Saksframlegg

Saksgang:

Styre	Møtedato
Styret Helse Sør-Øst RHF	22. august 2024

Sak 083-2024

Det digitale trusselbildet mot spesialisthelsetjenesten

Forslag til vedtak:

Styret tar rapporten til orientering.

Hamar, 15. august 2024

Terje Rootwelt
administrerende direktør

1 Hva saken gjelder

Mange farer og trusler kan påvirke evnen til å levere spesialisthelsetjenester. Ekstremvær, brann, feilkonfigurering av servere og programvarefeil er eksempler på *utilsiktede* hendelser som kan sette hele eller deler av den digitale infrastrukturen ut av funksjon. Denne styresaken handler om cyberangrep, etterretning og andre *tilsiktede* hendelser som utgjør en trussel mot våre digitale løsninger.

Helse- og omsorgsdepartementet har bedt de regionale helseforekene om å utarbeide en årlig rapport om trusler og trender innen 1. juni hvert år. Trusselvurderingen[1] er utarbeidet og formidlet til departementet innen fristen.

Trusselvurderingen for spesialisthelsetjenesten utarbeides på bakgrunn av de åpne trusselvurderingene fra E-tjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM), også omtalt som EOS-tjenestene. Årets rapport er, som i 2023, utarbeidet i samarbeid mellom de fire regionale IKT-foretakene og HelseCERT (Norsk helsenett SF).

Formålet med rapporten er å gi grunnlag for en omforent situasjonsforståelse blant ledere og medarbeidere i spesialisthelsetjenesten, slik at vi bedre evner å vurdere risiko vi står ovenfor og kan iverksette tiltak ut fra dette. Trusselvurderingen skal gi innsikt i hvordan man kan forstå hva som truer spesialisthelsetjenestens verdier og hvilken risiko dette utgjør. Trusselaktørene og deres angrepsmetoder vurderes og overvåkes, samtidig som det må skapes forståelse i organisasjonen for hvordan sårbarheter kan utnyttes av disse. Systematisk og god håndtering av sårbarheter er et viktig virkemiddel for å redusere risiko.

Spesialisthelsetjenesten er en grunnleggende tjeneste i samfunnet og har en viktig beredskapsfunksjon for ivaretakelse av liv og helse. Dette gjør spesialisthelsetjenesten trusselutsatt på lik linje med andre deler av totalforsvaret og kritisk infrastruktur.

2 Hovedpunkter og vurdering av handlingsalternativer

Et vellykket cyberangrep mot spesialisthelsetjenesten kan medføre store konsekvenser for spesialisthelsetjenestens evne til å utføre sine primæroppgaver. Dagens trusselbilde er komplisert og i endring som følge av trusselaktørenes økte tilpasningsevne og utvikling av verktøy og metoder. Statistikken globalt viser en økning av angrep mot helsesektoren, og helsesektoren er den tredje mest angrepsutsatte sektoren.

Destruktive angrep i form av digital utpressing fra organiserte kriminelle aktører er vurdert til å utgjøre den største trusselen mot spesialisthelsetjenesten. Slike angrep utnytter sårbarheter i programvare til å kjøre løsepengevirus som krypterer data og gjør løsninger utilgjengelige. Trusselaktøren vil forsøke å holde seg skjult lenge nok til at de også rekker å helt eller delvis ødelegge sikkerhetskopier. Data og løsninger låses opp mot betaling.

[1] Trusselvurdering 2024 for spesialisthelsetjenesten - Sykehuspartner HF

Cyberoperasjoner og rekruttering av innsidere vil være blant de mest sentrale metodene for statlige aktører i 2024, og det forventes at Russland og Kina vil være spesielt aktive i sine forsøk på å rekruttere kilder og innsidere.

2.1. Aktørutvikling

Global statistikk viser at angrep mot helsesektoren har økt, sett opp mot fjoråret. Organiserte kriminelle aktører står bak de fleste angrep. De er opportunistiske og økonomisk motiverte med en økende grad av kartlegging og målrettet aktivitet mot de med betalingsevne og -vilje. Gjennom det siste året har det vært 20 prosent økning i omsetning knyttet til kompromitterte tilganger til datasystemer. Tilgangene kjøpes og selges i all hovedsak mellom organiserte kriminelle, men også til statlige aktører. Dette er en trend man forventer vil fortsette. Aktørene som spesialiserer seg på salg av tilganger knytter tettere bånd til aktørene som utvikler verktøy for å finne og utnytte tilgangene.

I de åpne trusselvurderingene fra EOS-tjenestene beskrives Russland som den største etterretningstrusselen mot Norge, og Kina som en økende trussel. Den økte aktiviteten fra disse aktørene ses i all hovedsak i cyberdomenet. Russland har mistet diplomatisk fotfeste i vesten. Bare i Norge har 15 russiske diplomater blitt utvist siden krigen i Ukraina startet, noe som medfører at de må finne alternative informasjonskilder. For spesialisthelse-tjenesten betyr det blant annet økt innsiderisiko.

Statlige aktører prioriterer spionasje og informasjonslekkasje, og bedriver i liten grad destruktive cyberoperasjoner. Unntaket er Nord-Korea som benytter både offentlig kjente skadevarer og egenutviklede skadevarer i cyberangrep. Nord-Korea utnytter sårbarheter i internetteksponerte tjenester og skytjenester, og det har blitt observert kampanjer hvor målsetningen er å få tilgang til påloggingsopplysninger for å benytte disse i senere angrep.

Forskningsdata, beredskapsinformasjon og helseopplysninger er noen av verdiene som statlige aktører ønsker tilgang til. Globalt er medisinsk forskning et område som spesielt statlige aktører er opptatt av. Forskning er en viktig og integrert del av helsesektoren, og spesialisthelsetjenesten har samarbeid med ulike forskningsinstitusjoner. I økende grad benytter trusselaktørene innsidere, tredjeparter og underleverandører for å få tilgang til informasjon. Dette krever økt oppmerksomhet om innsiderisiko, innsikt og kontroll med leverandørkjeder, samt bedre forståelse for verdiene spesialisthelsetjenesten besitter. Krav om bakgrunnssjekk er på høring[2]. Trusselvurderingen er relevant for utarbeidelsen av høringssvar fra Helse Sør-Øst RHF.

De åpne trusselvurderingene fra PST, NSM og E-tjenesten viser alle et skjerpet trusselbilde knyttet til leverandørkjeder og statlige aktører. Det er krevende å vurdere risiko og sårbarheter for informasjonssikkerhet i lange leverandørkjeder. Regelverket setter også begrensninger i muligheten til å diskriminere på geografisk tilknytning alene, for eksempel at et europeisk selskap har eier fra et høyrisikoland. Det er dermed utfordrende å stille krav som balanser nytteverdi opp mot leverandørkjederisiko. Leverandørkjedene er ofte lange og med forgreininger til leverandører fra høyrisikoland. For eksempel kan et europeisk datterselskap, med morselskap i høyrisikoland, levere et tilbud som ivaretar alle funksjonelle krav, til en lav pris. For løsninger som omfattes av sikkerhetslovens krav til

[2] Høring - krav om bakgrunnssjekk - regjeringen.no

leverandørklarering, håndteres leverandørrisikoen i stor grad av Nasjonal sikkerhets-myndighet.

Hacktivisters evne til å utgjøre en trussel varierer. Enkelte grupper er ikke i stand til å utføre mer enn forstyrrende distribuerte tjenestenektangrep (DDoS), mens andre har kapasitet til å gjennomføre større koordinerte operasjoner og kompromittere utvalgte mål. Man har sett en økning i evnen hos enkelte grupperinger det siste året, der flere store vellykkede angrep har blitt gjennomført.

2.2. Teknologiutvikling gir nye angrepsflater

Bruk av skytjenester øker i omfang. Ved overgang til ny teknologi vil noen angrepsflater kommet til og andre bli borte. Skytjenester har mange sikkerhetsmessige fordeler, men det kan være kompliserte å sette dem opp på en trygg måte. De fleste sikkerhetshendelser i skytjenester er et resultat av feilkonfigurering hos kunden. Skytjenestene er gjerne integrert med interne IKT-systemer, og ved feil oppsett kan det skapes en utilsiktet ekstern eksponering av interne tjenester. Samtidig gir skytjenester muligheter for realisering av gevinster fra teknologiutvikling og digitalisering, samt at det også kan bidra til bedre sikkerhet.

Kunstig intelligens er systemer som, med en grad av autonomi, utfører handlinger basert på tolkning og behandling av strukturerte eller ustrukturerte data for å oppnå et spesifikt mål. Virksomheter må ta i bruk kunstig intelligens på en trygg og ansvarlig måte, mens trussel-aktørene kan ta i bruk teknologien raskere uten tanke på trygge rammer og reguleringer. Dette skaper ujevne odds. Flere rapporter viser til en betydelig økning av falske videoer benyttet i bedragerier. I Hong Kong ble en regnskapsmedarbeider lurt til å overføre omkring 250 millioner kroner etter en 45 minutter lang videokonferanse. I ettertid avdekket etterforskningen at regnskapsmedarbeideren var det eneste ekte mennesket i samtalen; de andre deltakerne var KI-genererte kopier av selskapets ledelse.

3 Administrerende direktørs anbefaling

For å motstå avanserte cyberangrep kreves det en helhetlig tilnærming til sikkerhets-arbeidet, hvor vi må ha flere og gode sikkerhetsbarrierer som er effektive mot både opportunistiske angrepsforsøk og angrep fra avanserte statlige aktører. Spesialisthelse-tjenesten må derfor ha velutviklede metoder for å avdekke uønsket aktivitet, for å håndtere denne aktiviteten og for å igangsette nødvendige risikoreduserende tiltak.

Rapporten vil bli benyttet til bevisstgjørings- og opplæringstiltak i Helse Sør-Øst, og som grunnlag for vurderinger i arbeid med risiko- og sårbarhetsvurderinger. Rapporten er presentert for de administrerende direktørene ved helseforetakene, og Sykehuspartner HF tilbyr å presentere rapporten i helseforetakenes styrer og ledergrupper.

Administrerende direktør anbefaler at styret tar rapporten til orientering.

Trykte vedlegg:
- Ingen

Utrykte vedlegg:
- Trusselvurdering 2024 – det digitale trusselbildet mot spesialisthelsetjenesten