Nasjonalt senter for e-helseforskning

SAK TIL STYRINGSGRUPPEN

Status Praksisnett

Saksnummer	5-2024
Avsender	Senterleder
Møtedato	16.02.2024

Bakgrunn for saken

Praksisnett har vært tema for flere saker i styringsgruppen, og sist gjennom en orientering fra prosjektleder professor Guri Rørtveit i form av faglig presentasjon i møte 9.11.2023. I sak 25/2023 etterlyste styringsgruppen en ROS-analyse og helhetlig vurdering av Praksisnett. Praksisnetts IT-del har utarbeidet en ROS-analyse, se vedlegg 1.

I desember 2023 ble det klart at prosjektleder går over i ny rolle som direktør for Folkehelseinstituttet, og professor Bjørn Bjorvatn ved Universitetet i Bergen tar over prosjektledelsen. I styringsgruppemøte for Praksisnett 05.02.2024 orienterte prosjektledelsen om konsekvenser og videre framtid for Praksisnett. NSEs rolle i prosjektet er per i dag ikke endret.

Praksisnett har en finansieringsutfordring. Per i dag har prosjektet noe restmidler fra Norges forskningsråd, i tillegg til finansiering over statsbudsjettet og brukerfinansiering. Dette er imidlertid ikke tilstrekkelig for å opprettholde full drift, noe som særlig går ut over IT-delen, som NSE har ansvar for. Styringsgruppen for Praksisnett klarte ikke å komme til enighet om et budsjett i møtet 05.02.2024, og ny behandling er satt til 05.03.2024.

Styringsgruppen for Nasjonalt senter for e-helseforskning har tidligere støttet å prioritere Praksisnett gjennom egenfinansiering, men gitt senterets budsjettsituasjon ser ikke senterleder at det er mulig. Senterleders vurdering er at det er svært krevende å bidra med mer egenfinansiering, samtidig som budsjettet for drift av infrastrukturen er på et minimumsnivå. Senterleder ber om styringsgruppens innspill til hvordan NSE skal forholde seg videre.

Forslag til vedtak

Formuleres i møtet.

Vedlegg

1. Referat fra møte i styringsgruppen i PraksisNett 05.02.2024 (ikke godkjent, unntatt offentlighet)
2. Sammendrag av ROS-analyse Praksisnett

Sammendrag av risikoanalyse av PraksisNett sin IT løsning.
Versjon 5 - 3 januar 2024

Sammendrag
Trusler mot Snow systemets allmennpraksisservere ble identifisert og evaluert i Snow-teammøter høsten 2023. 24 trusler ble identifisert og evaluert. En trussel ble evaluert til potensielt å resultere i et høyt risikonivå som krever implementering av ytterligere sikkerhetskontroller.

Bakgrunn
Bakgrunn for risikovurderingen er granskningen Datatilsynet i Norge utførte våren 2020 i etterkant av et mislykket forsøk på hacking av en Snow boks-server i september 2019. Som et resultat av denne undersøkelsen krevde Datatilsynet en oppdatert risikovurdering av den komplette Snow-løsningen, inkludert de omkringliggende systemkomponentene som blir brukt for å muliggjøre gjenbruk av elektroniske helsejournaldata for sykdomsovervåking, kvalitetsforbedringsarbeid og forskning.

Den forrige versjonen av risikovurderingen slo sammen vurderingen av den frittstående fjernstyringsløsningen. Denne revisjonen oppdaterer systembeskrivelsen, trusler, konsekvenser, risiko og tiltaksplan. Denne versjonen inkluderer også vurdering av løsninger som brukes til å integrere med skybaserte EHR-systemer. Denne versjonen er del av den årlige oppdateringen av risikovurderingen som kreves av Datatilsynet.

Tidligere risikovurderinger av Snow systemet har vært gjennomført i 2015 og deretter oppdatert i 2016, 2020 og 2022. En tidlig risikovurdering av Snow løsningen, før bruk av dedikert maskinvare, ble utført i mai 2011, før installasjon av den første Snow serveren på EPJ-servere på allmennlegekontor i 2012. Rapporter fra disse risikovurderingene er tilgjengelig på norsk.

Konklusjoner og anbefalinger
Trusler mot Snow systemet og driftsløsningen til PraksisNett sitt IT system ble identifisert og evaluert i Snow-team møter høsten 2023.

24 trusler ble identifisert og evaluert. 13 identifiserte trusler kan potensielt føre til alvorlige konsekvenser. 1 av disse truslene, R2 – uautorisert tilgang til EPJ-data, har en sannsynlighet klassifisert som "mulig", som resulterer i høy risiko. Denne trusselen er imidlertid fortsatt hypotetisk siden datauttrekksgrensesnittet (API) ikke er ferdig designet eller implementert ennå. I en fremtidig implementering bør en derfor legge inn ytterligere sikkerhetskontroller, sammenlignet med dagens løsninger, for å redusere sannsynligheten for trusselen.

3 trusler kan potensielt føre til moderate konsekvenser. Sannsynligheten for en av disse truslene (R1 – utilgjengelighet av tjenesten) er sannsynlig, forekommer ofte, og trenger derfor ekstra oppmerksomhet for å unngå å påvirke nytten og brukervennligheten til systemet.

Evaluert risiko for 12 trusler er moderat. Dersom konsekvensdelen for R1 og R2 kunne øke, vil det føre til en uakseptabel høy risiko. Men da risikoen for R1 - utilgjengelighet av en ukritisk tjeneste, er det vanskelig å se hvordan konsekvensdelen kan øke til et slikt nivå. For R2 – Uautorisert tilgang til EPJ-data vil konsekvensdelen kunne øke til kritisk dersom en stor mengde EPJ-data kan eksponeres for uvedkommende. Dette er spesielt et potensial for skybaserte EPJ-systemer.

En økning i sannsynligheten for trussel R2, R9, R19, R21 og R23 kan øke risikoen til et høyt eller kritisk og derfor et ikke-akseptabelt risikonivå. De implementerte kontrollene for trussel R13 – spredning av skadelig programvare, vil redusere sannsynligheten til usannsynlig. Selv om sikkerhetskontroller brukes på R9, R19, R21 og R23, antas det at risikoen ikke vil bli vesentlig påvirket. Disse risikoene bør derfor overvåkes nøye. Tiltaksplanen inkluderer oppgaver for å unngå disse truslene. Trussel R9, fysisk tilgang til Snow-boksen, forblir uendret fordi etablering av kontroller for å redusere denne trusselen er utenfor mulighetene til Snow-teamet, som drifter PraksisNett-forskningsinfrastrukturen. Mange sikkerhetskontroller brukes allerede for å unngå denne risikoen. Instruksjonene for å installere Snow-boksen er imidlertid å plassere serveren der den ikke er tilgjengelig for alle bortsett fra de som har legitim tilgang til Snow-boksen.

R19, «supply-chain» angrep på Snow servere gjennom programvarebiblioteker. Det er vanskelig å se hvordan konsekvensdelen av risikoen vil øke ettersom dataene som er lagret på Snow-boksen blir pseudonymisert og kryptert.

R21, systeminntrenging gjennom programvaresårbarheter (som nulldagssårbarheter) fører til EPJ-dataeksponering. Bruk av SentinelOne (i fremdrift) og ConnectWise automate (planlagt) reduserer sannsynligheten for denne trusselen.

R23, tilgang til identifiserbare EPJ-data i transitt mellom EPJ og DRC. Trussel anses utenfor vårt ansvar. Kryptering av eksport til DRC vil redusere konsekvensen.

Trussel R10 Uautorisert ekstern tilgang til Snow boks: Hvis NHN implementerer de foreslåtte kontrollene som er oppført i tiltaksplanen for risiko R10, vil risikonivået for denne trusselen reduseres ytterligere. De resten av truslene hadde ubetydelige eller moderate potensielle konsekvenser.

Sammendrag av konklusjoner
Risikovurderingen konkluderer med at risikoen knyttet til en potensiell fremtidig trussel er vurdert til å være uakseptabel og trenger implementering av ytterligere sikkerhetskontroller sammenlignet med dagens design av løsning for uttrekk. Hvis sannsynligheten for syv andre trusler øker, vil risikonivået øke til et nivå som krever ytterligere sikkerhetskontroller. Forutsetningen for å bevare et aksepterbart risikonivå for fremtiden avhenger av et tett samarbeid med Norsk helsenett og EPJ leverandørene.