NITO NORGES STØRSTE ORGANISASJON FOR INGENIØRER OG TEKNOLOGER

Direktoratet for e-helse
Robert Nystuen

22. september 2017

Vår ref. 521282/v2 Deres ref. 17/513-7

Bruk av private leverandører i helse- og omsorgssektoren

Viser til invitasjon og takker for muligheten til å gi innspill om informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren. NITO, Norges Ingeniør- og Teknologorganisasjon er Norges største organisasjon for ingeniører og teknologer med ca. 85 000 medlemmer. Omlag 10 000 av disse jobber med IKT, og NITO har et eget IKT-fagutvalg som jobber aktivt med IKT-sikkerhet. Våre medlemmer jobber både i privat og offentlig sektor, og ser problemstillingene som tas opp av direktoratet fra mange sider. Når NITO har et stort engasjement for IKT-sikkerhet er det ikke utelukkende fordi vi er opptatt av norske arbeidsplasser, men fordi vi frykter at helsemyndighetene ikke er tilstrekkelig rustet og forberedt i møtet med et nytt og komplekst fagområde. Stadig større bruk av IKT og skybaserte løsninger krever ny og annen sikkerhetskompetanse.

NITO bes om å adressere to spørsmål. Til spørsmål én om hvordan benytte private underleverandører på en trygg måte, vil vi trekke fram behovet for nasjonale minimumskrav for informasjonssikkerhet, slik beskrevet under. Når det gjelder tjenester som ikke bør overlates til private underleverandører, mener NITO at dette ikke bør gjøres dersom det går utover behovet for å skjerme store mengder helseopplysninger, eller at det går utover nasjonal beredskap og helseberedskap. NITO mener at drift av IKT-infrastrukturen i dag er for sårbar til å settes ut til private underleverandører. Når det gjelder sikkerhetsloven mener NITOs at i de tilfeller hvor det er sammenfall mellom nasjonal eller regional helseberedskap og IKT-systemer, bør det vurderes å klassifisere IKT-systemene etter bestemmelsene om objektsikkerhet. Dette kan også gjelde større datasentre.

IKT må være en del av helseberedskapen

Helsesektoren har et nasjonalt ansvar for helsetilbudet til befolkningen, og for helseberedskapen. IKT er et stadig viktigere element i dette bildet. NITO mener at IKT-systemer i helsesektoren i økende grad er av betydning for den nasjonale og regionale helseberedskap. Dersom IKT unntas fra beredskapstankegangen fremstår det som at man ikke tar beredskapen tilstrekkelig alvorlig.

Helsesektorens forvaltning av informasjon dreier seg videre om konfidensialitet. For eksempel dersom opplysningene skulle finne veien til en avisforside eller benyttes til politisk eller økonomisk utpressing. I tillegg er helseopplysningers integritet livsviktig. Manipulasjon av helseopplysninger vil kunne føre til blant annet feilmedisinering. Økende digitalisering gjør at integriteten i helsesystemene er i ferd med å utgjøre forskjellen på liv og død for den enkelte.

En ny rapport om sikkerhet og sårbarhet utført av Helsedirektoratet understøtter NITOs syn.[1] Den sier at IKT er en innsatsfaktor på linje med vann og strøm og definerer dette som kritisk infrastruktur. Det påpekes også at IKT-trusselbildet endrer seg og inkluderer økt interesse for personopplysninger. Det vises også til manglende forståelse for IKT og informasjonssikkerhet som en del av det totale trusselbildet i helsesektoren, særlig blant ledere.

[1] «Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren», https://helsedirektoratet.no/publikasjoner/overordnede-risiko-og-sarbarhetsvurderinger-for-helse-og-omsorgssektoren

Mer IKT-kompetanse og involvering av tillitsvalgte
IKT-kompetansen må styrkes i besluttende funksjoner, og det må til en økt forståelse for at IKT-sikkerhet koster. Vi ser ofte eksempler på at outsourcing brukes som et argument for at virksomheter skal få fart på digitaliseringen. Underliggende er det ofte et ønske og tro på å spare penger ved å flytte tjenester til lavkostland. Ledelse med manglende kompetanse som utkontrakterer IKT-virksomhet kan ikke nødvendigvis forvente at alt løser seg. Sikkerhetsutfordringer kommer da gjerne tilbake også i form av ekstra kostnader med å rette opp. HSØ-saken illustrerer at man går for fort fram og outsourcer før man har kontroll i eget hus.

NITO mener for øvrig at ved outsourcing eller offshoring skal det være åpenhet mot de tillitsvalgte, og det må informeres om hvilke underleverandører som benyttes i lavkostland, og hvordan disse følges opp og kontrolleres.

Behov for nasjonale tiltak og krav for bruk av private leverandører
HOD ber direktoratet om å foreslå rutiner som sikrer etterlevelse av gjeldende krav. NITO setter spørsmålstegn ved om gjeldene krav er godt nok utformet. NITO mener vesentlige nasjonale rammebetingelsene ikke er på plass. Ut fra dagens rammeverk for informasjonssikkerhet virker oppdragsbeskrivelsen fra HOD for snever.

Etabler et nasjonalt rammeverk for informasjonssikkerhet
NITO mener det er behov for nasjonale sikkerhetskrav som treffer offentlige og private aktører likt, inkludert IKT-tjenestetilbydere og underleverandører. De nasjonale sikkerhetskravene bør ikke baseres på frivillighet, men utformes som minstekrav, med tilhørende kompenserende tiltak og avviksrapportering. Norm for informasjonssikkerhet i helsesektoren benytter seg ikke av slike standardiserte sikkerhetstiltak, men forutsetter i stedet at helseforetakene «finner opp hjulet hver for seg».

Standardiserte minimumskrav har store fordeler. På et overordnet nivå medfører det at samtlige medarbeidere følger de samme sikkerhetskravene, uavhengig av organisatorisk tilhørighet. For sektorens del forenkler det gjenbruk av verktøy, prosedyrer og personell på tvers av virksomheter, samt etablerer et helhetlig og gjennomgående sikkerhetsnivå. Ved at det enkelte foretak slipper å lage «hjemmelagde» sikkerhetskrav og mekanismer kan foretakene bruker mer tid og ressurser på sin kjernevirksomhet.

Helsenorm for informasjonssikkerhet lister opp en rekke krav som den enkelte virksomhet har ansvar for. (Blant annet å utarbeide sikkerhetsstrategi, etablere nivå for akseptabel risiko, gjennomføre risikovurderinger). At den enkelte virksomhetsleder skal gjøre alt dette er for det første litt som at «bukken skal passe havresekken». NITO mener det må oppnevnes konkrete personer som har sikkerhetsansvaret. For det andre mangler det kompetanse på ledernivå til å gjennomføre og prioritere dette. Etter vår erfaring overlater man ikke informasjonssikkerhet til virksomhetsleder selv i sektorer som jobber med sikkerhet hver dag, f.eks. forsvarssektoren.

Hovedmomenter i et nasjonalt rammeverk
Det første spørsmålet fra direktoratet for E-helse gjelder «hvilke kriterier, betingelser og tiltak anser organisasjonenes som nødvendig for å kunne benytte private underleverandører på en trygg og ansvarlig måte»? Dette dekkes gjennom å etablere et nasjonalt rammeverk som styrker og standardiserer følgende punkter:

1. Fysisk sikkerhet. Passiv sikring av bygninger, rom og datasentre.
2. Personell. Bakgrunnssjekk av alt nøkkelpersonell.
3. Anskaffelser. Krav om IKT-sikkerhetskompetanse ved anskaffelser, standardiserte minstekrav til IKT-sikkerhet i kontraktene.

4. Teknisk IKT-sikkerhet. Overordnet sikkerhetspolicy, sikker arkitektur/design, sikker konfigurasjon, sikker koding, sikkerhetslogging.
5. Prosesser og styringssystemer. Sikker IKT-drift og -utvikling, hendelseshåndtering og gjenoppretting.
6. Helseberedskap. IKT-understøttelse av kritiske helsetjenester i både fred, krise og krig.

Nærmere om punktene i nasjonalt rammeverk

1. Fysisk sikkerhet
Det bør etableres minstekrav til sikkerheten i fysiske bygningsmasser der det er sensitivt IKT-utstyr, eller hvor det behandles sensitive opplysninger. Dette innebærer krav til etablering og til nivå på adgangskontroll. Vurder inndeling av datasentre, rack og serverrom etter risikokategori; se punkt om "Intern-inndeling av IKT-komponenter etter risiko" under Teknisk IKT-sikkerhet.

2. Personell
Det bør etableres minstekrav til bakgrunnssjekking av personell som skal ha spesielt utvidede tilganger. Dette gjelder bl.a. IKT-administratorer, forvaltere av IKT-kryptosystemer og forvaltere av adgangskontrollsystemer. Det betyr at det må være dedikerte personer hos leverandør som får tilgang til aktuelle data.

3. Anskaffelser
Det må innarbeides solide standardklausuler i kontrakt om IKT-sikkerhet, med henvisninger til både personell, prosesser og teknologi (PPT). Det er en selvfølge at det etableres databehandleravtaler. I denne sammenheng må det stilles forventinger, og man må hensynta GDPR (fra mai 2018). NITO mener kontrakten må sørge for at serverne er fysisk plassert i Norge og at dataeier har rett til revisjoner som ikke er varslet i forkant.

Det bør også være et krav at kontrakter vurderes av personell med IKT-sikkerhetskompetanse, enten man har dette i den anskaffende virksomheten, eller støtter seg på slik kompetanse i departement eller direktorat. Spesielt viktig er det at man krever "sikker programvareutvikling" når man kjøper ny eller vedlikeholder gammel programvare. I dette ligger både sikker koding og en forpliktelse om retting av sikkerhetsproblemer i hele applikasjonens levetid.

4. Teknisk IKT-sikkerhet
Generelt bør man etablere felles retningslinjer for sikkerhetspolicy, sikker arkitektur/design, sikker konfigurasjon, sikker koding og sikkerhetslogging.

Det må sikres at det ikke gis tilgang til data og IT-systemer som inneholder beskyttet informasjon. Da må det avklares om man har behov for å lagre de dataene man har, hvordan de lagres osv. Videre må det være dedikerte terminaler hos leverandør, all aktivitet i serverne skal registreres, også lesetilgang. Linjene som benyttes mellom leverandør/dataeier og servere skal være kryptert «på øverste nivå» og dataeier skal ha eierskap til, og styring med, krypteringsnøklene.

<u>Spesielt om fjernaksess</u>
Dagens nettverksteknologi tillater kopiering av enorme mengder data på kort tid, selv over en bredbåndsforbindelse i et privat hjem. Man bør derfor ikke basere seg på ubegrenset tilgang på nettverksnivå, men i stedet tilby virtuelle arbeidsflater med svært begrensede muligheter for å kopiere ut (potensielt sensitive) data.

For utenlandske leverandørers tilgang til fjernstyring av medisinsk utstyr og applikasjoner, eksempelvis i forbindelse med vedlikehold eller feilretting, bør aksessen snevres inn til forhåndsgodkjente, korte tidsintervaller med innsnevrede brukerrettigheter. Aller helst bør slik tilgang overvåkes av personell lokalisert i helseforetakets bygningsmasse; i alle fall dersom brukerrettighetene er av et visst omfang. Tidsintervallene for

vedlikehold bør autoriseres i samsvar med bruksmønsteret for helseforetakets øvrige aktiviteter - både planlagt og akutt, slik at man unngår forstyrrelser på medisinsk utstyr (og tilhørende IKT-støttefunksjoner) som er i bruk. Ideelt bør helseforetakene få etablert en leverandørportal med virtuelle arbeidsflater, hvor de beskrevne begrensningene er normalen.

* Dette tiltaket vil ikke hindre en kompetent hacker å utføre stor skade, men begrenser risikoen for uhell og vandalisering ved ordinært vedlikehold.

Intern-inndeling av IKT-komponenter etter risiko

En viktig forutsetning for å kunne håndtere økt risiko i IKT-systemer, er effektiv filtrering, sikkerhetslogging og hendelseshåndtering. Dette er komplekst i seg selv, men vesentlig enklere i en ryddig IKT-arkitektur.
NITO anbefaler derfor en sikkerhetskartlegging med sikte på å identifisere sammenhengene mellom helseforetakenes medisinske funksjoner og IKT-tilknyttet medisinsk utstyr, herunder skadepotensiale for helsepersonell, pasienter og medisinske funksjoner / helsetilbud ved manipulasjon eller bortfall. Kartleggingen bør også omfatte IKT-arkitekturmessige avhengigheter, eksempelvis IKT-støttesystemer og fysiske/virtuelle servere.

Deretter bør man etablere risikonivåer i samsvar med den medisinske aktiviteten utstyret understøtter, både med tanke på tilgjengelighet, integritet og konfidensialitet. Til slutt bør sensitive IKT-komponenter plasseres i dedikerte fysiske og virtuelle nettverkssoner med robust perimeterbeskyttelse, kategorisert etter risikonivå.

Kryptografisk integritetsbeskyttelse av alle helsedata

For å motstå eller detektere manipulasjon av helsedata - antakeligvis den viktigste grunnsteinen i fremtidens helse-IKT, må det etableres kryptografiske løsninger som signerer og verifiserer helsedata på et akseptabelt tillitsnivå. Frem til slik beskyttelse er på plass, kan man i prinsippet ikke vite om det er det siste dataviruset, innsideren hos IKT-driftsleverandøren eller legen som har foreskrevet behandlingen og medisinene i IKT-systemet. En kryptografisk signatur sporer opplysningene til den maskinen som har utført den.
NITO mener derfor at helsesektoren må etablere minstekrav til, og IKT-løsning for, elektronisk signering av helsedata i helseforetakene og Nasjonalt Helsenett (objektbasert kryptografisk signering og verifikasjon). Spesielt viktig er maskin-til-maskin (m2m)-kommunikasjon som i eksempelet med "støttesystem for medisinering".

NITO er kjent med at dagens helseløsninger ikke har slik støtte. Bakgrunnen for å fremme et slikt krav er "høna eller egget"-dilemmaet; uten et backend-system for signaturer kommer det neppe støtte i frontend-systemer.

5. Prosesser og styringssystemer

Det må etableres sikker IKT-drift og -utvikling, sikker hendelseshåndtering og sikker gjenoppretting. Hendelseshåndtering og gjenoppretting må etableres i harmoni med relevante medisinske funksjoner og generell beredskap i foretaket. Herunder planverk og prosedyrer for eskalering av hendelser, samt ekstern bistand.

Spm 2: Tjenester som ikke bør overlates til underleverandører

NITO mener tjenester ikke bør overlates til private underleverandører dersom det går utover behovet for å skjerme store mengder helseopplysninger eller at det går utover nasjonal beredskap og helseberedskap.

NITO mener derfor at drift av IKT-infrastrukturen i dag er for sårbar til å settes ut til private underleverandører. Man må ha kontroll over driften, og gitt dagens situasjon betyr det at man må ha eget personell som drifter IKT-infrastrukturen. Settes dette ut i dag vil vi ikke vite hva leverandøren gjør.

Outsourcing innebærer ofte offshoring fordi underleverandører må spare kostnader. Bruk av underleverandører kan gi ansvarspulverisering mellom utførende leverandør og dataeier. Det gir lavere

kontroll.

Spesielt om sikkerhetsloven

Sikkerhetsloven tar for seg både informasjon og objekter av nasjonal betydning eller med nasjonalt skadepotensiale. Helseopplysninger er per definisjon individuelle, og omfattes derfor normalt ikke av bestemmelsene om skjerming iht sikkerhetsloven. For objekter stiller det seg annerledes:
"Et skjermingsverdig objekt er eiendom, område, bygning, anlegg, transportmiddel eller materiell, som kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, om det blir utsatt for sikkerhetstrusler. Objekter kan være et direkte eller et indirekte mål."
NITOs syn er at i de tilfeller hvor det er sammenfall mellom nasjonal eller regional helseberedskap og IKT-systemer, bør det vurderes å klassifisere IKT-systemene etter bestemmelsene om objektsikkerhet. I tillegg bør man vurdere datasentre av en viss størrelse når disse understøtter større helseforetak.

Med vennlig hilsen

Trond Markussen
President

Steinar Sørlie
Generalsekretær