HelseCERT
Situasjonsbilde 2021

Norsk helsenett

Innhold

Oppsummering

De mest aktive trusselaktørene mot norsk helsesektor har vinningskriminalitet som motiv. Sektoren utsettes for både målrettet og ikke-målrettet aktivitet.

De mest kompetente trusselaktørene mot norsk helsesektor er statsstøttede grupperinger (Advanced persistent threat, APT). Gruppenes motiv er både knyttet til industrispionasje, for eksempel tyveri av forskningsdata, og å bygge kapabiliteter for å slå ut nasjonalt kritisk infrastruktur. De har også en interesse av å hente ut opplysninger om enkeltpersoner som for disse grupperingene utgjør etterretningsmål.

Det er **meget sannsynlig** at virksomheter i helsesektoren utsettes for kampanjer fra vinningskriminelle.

Det er **meget sannsynlig** at avanserte trusselaktører forsøker å tilegne seg forskningsdata og helseopplysninger.

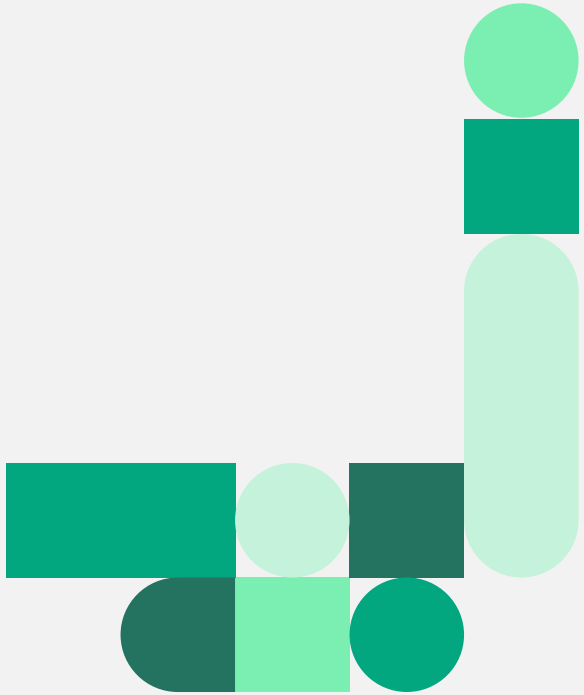
Det er **sannsynlig** at skadevarekampanjer fra vinningskriminelle påvirker sentral IKT-infrastruktur og dermed rammer pasientbehandlingen.

Det er mulig at nasjonalstater forsøker å bygge kapabiliteter for å sabotere nasjonal e-helseinfrastruktur med formål å drive destabilisering.

Bakgrunn

Helse- og omsorgsektoren (heretter omtalt som helsesektoren) er inne i en fase med kraftig digitalisering. Pasientsikkerhet er et viktig fundament i helsetjenesten, og med den økende digitaliseringstakten seiler digital sikkerhet opp som et viktig element som påvirker pasientsikkerheten. Helsetjenesten må både sørge for å ivareta sikkerhet og personvern i forvaltningen av helsedata, og sørge for at de tjenestene som inngår i de digitale verdikjedene er tilgjengelige og operative til enhver tid. I denne rapporten trekker vi fram aktuelle trender, trusler og sårbarheter gjeldende helsesektoren, og aktuelle anbefalinger. Rapporten er avgrenset til å beskrive tilsiktede handlinger, og tar ikke for seg utilsiktede hendelser.

Formålet med denne rapporten er å gi et kortfattet situasjonsbilde for helsesektoren i Norge.



Trender

Løsepengeaktører har blitt mer sofistikerte, og angrep som tidligere primært rammet en maskin, rammer nå hele virksomheter.

LØSEPENGEGRUPPER

Et ledd i denne utviklingen, er at organiserte grupper aktivt leter etter virksomheter med svakheter. Siden svakhetene som utnyttes varierer, ser vi at hvilke virksomheter som rammes kan framstå som tilfeldig. Angriperne skaffer fotfeste og utvider deretter kontrollen i virksomheten, før de stjeler data de anser som sensitiv, og krypterer data og systemer de har tilgang til.

Dette gir angriper mulighet til å kreve løsepenger både for å låse opp data, og ikke publisere stjålet informasjon.

Vi er kjent med at angripere har skaffet fotfeste gjennom utnyttelse av kjente sårbarheter. Dette gjør de ved bruk av brukernavn og passord mot systemer som ikke har vært sikret med flerfaktorautentisering, samt kjøp av tilgang til systemer fra andre kriminelle aktører.

Løsepengegruppene jobber kontinuerlig med å skaffe seg tilgang til virksomheter. Når de har fotfeste i en virksomhet, bruker de en rekke verktøy for å utvide kontrollen. Om de oppnår fotfeste i en virksomhet, kan kryptering komme etter timer, dager eller uker.

Virksomheter angripes ukritisk, og flere sykehus i Tyskland, Australia og USA har vært hardt rammet. Vi vurderer at sykehus i Norge er et mål på lik linje med sykehus i utlandet.

Arbeidet de siste årene med å lukke sårbarheter, herde arbeidsflaten og sikre spesialisthelsetjenesten bak Helsenettet, har så langt bidratt til at

Ransomware Düsseldorf universitetssykehus:

Angriperne fikk tilgang gjennom en kjent sårbarhet (CVE-2019-19781) hos Düsseldorf universitet. Patch ble installert så fort den kom ut, men da hadde angriper allerede fotfeste. Angriper var deretter i nettverket i over åtte måneder før de gjennomførte kryptering. Wired har en artikkel som oppsummerer dette angrepet. [1]

Løsepengevirus traff USA hardt i 2019:
Totalt 764 helsetilbydere ble rammet av løsepengevirus. Emisoft har en lengre artikkel med gjennomgang av hva som ble rammet og noen av konsekvensene. [2]

Metodikk:
Angrepsmetodikk og verktøy brukt av forskjellige løsepengegrupper varierer. Metodene brukt som inngangsvektor inkluderer blant annet RDP-brute force og tilgang fra e-post spredt skadevare som Dridex, Emotet og Trickbot.

Microsoft har en bloggpost som går gjennom dette i mer detalj, inkludert hvordan angriperne beveger seg videre i nettverket. [3]

[1] https://www.wired.co.uk/article/ransomware-hospital-death-germany
[2] https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019
[3] https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster

norske sykehus ikke har vært rammet av slike angrep.

Vi ser imidlertid at det fortsatt er mange som benytter gamle systemer og som har utfordringer med teknisk gjeld. Et eksempel på dette er hendelsen ved Sykehuset Innlandet HF hvor det ble gjennomført et datainnbrudd mot et eldre sårbart system. Via dette systemet fikk angriper tilgang til interne databaser.

MASSESPREDT SKADEVARE

Da Norge ble mål for en massespredt skadevarebølge på sensommeren 2020 ble flere kommuner og mindre klinikker rammet hardt (se faktaboks om Emotet). Det som skilte denne bølgen fra tidligere tilsvarende bølge, var at e-postene var på norsk, og så ut til å komme fra kjente avsendere. Slike infeksjoner ender ofte med løsepengevirus.

Vi forventer å se mer av slike hendelser framover, og IKT-systemene til de mindre aktørene må sikres bedre.

Mens spesialisthelsetjenesten begynner å få grunnleggende herding på plass, er dette mangelfullt flere steder i primærhelsetjenesten og blant mindre aktører i helsesektoren.

Emotet:
Skadevaren Emotet begynte som en banktrojaner i 2014. Den har siden blitt videreutviklet, og benyttes til informasjonstyveri og videresalg av tilgang. Emotet spres gjennom e-poster, hovedsakelig med MS Word dokumenter med skadelig makrokode. Makroen laster ned trojaneren og installerer denne. Umiddelbart etter installasjon vil Emotet forsøke å stjele e-poster og passord, for deretter å bruke disse for videre spredning. Om det infiserte systemet anses som verdifullt vil trusselaktøren selge tilgangen til løsepengegrupper. For at angrepet skal lykkes kreves det at offeret åpner e-posten, deretter vedlegget og til slutte aktiverer makroer. Varsel NCSC [1]. (Enkelte av aktørene bak Emotet ble arrestert i starten av 2021, og denne skadevarefamilien er ikke lengre aktiv)

[1] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/varsel-om-pagaende-emotet-kampanje

Universitetet i Tromsø (UiT) svindlet for 12 millioner kroner:
Svindler utga seg for å være UiT til en leverandør og fikk tilsendt utestående fakturaer. Svindler endret kontonummer til sitt eget og sendte de modifiserte fakturaene til UiT.
Pressemelding fra UiT. [1]

Norfund svindlet for 100 millioner kroner:
Svindler skaffet tilgang til intern saksinformasjon om et bistandsprosjekt, og satte deretter opp et falskt foretak i utlandet som etterlignet det reelle. Svindler meldte så at de på grunn av koronaproblemer hadde endret kontaktinformasjon, og et nytt kontonummer de ønsket bistandsmidlene utbetalt til.
Norfund pressemelding. [2]

[1] https://uit.no/nyheter/artikkel?p_document_id=659434
[2] https://www.norfund.no/no/norfund-er-utsatt-for-alvorlig-svindel

SVINDELFORSØK

De siste årene har vi sett en profesjonalisering av økonomiske svindelgrupper. Disse gruppene gjør gjerne grundig forarbeid, inkludert rekognosering, for å fremstå mest mulig troverdig ovenfor ofrene. De er villige til å kjøre lange operasjoner hvor de holder e-postdialoger gående over lang tid. I likhet med løsepengegruppene varierer metodene og målene. Svindlene vi ser kan grovt grupperes slik:

- Fakturasvindel - hvor svindlerne forsøker å skaffe legitime fakturaer og endrer kontonummer på disse.

- Direktørsvindel - hvor de forfalsker kommunikasjon så den ser ut til å komme fra en direktør som trenger en "konfidensiell hastebetaling".

- BEC - hvor de forsøker å skaffe tilgang til e-post-kommunikasjon for å skreddersy svindler basert på innsideinformasjon.

Her er det viktig at virksomheter har sikkerhetstiltak på plass for å sikre hvor de overfører penger. HelseCERT har et sett med tiltak vi anbefaler for å sikre at alle betalinger er korrekte og går til korrekt mottaker.

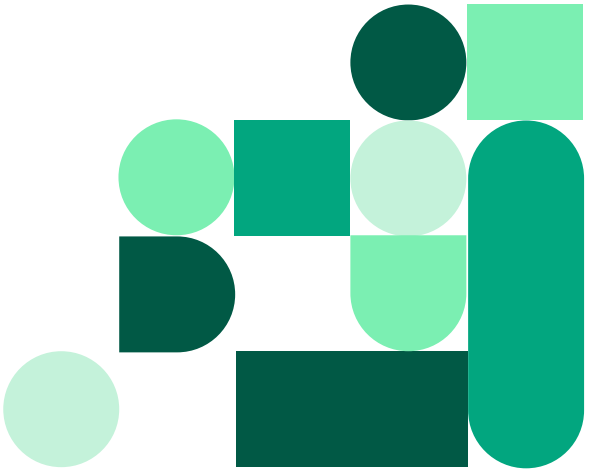
INDUSTRISPIONASJE

Forskningsdata er et verdifullt mål for trusselaktører. Sykehus og andre helseinstitusjoner som bidrar til, og har tilgang til forskningsdata, må være forberedt på at trusselaktører aktivt forsøker å skaffe tilgang til disse. Dette er spesielt dagsaktuelt i den pågående pandemien. HelseCERT forventer at forskning knyttet til COVID-19 vil kunne være av interesse for ressurssterke angripere, på lik linje med annen virksomhet der man sitter på informasjon som kan være av verdi for andre.

Målrettede angrep fra trusselaktører forventes å før eller siden bryte skallsikring, og beskyttelse i dybden blir da kritisk både for å begrense spredning og oppdage infeksjon.

VERDUKJEDEANGREP

I 2020 har vi også sett noen profilerte verdikjedeangrep. Dette er ikke et nytt konsept. Trusselaktører ser på



verdikjeder som et mulig svakt ledd hvor de kan utnytte svakheter hos en (under)leverandør til å angripe et mål med bedre beskyttelse. I angrepet mot Helse Sør-Øst i 2018, var angripers antatte mål å skaffe seg tilgang til kildekode til et e-læringssystem for å bruke kunnskap om dette til å angripe andre mål. Verdikjedeangrep er, og vil fortsette å være, en trussel. En virksomhet vil i liten grad ha mulighet til å teste alle systemer, og systemoppdateringer fra tredjeparter. Innkapsling av slike systemer blir et viktig sikringstiltak. Beskyttelse i dybden blir også her en viktig sikringsmetode for å begrense skaden ved en eventuell infeksjon.

Målrettede verdikjedeangrep, som Solarwinds-angrepet, kan være vanskelige å oppdage av flere grunner. Trusselaktøren er ofte kompetent, villig til å kjøre en lang operasjon og får skadevaren sin installert gjennom vanlige rutiner og prosesser hos målet. For å kunne øke motstandsdyktigheten mot slike angrep er det viktig å bygge forsvarbar infrastruktur. Dette er infrastruktur som er tilrettelagt for å kunne motstå og håndtere cyberangrep, der systemer kan isoleres fra resten av infrastrukturen og man har god synlighet igjennom logging fra både sentral infrastruktur og endepunkter.

Om kompromitteringen skulle være et faktum vil god intern logging være en kritisk suksessfaktor for å kart-legge omfang og utbredelse av angrepet, og gjøre god og effektiv håndtering mulig.

Ord og uttrykk

ORDLISTE

SPESIALHELSETJENESTEN:
Sykehus, distriktspsykiatriske sentre, opptrenings- og rehabiliteringsinstitusjoner, institusjoner for tverrfaglig spesialisert rusbehandling, prehospitale tjenester, privatpraktiserende spesialister og laboratorie- og røntgenvirksomhet.

Organisert i fire regionale helseforetak, med fire tilhørende IKT-driftsorganisasjoner: Sykehuspartner, HVIKT, HNIKT og HEMIT.

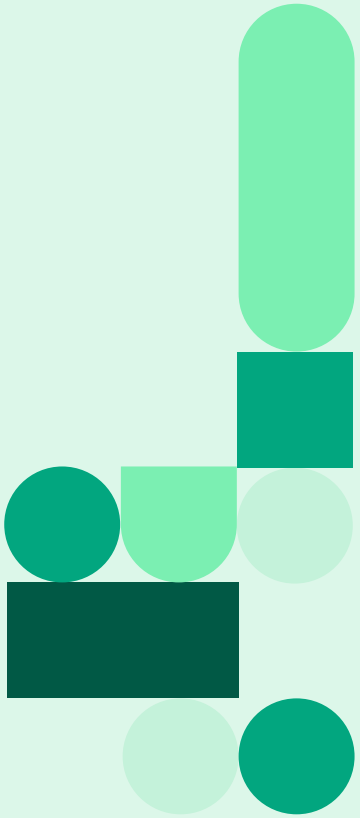
PRIMÆRHELSETJENESTEN:
Allmennleger, kommunale helsetjenester m.m.

APT: Advanced persistent threat. Primært brukt om statsstøttede grupper som driver med offensive, digitale operasjoner.

VERDIKJEDE:
Verdikjeder brukes til å definere kjeden som er med på å skape varer/tjenester (verdier) i en virksomhet og inkluderer underleverandører. Lange verdikjeder oppstår når en underleverandør bruker en annen underleverandør, som igjen bruker en annen underleverandør. En lang verdikjede bidrar til en større angrepsflate som trusselaktører kan utnytte til å angripe en virksomhet, og det kan være vanskelig å danne seg et totalt risikobilde for virksomheten som er på toppen.

LØSEPENGEVIRUS:
Ondsinnet kode som krypterer informasjon, og deretter krever løsepenger for at informasjonen skal bli dekryptert. Man betaler i den forventningen om at man får nøkkelen for å låse opp sin eiendel (informasjonen).

TEKNISK GJELD:
Mangel på vedlikehold og oppdatering av teknologi og systemer som over tid gjør at en virksomhet ender opp med å ha et lappeteppe av sårbare systemer, uheldige konfigurasjoner og halvferdige prosjekter og løsninger som man vet burde vært fikset, men hvor man mangler ressursene til å implementere en mer optimal teknisk løsning. Årsaken til teknisk gjeld er normalt at man velger kjappe og kortsiktige løsninger på bekostning av god og langsiktig planlegging.



BEC:
Business Email Compromise er et angrep hvor en angriper får tilgang til en e-postkonto i en virksomhet, og bruker denne for å lure ansatte i bedriften til å gjennomføre feilaktige utbetalinger.

PASSORDSPRAYING:
Med passordspraying angriper man mange brukere med noen få utvalgte passord. Det viser seg at hvis en virksomhet har mange nok ansatte vil noen med stor sannsynlighet bruke noen gjentagende passord som kan gjettes. Eksempel på dette er passord som bruker en kombinasjon av årstid og årstall, for eksempel; "Vinter2021".

SANNSYNLIGHETSORD

Vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte, er det benyttet sannsynlighetsord (se tabell).

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