Landstingsstyrelsens förvaltning
Informationssäkerhet

TJÄNSTEUTLÅTANDE
2014-02-18

LS 1311-1456

Handläggare:
Vesna Lucassi

Landstingsstyrelsens
arbetsutskott

Förslag på kort- och långsiktiga lösningar för bättre och tydligare IT-säkerhet

Ärendebeskrivning

Arbetsutskottet gav i slutet av år 2013 landstingsdirektören i uppdrag att skyndsamt återkomma med förslag på kort- och långsiktiga lösningar för om möjligt bättre och tydligare IT-säkerhet. Ärendet behandlar förslag till lösningar enligt detta uppdrag.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 18 februari 2014

Förslag till beslut

Arbetsutskottet föreslår landstingsstyrelsen besluta

att uppdra åt landstingsdirektören att genomföra en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras gällande IT-säkerhetsåtgärder och hantering av IT-säkerhetsrelaterade incidenter

att uppdra åt landstingsdirektören att inrätta en övergripande funktion med uppgift att stödja landstingets verksamheter med att upptäcka och hantera IT-säkerhetsrelaterade hot och incidenter

att uppdra åt landstingsdirektören att säkerställa att utökade IT-säkerhetskrav, såsom separering av nätverkstrafik, ställs i den nya plattformen för SLLnet samt för att skyddet i den gemensamma arbetsplatsplattformen stärks

att uppdra åt landstingsdirektören att utreda central teknisk lösning för att upptäcka avvikelser och potentiella hot i landstingets nätverk och kritiska IT-system

att uppdra åt landstingsdirektören att i budget för år 2015 och för planåren 2016-2017 beakta kostnader i enlighet med föreslagna åtgärder.

Förvaltningens förslag och motivering

Sammanfattning
Arbetsutskottet gav den 5 november 2013 landstingsdirektören i uppdrag att skyndsamt återkomma till arbetsutskottet med förslag på kort- och långsiktiga lösningar för om möjligt bättre IT-säkerhet (LS 1311-1456). Stockholms läns landsting står inför stora satsningar både inom trafik och vård med höga krav på informations- och IT-säkerhet. För att uppnå satta mål behöver landstinget successivt öka sin IT-säkerhetsberedskap. Landstingsdirektören har genomfört en utredning och redogör i detta tjänsteutlåtande för lösningar och förslag gällande tydligare styrning, stärkt organisation, förbättrade processer samt stärkt skydd i nätverk och arbetsplatsplattform.

Bakgrund
Informationssäkerhet är idag en stor utmaning, både nationellt och globalt. Den snabba IT-utvecklingen, komplexa systemberoenden och ökad informationsdelning påverkar alla samhällsprocesser och ställer allt högre krav på informationshanteringen. Samtidigt innebär den höga förändringstakten och behovet av exponering mot internet att hotbilden ständigt förändras. Under de senaste åren har hotbilden kopplad till informationssäkerhet kraftigt ökat i samhället. Både dagens och framtida IT-angrepp kommer från resursstarka och kunniga aktörer som har uttalade mål och syften med sina angrepp. I dag finns ett reellt hot mot samhällsviktig verksamhet, och kritisk infrastruktur förväntas bli särskilt utsatt. Syftet är ofta att skaffa sig informationsöverläge genom inhämtning av t.ex. skyddsvärda uppgifter och forskningsresultat. Hotbilden beror även på omvärldshändelser och på hur verksamheter agerar i olika sammanhang. Exempelvis introducerar mobila enheter, som används för att få tillgång till system och molndata via webbläsarbaserade och mobila applikationer, nya säkerhetshot i verksamheters nätverk som behöver hanteras. Under de senaste åren har verksamheten hos olika samhällsaktörer påverkats eller slagits ut till följd av sårbarheter, IT-angrepp och skadlig kod och de ekonomiska konsekvenserna av incidenterna ökar.

Stockholms läns landsting står inför stora satsningar både inom trafik och inom vård. Ambitionerna i Framtidsplan för hälso- och sjukvården, Regionalt trafikförsörjningsprogram för Stockholms län och den regionala digitala agendan, en strategi som samordnar åtgärder på IT-området inom

bland annat säkerhet, infrastruktur, tillgänglighet och användbarhet, ställer höga krav på informations- och IT-säkerheten. För att uppnå satta mål och samtidigt säkerställa patientsäkerheten och patientintegriteten i en komplex och integrerad miljö där IT är verksamhetskritiskt för behandlingar i vården, liksom för andra delar av landstingets verksamheter, krävs att landstinget successivt ökar sin förmåga att hantera IT-säkerhetsrelaterade hot och incidenter. Viktiga framgångsfaktorer är att utarbeta strategier och förändra både teknik och processer som kan ge insikt om aktuell hotbild och aktuella risker i landstingets verksamheter. Avgörande är också att landstinget, i samverkan med andra samhällsaktörer, stärker sin förmåga att hantera incidenter när de väl uppstår.

I samband med att landstingsstyrelsens arbetsutskott fick information om vårdens IT-säkerhet beslutade utskottet den 5 november 2013 (LS 1311-1456) om uppdrag till landstingsdirektören att skyndsamt återkomma till arbetsutskottet med förslag på kort- och långsiktiga lösningar för om möjligt bättre och tydligare IT-säkerhet. Dessa redovisas nedan.

Överväganden
Landstingdirektören har utrett möjligheterna att åstadkomma en bättre och tydligare IT-säkerhet. I de överväganden som har gjorts har målet att förverkliga den digitala agendan, hänsyn till patientsäkerhet och patient-integritet, landstingets policy och riktlinjer för informationssäkerhet samt administrativ förenkling varit vägledande. Arbetet har skett i dialog med berörda förvaltningar och bolag.

För att hålla en god IT-säkerhetsberedskap som är i paritet med morgondagens hotbild behöver landstingets förmåga öka inom områdena styrning, organisation och kompetens samt processer och teknologi.

Förslag på lösningar gällande styrning
En omfattande och komplex IT-miljö med gränsöverskridande risker och hot kräver ökad styrning, sammanhållen struktur, standardiserade processer samt förmåga att göra riskavvägningar utifrån ett landstings-övergripande perspektiv. En översyn av roller, ansvar och beslutsmandat behöver genomföras så att tydliga beslutskedjor finns etablerade för t.ex. upptäckt, eskalering, åtgärder och kommunikation gällande IT-säkerhets-åtgärder och incidenthantering. I översynen bör även ingå att föreslå beslutsmandat att snabbt stänga ner nätverkskopplingar som innebär en allvarlig IT-säkerhetsrisk.

Förslag på lösningar gällande organisation och kompetens
Det finns idag ett framväxande behov av specialistkompetens gällande IT-säkerhet. Exempel på uppgifter där behov av stöd finns är krisagerande vid allvarliga IT-incidenter (t.ex. skadlig kod som berör flera verksamheter), insamling och analys av data, återställande av system, samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av inträffade incidenter etc. Bedömningen är att sådana insatser skulle kunna förenklas genom inrättandet av en landstingsövergripande funktion med uppgiften att stödja verksamheterna med att upptäcka och hantera IT-säkerhets-incidenter. På kort sikt föreslås ett inrättande med stödjande uppgift, på längre sikt bör funktionen även arbeta operativt med att identifiera och agera för åtgärdande av akuta brister avseende säkerheten i IT-miljön i landstinget , t.ex. att genomföra tekniska analyser och att samla in bevis vid potentiella dataintrång.

Förslag på lösningar gällande processer
Förvaltningen föreslår på lång sikt att en central teknisk lösning införs för att upptäcka avvikelser mot normalt beteende dvs. potentiella hot, i landstingets nätverk och kritiska IT-system. Den överblick som en samlad process ger skapar möjlighet till prioriteringar utifrån verksamheternas behov. En utredning bör genomföras skyndsamt med målet att ta reda på förutsättningarna för en sådan lösning.

Förslag på lösning gällande teknologi
Stockholms läns landsting har inrättat ett nätverk, SLLnet, för att på konkurrensneutrala villkor erbjuda ett transportnät till parter, t.ex. vårdgivare, som genom avtal har behov av att kommunicera med och leverera data till Stockholms läns landsting. SLLnet förvaltas idag av SLL IT. För att ha bättre förutsättningar att möta utmaningarna i landstingets verksamheter krävs förändringar i landstingets strategier för nättrafik och datahantering. Existerande avtal för SLLnet upphör att gälla den 31 december 2015, och existerande hårdvaru- och konsultavtal för de lokala nätverken (de till SLLnet anslutande näten) upphör år 2014. Arbetet med att planera nya upphandlingar pågår. Därför föreslås att ytterligare säkerhetsprinciper och säkerhetskrav i den framtida plattformen skyndsamt identifieras och klarläggs. Möjligheterna att ytterligare separera nätverkstrafik bör exempelvis övervägas, liksom möjligheten till en ökad separation av hårdvara samt integritetskänsliga data som är kopplade till kritiska system. Separation av datatrafik medför att spridning av skadlig kod och/eller IT-angrepp kan begränsas på ett enklare sätt i händelse av incident. Behov finns även att på sikt uppgradera befintliga lokala nätverk, t.ex. på sjukhusen, med nya tekniska lösningar och ökad separation av nätverkstrafik.

För närvarande pågår det ett arbete med att införa en enhetlig PC-arbetsplats vid de stora sjukhusen i landstinget. På kort sikt föreslås att skyddet i den gemensamma arbetsplatsplattformen stärks ytterligare i syfte att ta höjd för den ökande hotbilden. Införande av en standardiserad IT-arbetsplats med förstärkt IT-säkerhetsskydd bör på sikt även ske för resterande arbetsplatser inom landstinget, i syfte att möjliggöra ett snabbt agerande vid potentiella IT-säkerhetsincidenter kopplade till IT-arbetsplatser.

På sikt bör även verktyg och rutiner införas gällande en standardiserad och centraliserad användarautentisering som är kopplad till den kommande nätverksstrukturen.

Förslag på omedelbara åtgärder
Landstingsdirektören föreslås få i uppdrag att genomföra en översyn i syfte att etablera tydliga beslutskedjor gällande IT-säkerhet samt att skyndsamt inrätta en stödjande funktion med uppgiften att upptäcka och hantera IT-säkerhetsrelaterade hot och incidenter. Landstingsdirektören föreslås även få i uppdrag att säkerställa att utökade IT-säkerhetskrav, såsom separering av nätverkstrafik, ställs i upphandling av ny nätverkslösning, då existerande avtal för SLLnet upphör att gälla, samt för att skyddet i den gemensamma arbetsplatsplattformen stärks. Landstingsdirektören föreslås slutligen få i uppdrag att utreda en central teknisk lösning för att upptäcka avvikelser och potentiella hot i landstingets nätverk och kritiska IT-system.

Ekonomiska konsekvenser av beslutet

Omedelbara åtgärder
De föreslagna kortsiktiga uppdragen bedöms i nuläget rymmas inom tilldelad budgetram för år 2014. Avseende uppdraget gällande uppbyggnaden av en stödjande funktion för att upptäcka och hantera IT-säkerhetsrelaterade hot och incidenter, uppskattas detta medföra kostnader motsvarande cirka 5 miljoner kronor för år 2015 och framåt. Uppdraget gällande SLLnet beräknas i nuläget medföra utökade kostnader motsvarande cirka 85 miljoner kronor för åren 2015-2017. Kostnaderna föreslås beaktas i ordinarie budgetprocess för 2015 samt planår 2016-2017. Kostnaderna för föreslagna säkerhetsregleringar bör ställas i relation till de kostnader som uppstår för IT-säkerhetsincidenter utan regleringar, t.ex. driftavbrott till följd av ett större utbrott av skadlig kod eller dataintrång. Föreslagna lösningar kan förväntas ha en preventiv verkan på verksamhetens budget samt på andra negativa konsekvenser som kan uppstå i samband med allvarliga IT-relaterade incidenter.

Långsiktiga förslag
Föreslagna lösningar på sikt uppskattas medföra ytterligare kostnader under åren 2017-2020. Omfattning och ekonomiska konsekvenser bör utredas och säkerställas.

Miljökonsekvenser av beslutet

I enlighet med landstingets Miljöpolitiska program 2012-2016 har hänsyn till miljön beaktats och slutsatsen är att det inte är relevant med en miljökonsekvensbedömning i detta ärende.

Toivo Heinsoo
Landstingsdirektör

Anders Nyström
Biträdande förvaltningschef