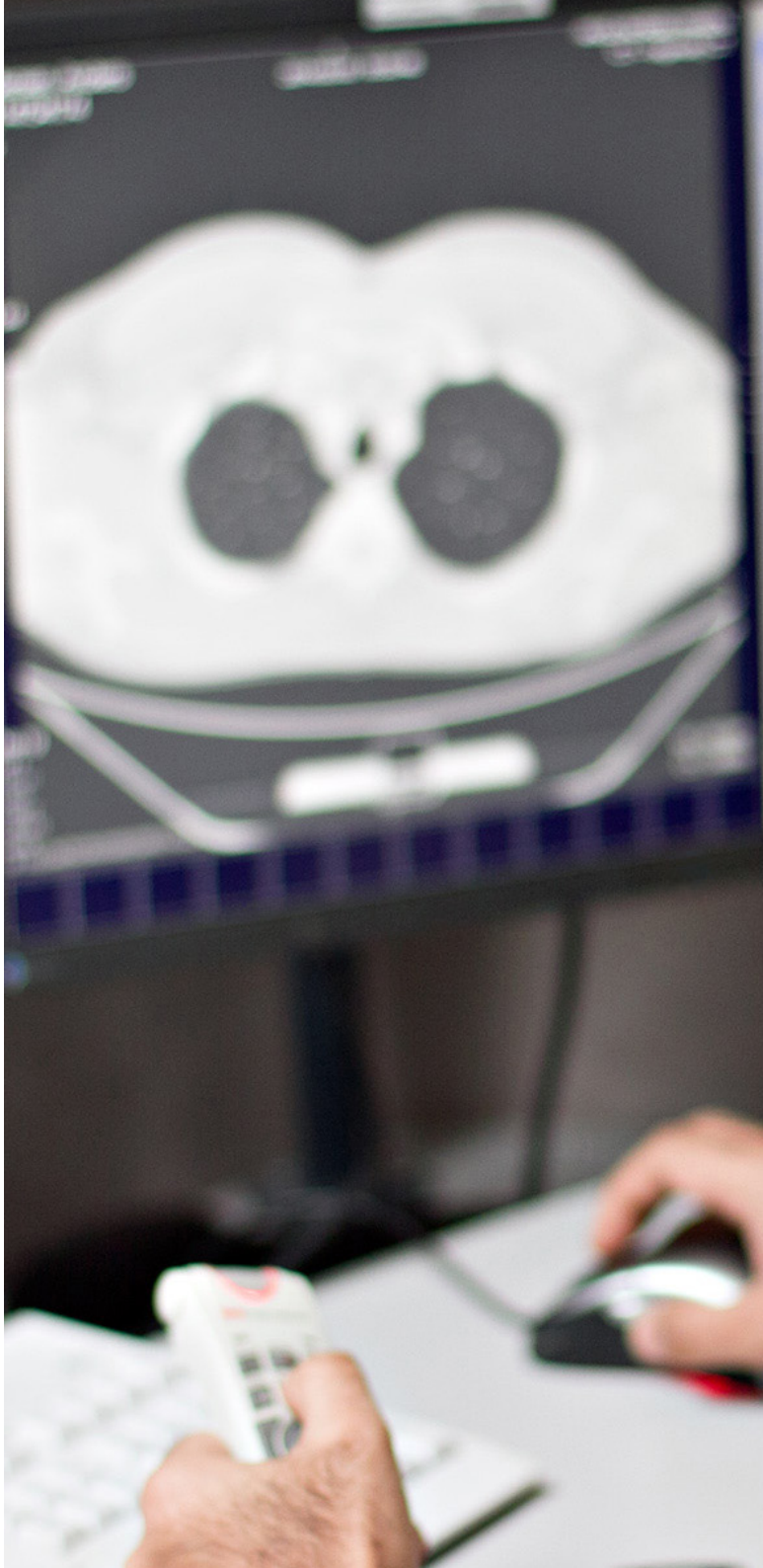
Det er viktig å være bevisst på at viljen til hacktivistgrupper kan endre seg raskt med bakgrunn i skiftende geopolitisk situasjonsbilde, betente mediesaker eller andre saker som kan fange hacktivisters oppmerksomhet. Vi ser en klar sammenheng mellom mediesaker og hvordan det fremprovoserer prioriterte mål. Felles for disse er at desto 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.

Evne

Evnenivået til hacktivister vurderes å være **lavt.**

Vi vurderer det som **sannsynlig** at tjenestenektangrep vil være hovedteknikken hacktivister benytter i tiden fremover.

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.



Illustrasjonsfoto: Sykehuspartner

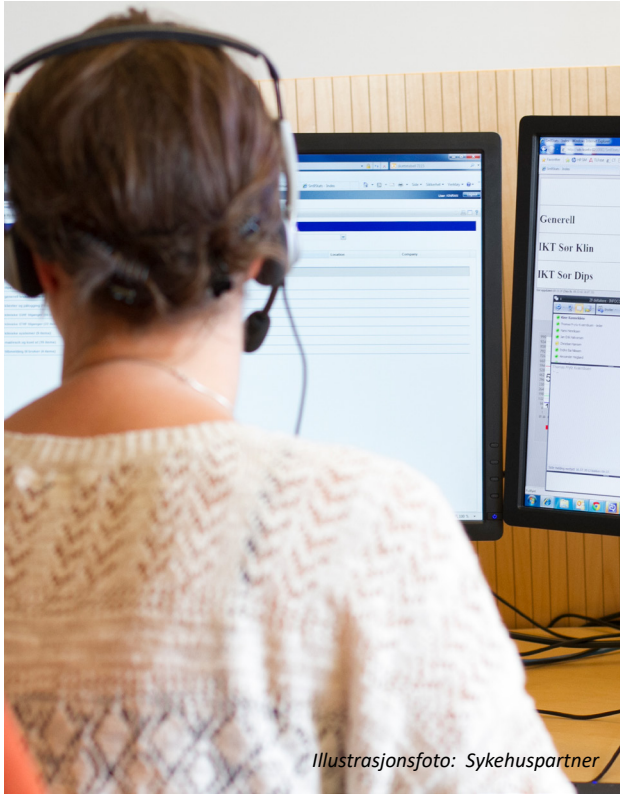
03. Selvmotiverte innsidere

Eksempel | Vurdering

DEL 4

Illustrasjonsfoto: Norsk Helsenett

SELVMOTIVERTE INNSIDERE



Illustrasjonsfoto: Sykehuspartner

En selvmotivert innsider har en egen motivasjon for å utføre innsidevirksomhet som potensielt kan påføre virksomheten skade. Motivasjonen til denne innsideren kan ha sitt opphav i følelser, idealisme eller egen vinning [89], [90].

- **Følelser:** Et eksempel på følelser kan være frustrasjon eller sinne som oppstår på bakgrunn av uenighet eller konflikt med arbeidsgiver. Denne typen motivasjon kan føre til alvorlige scenarioer siden formålet til innsideren kan være å påføre virksomheten skade [89], [90].
- **Idealisme:** Det finnes flere eksempler globalt hvor motivasjonen til en innsider har vært idealisme eller politisk standpunkt. I noen tilfeller av dette, har konsekvensen vært informasjonslekkasje [89], [90].
- **Egen vinning:** Egen vinning handler ofte om økonomi, men kan også være økte karrieremuligheter, oppnå status eller lignende. Motivasjonen for økonomisk vinning vil kunne oppstå på bakgrunn av tre faktorer:
  - Økonomisk press, eksempelvis at innsideren skylder penger.
  - Mulighetsbasert, innsideren ser at det er en mulighet for økonomisk vinning med liten risiko for å bli tatt.
  - Rasjonalisering, innsideren rettferdiggjør en kriminell handling, for eksempel kan en person mene hen er urettferdig kompensert og fortjener noe mer [89], [90], [91].

I 2021 rapporterte 8 % av et utvalg på 2 500 norske virksomheter at de har avdekket utro tjenere de siste to årene. Undersøkelsen viser at det er lite forskjeller mellom ulike bransjer og mellom det private og det offentlige [92]. Andre globale undersøkelser viser til at flere av innsidehendelsene som håndteres, involverer en misfornøyd ansatt som stjeler informasjon eller ødelegger data i forbindelse med oppsigelse [40].

Det er en fordel for innsidere at angrepet utføres fra innsiden av sikkerhetsbarrierer. I tillegg kan en innsider ha god kunnskap, eller lett tilegne seg kunnskap, om virksomhetens sårbarheter som for eksempel hvordan nettverket og sikkerhetsløsninger er satt opp. Gjennom bruk av legitime tilganger kan innsidere gjennomføre sine planer uten bruk av skadevare og dermed øke sine muligheter for å lykkes. Personell med administratorrettigheter kan være særlig skadelig som en bevisst innsider [89].

Eksempel

I mars 2020 ble en amerikansk virksomhet som drev med emballasje og forsendelse av medisinsk utstyr utsatt for en selvmotivert innsider. En tidligere ansatt som var permittert grunnet pandemien opprettet en falsk konto han kunne bruke til å få tilgang til virksomhetens database. Han benyttet kontoen til å endre informasjon om 115 000 forsendelser og slettet 2 300 bestillinger. Deretter slettet han kontoen slik at endringene ikke var reverserbare. Handlingen saboterte leveranse av kritisk utstyr til helsepersonell [93].

VURDERING SELVMOTIVERTE INNSIDERE

Vurdering

Hovedbekymringen med selvmotiverte innsidere er angrep der målet er å påføre virksomheten skade og det **meget høye** skadepotensialet en slik hendelse vil kunne ha. Vi vurderer det som **sannsynlig** at pasient-perspektivet fungerer som en moralsk barriere til vår fordel.

Vurdering av selvmotiverte innsidere skiller seg ut fra de andre trusselaktørene som er vurdert i denne rapporten. Det er forskjell på mulighetene personell i spesialisthelsetjenesten har til å kunne påføre virksomheten skade. I tillegg er viljen allerede gitt ved at aktøren er selvmotivert. Derfor har vi delt vurderingen inn i to ytterpunkter basert på evnenivå, som også gir skadepotensialet, og vurdert sannsynligheten for hver av disse fremfor viljen. Det presiseres at det finnes flere nyanser mellom disse ytterpunktene som er beskrevet i tabellen. Eksempler på nyanser er personer med høy fagkunnskap eller personell med stor tilgang til sensitiv informasjon, hvor skadepotensialet kan være høyere enn hos «folk flest», men lavere enn hos personell med administratorrettigheter eller lignende. Vår vurdering er at sannsynligheten reduseres gradvis med økt evnenivå og skadepotensiale.

Med mulighet til å påføre meget høy skade menes her personell med høyeste rettighetsnivå, teknisk kunnskap til å illegalt kunne skaffe seg høyeste rettighetsnivå, eller personell med annen kunnskap, myndighet eller fysisk adgang som gir de denne muligheten. Personell i denne kategorien utgjør en liten del av de ansatte i spesialisthelsetjenesten og for dette personellet er det også innført sikkerhetstiltak for å redusere sannsynligheten for hendelser med **meget høyt** skadepotensiale. Det vurderes **meget lite sannsynlig** at en av disse personene vil utføre et slikt angrep.

På den andre siden har vi vurdert personene med medium mulighet for å kunne påføre spesialisthelsetjenesten skade. Med det menes «folk flest» i spesialisthelsetjenesten, som betyr at dette innebærer langt flere personer enn i den førstnevnte gruppen.

I større virksomheter, som foretakene i spesialisthelsetjenesten, vil det alltid være ansatte som er misfornøyde, har sterke ideologier eller som ønsker å oppnå egen vinning. Det vurderes som **meget sannsynlig** at spesialisthelsetjenesten kan oppleve uønskede hendelser med medium skadepotensiale utført bevisst av egne ansatte. Vurderingen er basert på forskjellen i antall personer i de to kategoriene, og ikke ulik tillit til de to kategoriene av personell.

Det vurderes som **sannsynlig** at enklere tilgang til kriminelle verktøy og informasjon om hvordan man utfører angrep, og utvikling i kunstig intelligens, vil bidra til at flere personer kan oppnå **høyt** eller **meget høyt** skadepotensiale som selvmotiverte innsidere i tiden fremover.

Selvmotiverte innsidere - Overordnet vurdering mot spesialisthelsetjenesten:
(Viljenivået er gitt i begrepet selvmotiverte, derfor vurderer vi sannsynlighet i stedet for vilje)

Sannsynlighet	Evne	Skadepotensiale
Meget lite sannsynlig	Personell med evne og mulighet til å påføre spesialisthelsetjenesten meget høy skade	Meget høyt
Meget sannsynlig	Personell med evne og mulighet til å påføre spesialisthelsetjenesten medium skade	Medium

04. Trender

Skytjenester | Raskere utnyttelse av sårbarheter | Kunstig intelligens

Illustrasjonsfoto: Shutterstock

SKYTJENESTER

Skytjenester tas i økende grad i bruk av virksomheter. Ettersom verdiene flyttes ut i sky vil trusselaktørene tilpasse seg denne utviklingen [10], [54]. I 2022 var antall hendelser hvor trusselaktører utnyttet skytjenester globalt, nesten tre ganger høyere enn i 2021. Dette viser en trend hvor organiserte kriminelle- og statlige aktører videreutvikler sine verktøy og metoder for å kunne utnytte skytjenester [10]. Målene for angrepene er det samme som mot ikke-skybaserte løsninger [10]. Antall angrep mot skytjenester er fortsatt noe lavere enn angrep mot ikke-skybaserte nettverk, men ifølge sikkerhetsselskapet Check Point blir nyoppdagede sårbarheter oftere forsøkt utnyttet mot skytjenester [9].

For å holde følge med et trusselbilde i rask utvikling, investerer skyleverandører mye i sikkerhet og har god nytte av stordriftsfordeler på sikkerhetssiden [54] . Samtidig er det reelle sikkerhetsnivået et delt ansvar mellom skyleverandøren og kunden. En interessant betraktning er at angrepsvektorene som oftest benyttes er rettet mot sårbarhetene som kundene har ansvar for å håndtere. De mest brukte angrepsvektorene i skytjenester er følgende:

Det er utnyttelse av fjerntilgang ved bruk av gyldige kontoer som oftest benyttes av trusselaktører. Dette muliggjøres av svak tilgangsstyring, manglende flerfaktorautentisering, svake eller ingen passord, kontoer med for høye rettigheter, gjenbruk av passord, kompromittering av påloggingsopplysninger og lignende [54], [16], [9], [10], [94].

Utnyttelse av kompromitterte tilgangsnøkler (Access keys) og API-nøkler er også en mye utnyttet sårbarhet. Eksempler på slik kompromittering kan være at disse nøklene med et uhell er publisert offentlig, for eksempel på GitHub, eller på andre måter kompromittert av en trusselaktør [54], [9], [94]. En annen sårbarhet som i stor grad utnyttes er feilkonfigurasjoner [9], [54], [16], [94]. I tillegg blir ofte sårbarheter i internetteksponerte applikasjoner utnyttet av trusselaktører [9], [54], [10], [94].

Trusselaktører benytter seg også selv av skytjenester, enten som ressurs for å sette opp egen infrastruktur eller for å kompromittere infrastruktur til uvitende ofre for å utføre angrep derfra. Aktørene oppnår de samme fordelene som virksomheter ved å ta i bruk skytjenester, for eksempel økt skalerbarhet og pålitelighet. I tillegg til dette oppnår trusselaktører også fordeler som anonymitet og mulighet for å enklere forbigå sikkerhetsmekanismer siden aktiviteten deres ser ut som normal nettverkstrafikk fra en pålitelig kilde [54], [24], [16].

For mer informasjon rundt dette temaet har interesseorganisasjonen Cloud Security Alliance publisert en god rapport, Top Threats to Cloud Computing Pandemic Eleven, som beskriver sårbarheter og trusler mot skytjenester [94].

Illustrasjonsfoto: Shutterstock

Illustrasjonsfoto: Sykehuspartner

Illustrasjonsfoto: Sykehuspartner

Raskere utnyttelse av sårbarheter

NSM observerer at gjennomsnittstiden fra en sårbarhet blir offentlig kjent til trusselaktører forsøker å utnytte den, blir kortere. De peker videre på at dette særlig gjelder sårbarheter som tillater fjernkjøring av kode fra ikke-autentiserte brukere. Dette gjelder spesielt i tilfeller hvor utnyttelseskoden er offentlig kjent. Utnyttelsen av sårbarheter i Log4j-programvaren er et eksempel på begge deler [37]. Teknologiselskapet Microsoft viser til at gjennomsnittstiden før sårbarheten utnyttes av aktører er 14 dager og presiserer at dette gjelder utnyttelse av både statlige og organiserte kriminelle aktører. Videre er gjennomsnittstiden for når sårbarheten demonstreres (proof of concept) på GitHub 60 dager. Til slutt er gjennomsnittstiden 120 dager før sårbarheten er integrert i verktøy for skanning [24]. Dette viser viktigheten av gode rutiner for sikkerhetsoppdateringer.

Illustrasjonsfoto: Shutterstock

Kunstig intelligens

I 2022 har man sett en videre utvikling i kunstig intelligens. Ny teknologi som dette skaper også muligheter for trusselaktører. Kunstig intelligens, automatisering og ny teknologi brukes blant annet av trusselaktører til «deep fake», gjetting av passord, «bruteforcing» av passord, phishing og for å lage bedre skadevare. Listen over hvilke bruksområder ny teknologi som dette har for trusselaktører er lang [95].

For å demonstrere hvordan denne teknologien kan benyttes, som f.eks å bryte ned språkbarrierer brukte vi 10 minutter for å få ChatGPT til å lage et forslag til en spear phishing e-post for oss:

Write an invitation in norwegian to invite a doctor to hold a presentation at a conference in the doctors area of expertise,. keep the invitation professional without mentioning the recipients health or wellbeing. The recipient must use a link to look for more information about the conference.

Kjære [Doktor],

Vi ønsker å invitere deg til å delta som foredragsholder på vår kommende konferanse. Konferansen vil finne sted [dato og sted] og vil fokusere på [området for doktors ekspertise].

Vi tror din kunnskap og erfaring vil være uvurderlig for vårt publikum og at du vil være en flott tilføyelse til vår liste over foredragsholdere. Vi er sikre på at din presentasjon vil være både informativ og engasjerende.

Vennligst bruk følgende link for mer informasjon om konferansen og registreringsprosessen: [lenke].

Vi setter stor pris på din vurdering av vår invitasjon, og vi ser frem til å høre fra deg snart.

Vennlig hilsen,

[Konferansekomitéen]

Kilder: Chat GPT

Avslutning

Trusselvurderingen har tatt for seg organiserte kriminelle aktører, statlige aktører, hacktivister og selvmotiverte innsidere og vurdering av deres evne og vilje til å påvirke spesialisthelsetjenestens verdier. Hensikten med dette er å gi spesialisthelsetjenesten situasjonsforståelse og beslutningsstøtte.

Til tross for at mange virksomheter jobber aktivt med sikkerhet, viser rapporter til at det som oftest er svakheter i sikkerhetstilstanden som muliggjør vellykkede angrep [37], [24]. Denne trusselvurderingen peker spesielt på at trusselaktørene benytter:

- Sosial manipulering i form av phishing og spear phishing
- Fjerntilgangsløsninger
- Sårbarheter i internetteksponerte tjenester og servere

I tillegg står også ulike former for utnyttelse av påloggingsopplysninger sentralt i svært mange angrep. Virksomheter i spesialisthelsetjenesten må ha kontroll på og lukke sårbarheter knyttet til dette. Virksomheter bør også gjøre gode vurderinger og ha på plass nødvendige tiltak mot leverandørkjedeangrep, bruk av eksternt medie og utnyttelse av innsidere.

I et sikkerhets perspektiv er det effektivt å rette sikkerhetstiltak mot å hindre aktørene i initiell tilgang og dette er derfor et viktig steg å fokusere på. Samtidig må man erkjenne at aktørene vil bryte gjennom den første barrieren og da er det også viktig med gode sikkerhetstiltak i dybden. Dette kan være gjennom sikker arkitektur, overvåkning og deteksjon.

Det presiseres at dette er en vurdering av trusselbildet som kun er én av tre faktorer i risikobildet. Det viktigste her er at virksomheter tar i bruk denne rapporten og vurderer den opp mot eget verdibilde og sårbarhetsbilde. Da kan det gjøres gode risikovurderinger og man vil kunne oppnå effektiv risikostyring og gode prioriteringer i sikkerhetsarbeidet.

Illustrasjonsfoto: Shutterstock

KILDER

[1] Politiets Sikkerhetstjeneste, «Nasjonal trusselvurdering,» 2023.
[2] Etterretningstjenesten, «Fokus 2023,» Etterretningstjenesten, 2023.
[3] Nasjonal Sikkerhetsmyndighet, «Risiko 2023,» NSM, 2023.
[4] International Association of Chiefs of Police, «Cyber Attack Lifecycle,» [Internett]. Available: https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/. [Funnet 10 Januar 2023].
[5] Center for Cybersikkerhed, cfcs, «Trusselvurdering: Fjern adgangen,» Center for Cybersikkerhed, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/trusselsvurdering-fjern-adgangen.pdf, 2021.
[6] ATT&CK, MITRE, «attack.mitre.org,» ATT&CK Matrix for Enterprise, 2023. [Internett]. Available: https://attack.mitre.org/.
[7] Recorded future, «Dark Covenant: Connections between the russian state and criminal actors,» Recorded future, 2021.
[8] Nasjonal Sikkerhetsmyndighet, «Digitalt risikobilde 2021,» 2021.
[9] Checkpoint, «2023 Security report,» Checkpoint, 2023.
[10] Crowdstrike, «2023 Global Threat Report,» Crowdstrike, 2023.
[11] Recorded Future, «Dark Covenant 2.0,» 2023.
[12] Verizon, «Data Breach Investigation Report,» Verizon, 2022.
[13] Krebsonsecurity, «The Original APT: Advanced Persistent Teenagers,» [Internett]. Available: https://krebsonsecurity.com/2022/04/the-original-apt-advanced-persistent-teenagers/.
[14] Cybersecurity & Infrastructuce Security Agency (CISA), «Ransomware guidance and resources,» [Internett]. Available: cisa.gov/ransomware.
[15] Intern kilde.
[16] European Union Agency for Cybersecurity, «ENISA Threat Landscape,» 2022.
[17] Mandiant, «Trust Me, I'm a Professional: The Evolution and Commoditization of the Cyber Crime Ecosystem,» 2021.
[18] Politiet, «Politiets Trusselvurdering (PTV),» 2023.
[19] Europol, «IOCTA - Internet organised crime threat assessment,» 2021.
[20] European Union Agency for Cybersecurity, «ENISA Threat Landscape 2021,» 2021.
[21] Mandiant, «Mandiant News Analysis, Friday 29 Apr 2022».
[22] Økokrim, «Trusselvurdering,» 2022.
[23] Politiet, «Politiets trusselvurdering (PTV),» 2021.
[24] Microsoft, «Digital Defence Report 2022,» Microsoft, 2022.
[25] European Union Agency For Cybersecurity, «Threat Landscape: Main incidents in the EU and worldwide,» 2020.
[26] Curated Intelligence, «Initial Access Broker Landscape,» 221 Oktober 2021. [Internett]. Available: https://www.curatedintel.org/2021/10/initial-access-broker-landscape.html.
[27] Næringslivets Sikkerhetsråd (NSR), «Mørketallsundersøkelsen,» 2022.
[28] IBM, «Cost of a Data Breach Report 2022,» 2022.
[29] Center for Cybersikkerhed, «Cybertruslen mod sunhedssektoren,» 2022.
[30] P. Hannah T. Neprash, M. Claire C. McGlave, P. Dori A. Cross og e. al, «Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021,» Jama Health Forum, 2022.
[31] Politiet, «Politiets trusselvurdering 2022,» 2022.

KILDER

[32] Center for Cybersikkerhed, «Cybertruslen mod Danmark,» CFCS, 2022.
[33] Mandiant, «Industry Snapshot: Healthcare 2022 Q3,» 2022.
[34] Health Sector Cybersecurity Coordination Center (HC3), «2022 Healthcare Cybersecurity Year in Review, and a 2023 Look-Ahead,» 2023.
[35] Reliaquest, «The Top Ransomware Trends to Watch Out for in 2023,» [Internett]. Available: https://www.reliaquest.com/blog/ransomware-trends-2023/.
[36] Chainalysis, «Crypto Crime Report 2023,» 2023.
[37] Nasjonal Sikkerhetsmyndighet, «Digitalt Risikobilde 2022,» NSM, 2022.
[38] Mandiant, «Region Snapshot: Europe 2022 Q3,» 2022.
[39] Sophos, «The State of Ransomware in Healthcare 2022,» 2022.
[40] Paloalto Networks, «INCIDENT RESPONSE REPORT 2022,» 2022.
[41] Health-ISAC, «Current and Emerging Healthcare Cyber Threat Landscape - Executive Summary,» 2022.
[42] Mandiant, «Industry Profile: Healthcare 2021,» 2021.
[43] Office of the Director of National Intelligence Office of the USA, «Annual Threat Assessment 2022,» 2022.
[44] Ehelse.no, «Normen 6.1».
[45] Healthcare Information and Management Systems Society, «Healthcare Cybersecurity Survey,» 2021.
[46] Center for Cybersikkerhed, «Cybertruslen mod dansk forskning og universiteter,» CFCS, 2021.
[47] Insideprivacy, «OFAC Issues Updated Guidance on Ransomware Payments,» [Internett].
Available: https://www.insideprivacy.com/cybersecurity-2/ofac-issues-updated-guidance-on-ransomware-payments/.
[48] Kripos, «Cyberkriminalitet 2023,» 2023.
[49] Wired, «Conti's Attack Against Costa Rica Sparks a New Ransomware Era,» 12 Juni 2022. [Internett].
Available: https://www.wired.com/story/costa-rica-ransomware-conti/.
[50] BleepingComputer, «FBI: Hive ransomware extorted $100M from over 1,300 victims,» 17 November 2022. [Internett].
Available: https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims/.
[51] DNB, «Trusselvurdering,» 2022.
[52] Microsoft, «Digital Defence Report 2021,» 2021.
[53] Mandiant, «M-Trends 2022,» Mandiant, 2022.
[54] Google Inc, «Threat Horizons,» Google Inc, 2023.
[55] Mandiant, «Ransomware and Data Leak Trends: October – December 2022,» 2023.
[56] MedCity News, «What We Learned From Cybersecurity Attacks in Healthcare in 2022,» 18 desember 2022. [Internett].
Available: https://medcitynews.com/2022/12/what-we-learned-from-cybersecurity-attacks-in-healthcare-in-2022/.
[57] Health Sector Cybersecurity Coordination Center HC3, «HC3: Healthcare Cybersecurity Bulletin,» 2022.
[58] Healthcare Information and Management Systems Society, «HIMSS healthcare cybersecurity survey,» 2021.
[59] NRKbeta, «Trodde de betalte leverandøren- norsk universitet loppet for 12 millioner med ny svindel metode,» [Internett].
Available: https://nrkbeta.no/2022/02/03/trodde-de-betalte-leverandoren-norsk-universitet-loppet-for-12-millioner-med-ny-svindelmetode/.
[60] L. Bjerkan, «Bedragere lurte norsk bedrift for en halv milliard. Så ventet politiet halvannen måned med å advare mot metoden,» [Internett].
Available: https://www.aftenposten.no/okonomi/i/BmjvG/bedragere-lurte-norsk-bedrift-for-en-halv-milliardsaa-.
[61] FBI, «Internet Crime Report 2021,» 2021.

KILDER

[62] HelseCERT, «Situasjonsbilde 2021,» 2021.
[63] Økokrim, «Nasjonal risikovurdering 2022,» 2022.
[64] Crowdstrike, «What is Cyber Espionage?,» Crowdstrike, 28 Februar 2023. [Internett]. Available: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.
[65] Congressional Research Service, «Russian Cyber Units,» 2021.
[66] T. W. Post, «How the Russians hacked the DNC and passed its emails to WikiLeaks,» https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.
[67] Svensk Forsvarsmakt MUST, «MUST årsoversikt 2022».
[68] Etterretningstjenesten, «Fokus 2022,» 2022.
[69] PriceWaterhouseCoopers, «Cyber Threats 2021: Year in retrospect,» 2021.
[70] Mandiant, «Country Profile: China 2022,» 2022.
[71] NRK, «Iransk etterretning tar seg inn i mobiltelefoner i Norge,» 26 Februar 2023. [Internett]. Available: https://www.nrk.no/norge/iransk-etterretning-tar-seg-inn-i-mobiltelefoner-i-norge-1.16308804.
[72] Mandiant, «Country Profile: Iran (2022),» 2022.
[73] Mandiant, «Country Profile: North Korea (2022),» 2022.
[74] Microsoft, «Special report Ukraine: An overview of Russia's cyberattack activity in Ukraine,» 2022.
[75] Mandiant, «Country profile: Russia 2022,» 2022.
[76] CCDCOE, «Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO,» 2022. [Internett]. Available: https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/. [Funnet 20 Mars 2023].
[77] FN Sambandet, «FN Pakten,» [Internett]. Available: https://www.fn.no/om-fn/avtaler/fn-pakten. [Funnet 20 Mars 2023].
[78] E. V. W. Davis), Shadow Warfare, Cyber Policy in the United States, Russia, and China,, Rowman & Littlefield, 2021.
[79] Microsoft, «Microsoft investigates Iranian attacks against the Albanian government,» 08 September 2022. [Internett]. Available: https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/. [Funnet 15 Mars 2023].
[80] CISA, «Iran Cyber Threat Overview and Advisories,» [Internett]. Available: cisa.gov/iran. [Funnet 14 Mars 2023].
[81] Time Magazine, «Everything We Know About Sony, The Interview and North Korea,» 17 Desember 2014. [Internett]. Available: https://time.com/3639275/the-interview-sony-hack-north-korea/. [Funnet 10 Mars 2023].
[82] Kaspersky, «What is known about the Lazarus Group: Sony hack, military espionage, attacks on Korean banks and other crimes,» 24 Februar 2016. [Internett]. Available: https://www.kaspersky.com/blog/operation-blockbuster/11407/. [Funnet 9 Mars 2023].
[83] Mandiant, «GRU: Rise of the (telegram) MiniOns,» 23 September 2022. [Internett]. Available: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions.
[84] NRK, «Norske sykehus trues av russiske hackergrupper,» 28 Januar 2023. [Internett]. Available: https://www.nrk.no/norge/norske-sykehus-trues-av-russiske-hackergrupper-1.16275175.
[85] Center for Cybersikkerhed, «CFCS hæver trusselsniveauet fra cyberaktivisme mod Danmark fra MIDDEL til HØJ,» 2023.

KILDER

[86] Mandiant, «The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine,» 16 Mai 2022. [Internett]. Available: https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine. [Funnet 17 Mars 2023].

[87] Sentinel One, «NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO,» 12 Januar 2023. [Internett]. Available: https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/. [Funnet 24 Mars 2023].

[88] Microsoft, «KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks,» 17 Mars 2023. [Internett]. Available: https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/. [Funnet 23 Mars 2023].

[89] Center for Cybersikkerhed, «Cybertruslen fra bevidste og ubevidste insidere,» 2019.

[90] Proofpoint, «The Primary Factors Motivating Insider Threats,» 17 Februar 2021. [Internett]. Available: https://www.proofpoint.com/us/blog/insider-threat-management/primary-factors-motivating-insider-threats.

[91] N. Mansor, «Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research,» 2015.

[92] Næringslivets Sikkerhetsråd, «KRISINO,» 2021.

[93] Spirion, «Understanding malicious insider threat examples to avoid an insider attack,» 10 November 2021. [Internett]. Available: https://www.spirion.com/blog/malicious-insider-threat-examples/.

[94] Cloud Security Alliance, «Top Threats to Cloud Computing Pandemic Eleven,» Cloud Security Alliance, Top Threats Working Group, 2022.

[95] Health Sector Cybersecurity Coordination Center HC3, «Automation & Hacking: Potential Impacts on Healthcare,» 2022.

[96] Departementenes sikkerhets- og serviceorganisasjon, «NOU 2016:8 En god alliert – Norge i Afghanistan 2001–2014», 2016.

[97] Nasjonal Sikkerhetsmyndighet, «Risiko 2022,» 2022.

[98] Health- Information Security and Analysis Center, «CURRENT AND EMERGING HEALTHCARE CYBER THREAT LANDSCAPE,» 2022.

[99] Nasjonal Sikkerhetsmyndighet, «Temarapport Innsiderisiko,» 2018.

[100] Forsvarets Efterretningstjeneste, «Efterretningsmæssig risikovurdering,» 2020.

[101] PWC, «Conti cyber attack on the HSE; Independent Post Incident Review,» 2021.

VEDLEGG

Trusselvurdering 2023 - Angrepsvektorer

Trykk for å åpne vedlegg 1

Trusselvurdering 2023 - Metodikk

Trykk for å åpne vedlegg 2

Ved noen tilfeller er det mulig at knappene ikke vil åpne vedleggene automatisk.
Vedleggene må da åpnes manuelt.