HELSE NORD IKT

SAKSFRAMLEGG

Arkivreferanse: 2022/237-4
Saksbehandler: Knut Øyvind Johansen

Saksgang		
Saksnummer	**Møtedato**	**Utvalg**
52/23	13.09.2023	Styret Helse Nord IKT HF

Trusselvurdering 2023, gjennomgang

Innstilling til vedtak

Styret i Helse Nord IKT HF inviteres til følgende vedtak:

1. Styret i Helse Nord IKT HF tar gjennomgang av trusselvurdering 2023 til orientering.

Trusselbildet

Trusselvurdering 2023

HN IKT har samarbeidet med Sykehuspartner om å utarbeide en strukturert trusselvurdering for spesialisthelsetjenesten. Årets samarbeid har blitt ytterligere styrket ved inkludering av nøkkelkompetanse fra HelseCERT og Sykehuspartner CERT. Samarbeidet med Helse Vest IKT og Hemit er av samme omfang som ved forrige styrerapportering. Trusselvurderingen redegjør for, og vurderer, hvilke aktører som har vilje og evne til å utgjøre en trussel mot våre verdier. Rapporten beskriver også hvilke virkemidler trusselaktørene kan benytte. En endring fra tidligere er at trusselvurderingen nå vil være offentlig tilgjengelig, i motsetning til trusselvurdering for 2022 som var unntatt offentligheten.

Vurdering

Spesialisthelsetjenesten tiltrekker seg oppmerksomhet fra ulike trusselaktører i det digitale rom. 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. De digitale utpressingsaktørenes vilje mot spesialisthelsetjenesten vurderes som meget høy. Dette er basert på hva vi observerer, andre sentrale myndighetsorganer og sikkerhetsselskapers vurderinger og trusselaktørenes høye aktivitetsnivå mot helsesektoren globalt.

Helsesektorens behov for tilgjengelighet av IKT-systemer, og da implisitt den høye kritikaliteten ved nedetid, vurderes som den mest sentrale driveren til digitale utpressingsaktører. Dette innebærer også at kliniske systemer kan være et mål. Statlige aktører vurderes å utgjøre en betydelig trussel for spionasje mot spesialisthelsetjenesten.

Russland og Kina vurderes til å være 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.

Det siste året har man observert angrep mot norsk helsesektor fra hacktivister med bakgrunn i Norges støtte til Ukraina. Denne angrepskampanjen inkluderte også et av sykehusforetakene i Helse Nord. Det vurderes som sannsynlig at spesialisthelsetjenesten vil bli direkte forsøkt rammet av angrep gjennomført av pro-russiske aktivistgrupper. Basert på sammenlignbare angrep vurderer vi at skadepotensialet av et tjenestenektangrep fra hacktivister vil være lavt og kortvarig for spesialisthelsetjenesten.

Til tross for at mange virksomheter jobber aktivt med sikkerhet og digital motstandsdyktighet, viser rapporter 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 møte utviklingen i trusselbildet.

Trusselvurderingen for 2023 ble framlagt som vedlegg til styresak 32/23 i styremøte i juni 2023. I dette møtet ønsker vi å gjennomgå trusselvurdering 2023 for styret.

Administrerende direktørs vurdering

Trusselvurderingen gir oss ingen hvilepute innen informasjonssikkerhetsområdet. Vi ser at helseforetak i vår regionen spesifikt nevnes som mål, og at helsesektoren stadig blir et mer attraktivt mål for organiserte kriminelle.

Trusselaktørene utvikler raskt nye verktøy og metoder, og sårbarheter blir forsøkt utnyttet raskere. Dette betyr at et tradisjonelt perimeterforsvar ikke lengre er tilstrekkelig for å motstå angrep.

Vi som virksomhet må bygge inn sikkerhet i flere ledd gjennom sikkerhet i dybden og «zero trust», og kontinuerlig utvikle oss innen dette området.

Selv om statusen som ble framlagt for styret i styresak 32/23 i juni 2023 tilsier at vi i stort har en positiv utvikling i informasjonssikkerhetsarbeidet, utvikler også trusselbildet seg. Og det gjenstår fortsatt rom for betydelige forbedringer.

Oddbjørn Schei

Administrerende direktør

Dette saksframlegget er elektronisk godkjent og innehar derfor ikke håndskrevet signatur.

Vedlegg:

1 Trusselvurdering 2023 - foreløpig utgave

2 Trusselvurdering 2023 - Vedlegg 1 - Angrepsvektorer

3 Trusselvurdering 2023 - Vedlegg 2 - Metodikk