Landstingsstyrelsens förvaltning
SLL Informationssäkerhet

TJÄNSTEUTLÅTANDE
2015-09-09

LS 1404-0548

Handläggare:
Vesna Lucassi

Landstingsstyrelsens
innovationsberedning

Översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras för IT-säkerhetsåtgärder och hantering av IT-säkerhetsrelaterade incidenter

Ärendebeskrivning

Landstingsstyrelsen gav i slutet av år 2013 landstingsdirektören i uppdrag att genomföra en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras gällande it-säkerhetsåtgärder och hantering av it-säkerhetsrelaterade incidenter. Uppdraget innebar att utreda förutsättningarna för en ambitionshöjning inom informationssäkerhets-området. Detta tjänsteutlåtande utgör återrapportering till landstingsstyrelsen efter översynen.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 9 september 2015
Översyn av roller och ansvar gällande hantering av it-säkerhetsincidenter

Förslag till beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att godkänna översynen inklusive förslag om beslutsmandat

att ändra riktlinjerna för informationssäkerhet inom Stockholms läns landsting enligt landstingsdirektörens tjänsteutlåtande

att uppdra åt landstingsdirektören att utarbeta en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter enligt landstingsdirektörens tjänsteutlåtande

att uppdra åt landstingsdirektören att ta fram en plan för genomförande av övning gällande hantering av it-säkerhetsincidenter.

Förvaltningens förslag och motivering

Sammanfattning
Landstingsdirektören har utrett förutsättningarna för en effektiv hantering av it-säkerhetsrelaterade incidenter inom landstinget. It-säkerhets-incidenter kan överskrida vårdgivargränser men även externa organisatoriska och nationella gränser. En tydlig process för styrning av it-säkerhetsincidenter utgör en förutsättning för att en ambitionshöjning inom informationssäkerhetsområdet ska kunna genomföras. Efter genomförd översyn föreslås nu att åtgärder enligt förslag genomförs. En stärkt styrning samt gemensamma processer understödjer implementeringen av framtidens hälso- och sjukvård och kollektivtrafik.

Bakgrund
Landstingsstyrelsen gav i slutet av år 2013 landstingsdirektören i uppdrag att skyndsamt återkomma med förslag på kort- och långsiktiga lösningar för om möjligt bättre it-säkerhet, LS 1311-1456. Uppdraget innebar att utreda förutsättningarna för en ambitionshöjning inom informationssäkerhetsområdet. Landstingsstyrelsen gav därefter landstingsdirektören i uppdrag att genomföra en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras gällande it-säkerhetsåtgärder och hantering av it-säkerhetsrelaterade incidenter. En utredning av den övergripande styrningen gällande it-säkerhetsincidenter inom landstinget har genomförts. Utredningen har beaktat de organisatoriska förändringar som genomförs för tillfället liksom plan krisberedskap i Stockholms läns landsting, LS 1406-0750.

Överväganden
It-säkerhetsincidenter kan överskrida vårdgivargränser men även externa organisatoriska och nationella gränser. För att hantera sådana händelser effektivt och konsekvent finns det ett behov av landstingsövergripande process för styrning av it-säkerhetsincidenter och samordnad hantering it-säkerhetsrelaterade händelser.

I översynen konstateras att it- och informationssäkerhetsincidenter inom landstinget ska hanteras i enlighet med gällande krisberedskapsplan för Stockholms läns landsting. Det innebär att eskalering och rapportering av informations-säkerhetsincidenter ska ske enligt samma process som andra verksamhetsstörningar. Det är nödvändigt att verksamheterna har

inarbetade processer och rutiner för upptäckt, eskalering, beslut om åtgärder och kommunikation av incidenter och att informationssäkerhets-incidenter integreras i dessa processer.

Samtidigt behöver den övergripande styrningen av it-säkerhetsincidenter tydliggöras och stärkas. Gränssnitt behöver etableras mellan framför allt tjänsteman i beredskap, förvaltningar och bolags beredskaps-funktioner och krisledningsgrupper samt den nya funktion som inrättats för att upptäcka och hantera it-säkerhetsrelaterade hot och incidenter, SLL SOC.

Med utgångspunkt i ett antal identifierade typfall, det vill säga oönskade händelser, samt i ett antal styrande dokument identifierades ett antal nyckelroller som kan komma att behöva samverka i händelse av en it-säkerhetsincident samt vilken roll som bör ha beslutsmandat i de olika stegen. Landstingsdirektören kommer att inarbeta beskrivningarna gällande nyckelroller och ansvar enligt kapitel 5 i rapporten Översyn av roller och ansvar gällande hantering av it-säkerhet i till riktlinjerna för informationssäkerhet hörande tillämpningsanvisningar, samt i riktlinjerna där så är erforderligt.

Översynen visar vidare brister i nödvändiga beslutsmandat. Det föreslås att mandat tydliggörs gällande följande:

- mandat att besluta om kontroller
- mandat att besluta om att stänga anslutningar
- mandat att besluta om it-säkerhetsåtgärder

Översynen visar att landstingsdirektörens liksom förvaltnings- och bolagschefers beslutsmandat behöver stärkas och tydliggöras. Bland annat föreslås att landstingsdirektören, eller den som landstingsdirektören utser, beslutar om kontroll ska ske av loggar i central it-infrastruktur i syfte att identifiera och oskadliggöra hot mot landstingets IT-miljö eller informationstillgångar. Landstingsdirektören, eller den som landstingsdirektören utser, föreslås fastställa instruktioner för hur sådana kontroller ska genomföras, och landstingets förvaltningar och bolag samt privata vårdgivare och andra som genom avtal är bundna av dessa riktlinjer föreslås bistå i detta arbete.

Gällande mandat att besluta om avstängning av anslutningar mellan system föreslås bland annat att beslutsmandat även ges till tjänsteman i beredskap, TiB, i samråd med berörd förvaltnings-/bolagschef samt landstingets chefläkare.

Gällande mandat att besluta om it-säkerhetsåtgärder föreslås bland annat att beslutsmandat ges till även landstingsdirektören i de fall fler än en verksamhet påverkas.

Mandaten enligt kapitel 6 i rapporten Översyn av roller och ansvar gällande hantering av it-säkerhet föreslås inarbetas i till riktlinjerna hörande tillämpningsanvisningar samt i riktlinjerna där så är erforderligt. Härutöver föreslås att landstingsdirektören utarbetar en kontrollplan för uppföljning/revision.

Mot bakgrund av ovanstående föreslås att landstingsdirektören ges i uppdrag att även justera reglerna i riktlinjerna för informationssäkerhet i Stockholms läns landsting gällande kontrollåtgärder, nuvarande pkt [6.9.1]-[6.9.4], samt för incidenthantering, nuvarande pkt [12.1.1]-[12.1.4], enligt förslag i kapitel 7 i rapporten Översyn av roller och ansvar gällande hantering av it-säkerhet.

Några av de största utmaningarna gällande hantering av informations-säkerhetsincidenter handlar om att förändra arbetssätt. En av dem gäller klassificering av it-säkerhetsincidenter. Översynen har visat att det inom landstinget förekommer olika modeller för hur informationssäkerhets-incidenter ska klassas. Behov finns därför att ta fram en landstings-gemensam klassificeringsmodell för bedömning av skadeverkan och prioritering. Det föreslås att en sådan fastställs av landstingsdirektören i en till riktlinjerna hörande tillämpningsanvisning.

Slutligen föreslås att övningar genomförs med syftet att träna samarbete mellan landstingets olika verksamheter i hanteringen av informationssäkerhetsincidenter. Inte minst är det viktigt att träna kommunikationsåtgärder vid olika slags oönskade händelser.

Ekonomiska konsekvenser av beslutet

Det uppstår inga ekonomiska konsekvenser av beslutet. Kostnaderna för ovan beskrivna aktiviteter ryms inom ordinarie budget. Kostnader för eventuellt genomförande av övningar gällande hantering av informationssäkerhets-incidenter föreslås hanteras inom tilldelad årlig budgetram.

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
Direktör strategisk IT i SLL

Översyn av roller och ansvar gällande hantering av it-säkerhetsincidenter

LS 1404-0548

Landstingsstyrelsens förvaltning
SLL Säkerhet och beredskap
Box 22550, 104 22 Stockholm
Telefon: 08-737 25 00

Stockholms läns landsting

Landstingsstyrelsens förvaltning

Handläggare: Vesna Lucassi
SLL Informationssäkerhet

Innehållsförteckning

1 Sammanfattning 3
2 Inledning 4
3 Behovsanalys 6
4 Roller och ansvar 8
5 Övergripande process 10
6 Behov av justering av mandat 15
7 Förslag på justering i befintliga riktlinjer 19
8 Slutsatser och rekommendationer 22
Referenser 24
Dokumenthistorik 24

1 Sammanfattning

Landstingsstyrelsen gav landstingsdirektören i uppdrag att genomföra en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras gällande it-säkerhetsåtgärder och hantering av it-säkerhetsrelaterade incidenter.

Syftet med översynen är att på ett övergripande sätt beskriva behoven för att uppnå en effektiv hantering av it-säkerhetsrelaterade incidenter inom landstinget. En tydlig process för styrning och tydliga beslutskedjor utgör en förutsättning för att en ambitionshöjning inom området ska kunna genomföras.

Utredningen konstaterar att it- och informationssäkerhetsincidenter inom landstinget ska hanteras i enlighet med gällande krisberedskapsplan för landstinget. Det innebär att eskalering och rapportering av informations-säkerhetsincidenter ska ske enligt samma process som andra verksamhets-störningar. Dock behöver den övergripande styrningsprocessen förtydligas genom att gränssnitt etableras mellan framför allt tjänsteman i beredskap, förvaltningar och bolags beredskapsfunktioner och krisledningsgrupper samt säkerhetsoperativt center, SLL SOC.

Översynen av roller och ansvar genomfördes med utgångspunkt i en scenarioanalys av oönskade it-säkerhetshändelser. Viktiga roller och ansvarsområden som är nödvändiga för att it-säkerhetsincidenter ska kunna hanteras effektivt har identifierats.

Inom ramen för etableringen av den landstingsövergripande funktionen SLL SOC har en instruktion för hantering av it-säkerhetsincidenter tagits fram. I dessa beskrivs nödvändiga roller och ansvar för hantering av it-säkerhetsincidenter samt vilken roll som bör ha beslutsmandat i de olika stegen. Instruktionerna har genomlysts och korrigerats i förhållande till den övergripande styrprocessen där så har krävts.

Utredningen föreslår att:

- Ansvars- och rollbeskrivningarna liksom reglerna för kontrollåtgärder och för incidenthantering i riktlinjer för informationssäkerhet inom Stockholms läns landsting och tillhörande tillämpningsanvisningar uppdateras i syfte att åstadkomma ökad tydlighet
- nya mandat ges gällande beslut om kontroller, beslut om att stänga anslutningar, beslut om it-säkerhetsåtgärder samt att kontrollplan för uppföljning/revision tas fram
- en landstingsgemensam klassificeringsmodell för bedömning av skade-verkan och prioritering av informationssäkerhets-incidenter tas fram och fastställs av landstingsdirektören i en tillämpningsanvisning
- övningar av hantering av informationssäkerhetsincidenter genomförs.

2 Inledning

2.1 Bakgrund

Landstingsstyrelsen gav i slutet av år 2013 landstingsdirektören i uppdrag att skyndsamt återkomma med förslag på kort- och långsiktiga lösningar för om möjligt bättre it-säkerhet [1]. Uppdraget innebar att utreda förutsättningarna för en ambitionshöjning inom informationssäkerhetsområdet.

Landstingsstyrelsen gav därefter landstingsdirektören i uppdrag att genomföra en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras gällande it-säkerhetsåtgärder och hantering av it-säkerhetsrelaterade incidenter.

En översyn av den övergripande styrningen gällande it-säkerhetsincidenter inom landstinget har genomförts. Utredningen har beaktat de organisatoriska förändringar som genomförs för tillfället och som syftar till att skapa en mer sammanhållen ledning och ägarstyrning i landstinget [2].

Utredningens förslag redovisas i denna rapport.

2.2 Syfte

Utredningens syfte är att klargöra förutsättningarna för en effektiv hantering av it-säkerhetsrelaterade incidenter inom landstinget. En tydlig process för styrning av it-säkerhetsincidenter och tydliga beslutskedjor utgör en förutsättning för att en ambitionshöjning inom området ska kunna genomföras. En stärkt styrning samt gemensamma processer understödjer implementeringen av framtidens hälso- och sjukvård och kollektivtrafik.

2.3 Avgränsning

Översynen tar inte höjd för lokala roller och mandat som kan förekomma i förvaltningar och bolag. Den tar sin utgångspunkt i viktiga roller och mandat som är nödvändiga på övergripande nivå för att it-säkerhetsincidenter ska kunna hanteras på ett effektivt sätt inom Stockholms läns landsting.

2.5 Begrepp

Avvikelse	Händelse som utgör tänkbart brott mot informationssäkerhetsregelverk, säkerhetsåtgärder som inte fungerar som tänkt, eller händelser som kan utgöra hot mot landstingets informationstillgångar. Avvikelser behöver följas upp för att kunna arbeta med ständiga förbättringar av det systematiska informationssäkerhets-arbetet.
Incidenthantering	Process för att hantera incidenter.
Informationssäkerhetsincident	Informationssäkerhetsincidenter är oavsiktliga eller avsiktliga händelser som hotar landstingets informationstillgångar och bedöms leda till allvarliga konsekvenser. Exempel på sådana incidenter är brott mot sekretessen, allvarliga driftavbrott, dataintrång eller obehörigt användande av information. Incidenter kan även vara förlust av dator eller lagringsmedia.

3 Behovsanalys

Ett antal hypotetiska typfall har tagits fram för att stödja översynen. Dessa har sedan analyserats ur olika perspektiv. Ett av perspektiven var förutsättningar för en effektiv incidenthantering, det vill säga möjlighet att snabbt kunna starta en it-säkerhetsutredning och möjlighet att fullt ut genomföra en it-säkerhetsutredning. Ett annat viktigt perspektiv var förutsättningar för att stärka it-säkerheten, det vill säga möjlighet att utföra it-säkerhetsåtgärder på lokal och landstingsövergripande nivå och möjlighet att utföra kontroller på en landstingsövergripande nivå.

Några av de hypotetiska typfallen som arbetats fram beskrivs nedan. De bygger bland annat på rapporter, exempelvis hot- och riskrapporten Informationssäkerhet– trender 2015 [3], scenariorapporter [4] och erfarenheter från tidigare incidenter. Typfallen redovisas utan inbördes ordning.

3.1 Exempel på typfall

Under ett angrepp/dataintrång behöver ofta flera roller vara inkopplade för att kunna ge mandat om utredning och säkerhetshöjande åtgärder. Detta avsnitt ger exempel på olika typer av situationer där roller, ansvar och beslutsmandat tydliggörs.

3.1.1 Obehörig åtkomst med stulet användarkonto

Detta typfall innebär att en behörig användare får sitt användarkonto stulet. En utredning kan omfatta analys av flera loggar från olika system för att fastställa händelseförlopp.

3.1.2 Illasinnad kod[1]

Detta typfall omfattar angrepp genom att skadlig kod har en negativ påverkan på information och system exempelvis skadlig kod som raderar eller krypterar filer på en gemensam filserver. Incidenthantering kan i vissa fall komma att omfatta åtgärder som att stänga ned nätverkskopplingar för att minska smittospridningen.

3.1.3 Externa angreppsförsök

Detta typfall innebär angrepp där angripare är helt externa, exempelvis från andra länder utan direkt åtkomst till landstingets nätverk. Angripare kan komma att testa sig fram genom flera angreppsvägar, och kan i ett skede försöka gissa lösenord till en tjänst för att i nästa skede försöka hitta sårbarheter i

[1] Kod som vid exekvering orsakar avsiktlig störning eller skada – SIS HB 550 utgåva 3

andra. I detta typfall är det viktigt att kunna upptäcka ett pågående angrepp tidigt, exempelvis genom övervakning av information från flera olika datakällor.

3.1.4 Sårbarhet i server

Om en server har en utdaterad mjukvara med en känd sårbarhet kan detta leda till en situation där servern innebär ökad risk för verksamheten. För att upptäcka dessa slags händelser kan det behövas sårbarhetsskanning som kan testa servrar för sårbarheter antingen aktivt eller passivt.

4 Roller och ansvar

It-säkerhetsincidenter kan överskrida vårdgivargränser men även externa organisatoriska och nationella gränser. Landstingets förmåga att hantera sådana händelser effektivt och konsekvent kan förbättras genom en övergripande process för styrning av it-säkerhetsincidenter och samordnad hantering av it-säkerhetsrelaterade händelser. Nyckelroller och ansvar behöver framgå för att tydliga beslutskedjor och effektiv hantering av it-säkerhetsincidenter ska kunna uppnås.

4.1 Identifierade nyckelroller och ansvar

Landstingets informationssäkerhetspolicy och tillhörande riktlinjer [5] anger vad som ska uppnås med informationssäkerhetsarbetet och beskriver roller och ansvar samt hur arbetet ska organiseras.

Under år 2015 inrättades en stödjande funktion inom landstinget, SLL SOC, med uppgiften att upptäcka och hantera it-säkerhetsrelaterade hot och incidenter. SLL SOC:s uppdrag är att ge vägledning och rekommendationer till landstingets förvaltningar och bolag om åtgärder och strukturerade arbetssätt för att upptäcka och hantera it-säkerhetsrelaterade hot och incidenter. Syftet är att minska omfattningen och skadeverkan av it-säkerhetsrelaterade hot och incidenter.

För att etableringen av SLL SOC ska lyckas fullt ut och generera önskade nyttovärden krävs samverkan mellan SLL SOC och berörda linjeorganisationer med stöd av befintliga it-processer/funktioner inom landstingets förvaltningar/bolag. Tydliga gränssnitt behöver etableras.

En översyn av roller och ansvar i tjänstemannaorganisationen har genomförts med utgångspunkt i en scenarioanalys av olika slags oönskade händelser, se kapitel 3. Nedan redovisas de nyckelroller som på ett eller annat sätt kan komma att behöva samverka i händelse av en it-säkerhetsincident. Rollerna och respektive ansvar i incidenthanterings-processen behöver tydliggöras, förslagsvis i en av de till riktlinjerna hörande tillämpningsanvisningarna. Framtida övningar inom området kan leda till att ytterligare nyckelroller sedan identifieras.

Roll	Beskrivning och ansvar
Landstingsdirektör	Landstingsdirektören har landstingstingsstyrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och fördela resurser, så att målen kan uppnås.
Förvaltnings-/bolagschef	Ytterst ansvarig för informationssäkerheten inom resp förvaltning/bolag. Ytterst ansvarig för organisationen som omfattas av en incident.
IT-direktör/CIO	IT-direktör, CIO eller motsvarande. Ansvarig för it-verksamheten som omfattas av en incident.
OÄ, OÄ-IT	Objektägare resp. objektägare-IT för det objekt som berörs av en incident. Ansvarig för informationssäkerheten inom objektet som omfattas av en incident.
FL, FL-IT	Förvaltningsledare resp. förvaltningsledare-IT för det objekt som berörts av en incident. Ansvariga för förvaltningen av objektet som omfattas av en incident.
IT-chefer/-ansvariga	Chefer eller ansvariga inom IT med ansvar för leverans av applikationer och teknisk infrastruktur.
TiB	Tjänsteman i Beredskap. TiB SLL ansvarar för att avgöra om incidenter ska eskaleras till landstingsdirektör och krisledningsnämndens ordförande. TiB TF ansvarar för att avgöra om incidenter inom trafikförvaltningens ansvarsområde ska eskaleras till TiB SLL.
IM eller motsvarande funktion	Incident Manager eller motvarande inom driftorganisationer. Ansvarig för att operativt leda och administrera processen Incidenthantering inom it-verksamheten som omfattas av en incident. [6]
SLL SOC	Säkerhetsoperativt center inom SLL. Övergripande funktion med ansvar att stödja landstingets verksamheter med att upptäcka och hantera it-säkerhetsrelaterade hot och incidenter.
PÄ SOC	Processägare och ansvarig för verksamheten inom SLL SOC.
PL SOC	Objektledare SLL SOC. Ansvarig för att operativt leda och administrera processer inom SLL SOC.

5 Övergripande process

För att säkerställa att eventuella it- och informationssäkerhetsincidenter hanteras snabbt och effektivt inom landstinget behöver det finnas en formaliserad övergripande styrningsprocess för rapportering och hantering av incidenter. En standardiserad process ska säkerställa att de oönskade händelserna blir rapporterade på ett sådant sätt att lämpliga åtgärder omedelbart kan vidtas.

5.1.1 Övergripande process för styrning av it-säkerhetsincidenter

Krisberedskapsplan för Stockholms läns landsting [7] är ett styrande dokument för landstingets arbete med krisberedskap. Planen anger en inriktning för Stockholms läns landstings arbete före, under och efter olika typer av kriser och samhällstörningar, såväl allvarliga händelser som extraordinära händelser. Krisberedskapsplan för Stockholms läns landsting ska efterlevas av samtliga nämnder, styrelser och bolag inom landstinget och av samtliga som arbetar på uppdrag av landstinget.

Utredningen konstaterar att it- och informationssäkerhetsincidenter inom landstinget ska hanteras i enlighet med gällande krisberedskapsplan för landstinget. Utredningen föreslår att detta tydliggörs i de övergripande styrdokumenten för informationssäkerhet. Det är avgörande för hanteringen av alla typer av incidenter att krisberedskapsplanen är implementerad i landstingets verksamheter.

Förvaltningar och bolag har ett delegerat ansvar att leda och samordna egen verksamhet enligt uppgjorda planer. Vid behov aktiveras krisledningsgrupper, KLG, enligt fastställda beredskapslägen. Utredningen konstanterar att hanteringen av it-säkerhetshändelser ska integreras i de ordinarie planerna så lång det är möjligt. Hantering och eskalering ska ske enligt nedan.

Högt klassade incidenter eskaleras och rapporteras till TiB SLL. Efter initiala åtgärder ska TiB SLL i samverkan följa händelseutvecklingen och löpande bedöma om behov finns av ytterligare eskalering. TiB SLL ska i ett tidigt skede etablera kontakt med landstingets centrala kriskommunikationsfunktion för initial bedömning och hantering av kommunikationsinsats.

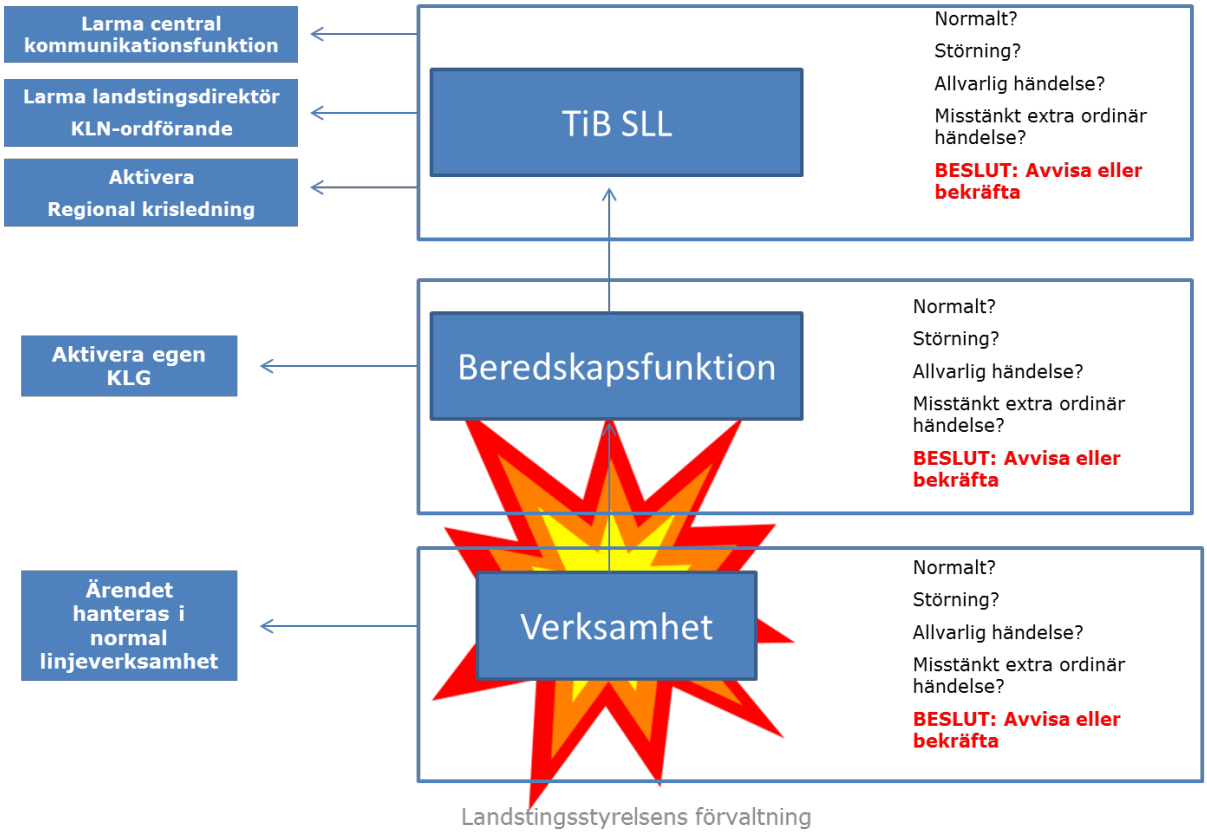

Bild 1: Nivåer i hantering av händelser enligt landstingets krisberedskapsplan.

I enlighet med gällande krisberedskapsplan ska verksamheterna ha inarbetade processer och rutiner för upptäckt, eskalering, beslut om åtgärder och kommunikation av incidenter. Det ska tydligt framgå i processerna och rutinerna vem som är operativt ansvarig för hantering av incidenter inom respektive förvaltning och bolag. Utredningen önskar särskilt betona vikten av att implementeringen av lokal krisberedskap sker skyndsamt och att resurser tillsätts för detta.

Översynen visar att det är nödvändigt att etablera viktiga gränsytor för att kunna integrera informationssäkerhetsincidenter i den ordinarie krisberedskapsprocessen och etablera tydliga beslutskedjor. Bilden nedan konkretiserar bild 1 genom att på ett principiellt sätt åskådliggöra dessa gränsytor.

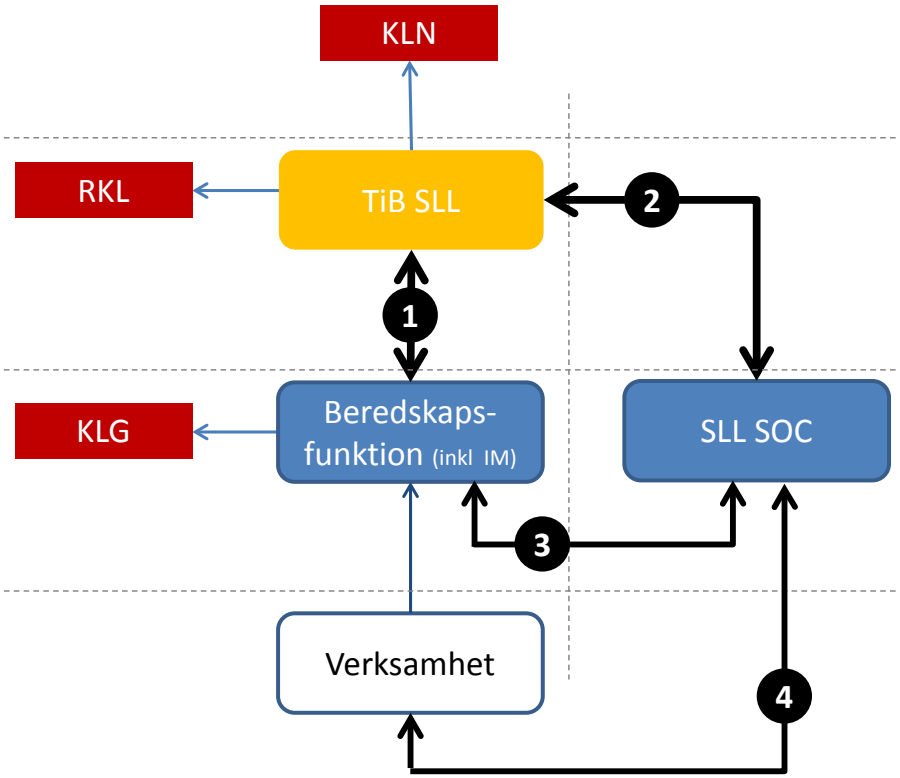

Bild 2: Bilden konkretiserar föregående bild 1 genom att på ett principiellt sätt åskådliggöra nödvändig gränsytor för att it-säkerhetshändelser ska kunna integreras i den ordinarie krisberedskapsprocessen.

Lokal beredskapsfunktion

Eskalering och rapportering av informationssäkerhetsincidenter ska ske enligt samma process som andra verksamhetsstörningar. Det innebär att it-säkerhetsincidenter ska eskaleras och rapporteras av verksamheten till den lokala beredskapsfunktionen. Utredningen önskar särskilt peka på att det är den lokala beredskapsfunktionens ansvar att säkerställa att högt klassade it-säkerhetsincidenter eskaleras och rapporteras vidare till TiB SLL (punkt 1 i bilden ovan). Den lokala beredskapsfunktionen kan vid behov lämna en förfrågan till SLL SOC om assistans (punkt 3 i bilden ovan)[2].

Ovanstående behöver integreras i och framgå av lokala planer, processer och rutiner för lokala beredskapsfunktioner.

I de fall it-säkerhetsincidenter upptäcks av it-verksamheten, exempelvis SLL IT eller motsvarande it-verksamhet inom landstinget, ska eskalering och rapportering på samma sätt ske till den lokala beredskapsfunktionen, d.v.s. IM-funktionen[3] eller motsvarande. Utredningen önskar särskilt peka på att det i detta fall är IM:s ansvar att säkerställa att högt klassade it-säkerhetsincidenter eskaleras och rapporteras vidare till även TiB SLL (punkt 1 i bilden ovan).

---

[2] SLL SOC har i nuläget beredskap under kontorstid.
[3] Incident manager

IM eller motsvarande funktion inom en it-verksamhet kan vid behov lämna en förfrågan till SLL SOC om assistans (punkt 3 i bilden ovan).

Ovanstående behöver integreras i och framgå av lokala planer, processer och rutiner för IM eller motsvarande funktion.

TiB SLL
Tjänsteman i beredskap, TiB SLL, finns på regional nivå inom landstinget och ska *"...omedelbart efter larm kunna påbörja samordning och ledning av landstingets insatser på regional nivå."*[4]. TiB SLL ansvarar vidare för att "*...avgöra om insatser ska eskaleras till landstingsdirektör och krisledningsnämndens ordförande*".[5] TiB SLL har enligt landstingets krisberedskapsplan befogenhet att fatta de beslut som krävs för att initiera och samordna det inledande arbetet. TiB SLL kan vid behov lämna en förfrågan till SLL SOC om assistans (punkt 2 i bilden ovan). Efter initiala åtgärder ska TiB SLL i samverkan följa händelseutvecklingen och löpande bedöma om behov finns av eskalering.

Ovanstående behöver integreras i och framgå av lokala planer, processer och rutiner för TiB SLL samt TiB TF.

SLL SOC
I SLL SOC:s uppdrag ingår flera uppgifter, varav en är en rådgivande och stödjande uppgift. Detta innebär, att i de fall händelser eller avvikelser upptäcks av verksamheten eller it-verksamheten eller larm inkommit till den lokala beredskapsfunktionen eller IM-funktionen, kan dessa göra en förfrågan om råd eller analys-assistans till SLL SOC (se punkt 4 ovan).

På motsvarande sätt kan händelser eller avvikelser gällande en verksamhet eller en it-verksamhet, upptäckas av SLL SOC och bedömas kräva vidare analys.

Inom ramen för översynen har en instruktion för SLL SOC gällande hantering av it-säkerhetsincidenter tagits fram. Instruktionen består av tre delar: Beslut om analys, Initiering av analys samt Avslut. Varje del innehåller beskrivningar av ansvar och roller för hantering av it-säkerhetsincidenter samt vilken roll som har beslutsmandat i respektive steg.

Övrigt
Att incidenter värderas mot klasser är en förutsättning för en effektiv incidenthantering. Utredningen konstaterar att det inom landstinget förekommer olika modeller för hur informationssäkerhetsincidenter ska klassas. Utredningen föreslår därför att en landstingsgemensam

---

[4] Avsnitt 5.1 i Plan krisberedskap Stockholms läns landsting. Planeringsinriktning inför allvarlig händelse samt Plan för krisledningsnämnden vid extraordinära händelser, LS 1406-0750.
[5] TiB TF ansvarar för att händelser inom trafikförvaltningens ansvarsområde eskaleras till TiB SLL

klassificeringsmodell för bedömning av skadeverkan och prioritering tas fram och fastställs av landstingsdirektören i en tillämpningsanvisning.

Rapporteringen av informationssäkerhets-avvikelser bör ske på samma sätt som för andra slags avvikelser, t.ex. genom HändelseVis[6].

Utredningen önskar i sammanhanget peka på att krishanteringssystemet bygger på ett underifrånperspektiv som utgår från lokal nivå till regional och central nivå [7]. En av huvudprinciperna i systemet är den s.k. ansvarsprincipen. Den innebär att den som har ansvaret för en verksamhet under normala förhållanden ska ha motsvarande ansvar vid allvarliga händelser och under höjd beredskap. Den andra huvudprincipen är likhetsprincipen. Den innebär att en verksamhets organisation och lokalisering så långt det är möjligt ska överensstämma i fred, kris och krig. Den tredje huvudprincipen är närhetsprincipen och innebär att störningar ska hanteras på lägsta möjliga nivå, d.v.s. där krisen inträffar och av dem som är närmast berörda. Huvudprinciperna gäller även hantering av it-säkerhetshändelser och ska framgå av lokala planer.

[6] HändelseVis är Stockholms läns landstings gemensamma IT-stöd för risk- och avvikelserapportering.

6 Behov av justering av mandat

Landstingsfullmäktige antar reglementen för nämnderna. I "Reglementen, arbetsordningar och delegationsordning" för Stockholms läns landsting klargörs uppgiftsfördelningen mellan nämnderna [8].

I Krisberedskapsplan för Stockholms läns landsting beskrivs roller och ansvar liksom uppdrag och direktiv till förvaltningar, bolag och upphandlade verksamheter.

Landstingets riktlinjer för informationssäkerhet innehåller en beskrivning av olika roller samt vilken roll som har beslutsmandat i olika delar gällande informationssäkerhet specifikt.

Vidare innehåller landstingets gemensamma förvaltningsstyrningsmodell (som utgår från pm3) beskrivningar av beslutsmandat.

Utredningen har genomfört en översyn av dessa beskrivningar och analyserat dem i förhållande till de hypotetiska typfallen som identifierats, se kapitel 3. Utredningen konstaterar att vissa beslutsmandat saknas för att tydliga beslutskedjor ska kunna etableras och synliggöras. Utredningens förslag på justerade mandat redovisas nedan.

6.1.1 Mandat att besluta om kontroller i syfte att identifiera hot mot landstingets informationstillgångar

Riktlinjer för informationssäkerhet inom Stockholms läns landsting anger på vilket sätt kontrollåtgärder får ske och hur loggning och kontroller får ske för att identifiera hot mot landstingets informationstillgångar. Översynen visar att landstingsdirektörens liksom förvaltnings- och bolagschefers beslutsmandat behöver stärkas och tydliggöras.

Härutöver är det ur ett juridiskt perspektiv nödvändigt att alla inom landstinget görs medvetna om att loggning sker av aktiviteter i it-systemen och att uppföljning av aktiviteterna sker i syfte att upptäcka brister och sårbarheter i it-miljöerna. Detta åstadkoms lämpligen genom att en informationsruta visa för medarbetare via skärmen vid inloggning.

För att tydliggöra mandat föreslås att följande tydliggörs i till riktlinjerna hörande tillämpningsanvisningar:

- Information om vad som sker på en användares dator lagras centralt och i enskild dator, s.k. loggning. Loggning görs för driftövervakning och felsökning men kan även göras för uppföljning av att gällande regler och riktlinjer följs samt för att identifiera hot (t.ex. intrångsförsök och skadlig kod) som kan utgöra en fara för landstingets IT-miljö och/eller informationstillgångar. Användare föreslås få information om detta via en informationsruta vid inloggning[7].

- Medarbetares användning av landstingets IT-system kan komma att följas upp vid misstanke om brott mot lag eller landstingets styrande regelverk.

- Förvaltningschef/VD eller motsvarande, eller person med delegation därifrån, beslutar om kontroll av medarbetares användning ska ske och om några åtgärder ska vidtas i det enskilda fallet i samband med överträdelser. Förvaltningschef/VD ska fastställa instruktioner hur sådan kontroll ska genomföras[8].

- Landstingsdirektören, eller den som landstingsdirektören utser, beslutar om kontroll ska ske av loggar i central it-infrastruktur i syfte att identifiera och oskadliggöra hot mot landstingets IT-miljö eller informationstillgångar. Landstingsdirektören, eller den som landstingsdirektören utser, ska fastställa instruktioner för hur sådana kontroller ska genomföras. Landstingets förvaltningar och bolag samt privata vårdgivare och andra som genom avtal är bundna av dessa riktlinjer ska bistå i detta arbete[9].

6.1.2 Mandat för avstängning av anslutningar mellan system

Om ett it-system, eller delar av ett it-system, behöver stängas av är det systemägarens[10] ansvar att så sker. Enligt landstingets gemensamma förvaltningsstyrningsmodell som utgår från pm3 innebär detta att ansvaret är objektägarens, OÄ. Om en nätverksanslutning behöver stängas av, t.ex. för att förhindra spridning av skadlig kod i samband med virusangrepp kan det vara flera olika it-system som inte blir åtkomliga och flera systemägare som behöver involveras.

---

[7] Förvaltningar, bolag eller privata aktörer ansvarar för att deras medarbetare som arbetar i landstingets it-miljö informeras om att loggning sker av vad man gör i it-miljön.
[8] Kontrollen sker mot specifik individ, t.ex. med hjälp av loggkontroller.
[9] Syftet med kontrollen är inte att kontrollera enskild användares aktiviteter i it-miljön. Syftet med denna skrivning är istället att skapa förutsättningar för kontroller av loggar i central it-infrastruktur för att kunna upptäcka hot, sårbarheter och avvikelser. Om problem sedan upptäcks i den centrala it-infrastrukturen som är kopplade till specifikt bolag eller förvaltning ska VD/förvaltningschef eller motsvarande fatta beslut om närmare kontroller.
[10] Begreppet systemägare motsvaras av flera roller enligt landstingets förvaltningsstyrningsmodell (som baseras på modellen pm3).

Översynen av ansvar och roller gällande avstängning av anslutningar mellan system visar att tydliga beslutsmandat idag saknas eller är otydliga. Det föreslås därför att beslutsmandat att stänga av anslutningar i enlighet med fastställda processbeskrivningar och utifrån fastställda kriterier även ges till tjänsteman i beredskap, TiB, i samråd med berörd förvaltnings-/bolagschef samt landstingets chefläkare. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats. Det föreslås vidare att delegationen framgår i gällande version av ”Arbetsordningar, reglementen och delegationsordning” för Stockholms läns landsting.

För att tydliggöra mandat föreslås:

- Delegationen gällande avstängning av anslutningar till tjänsteman i beredskap, TiB, i samråd med berörd förvaltnings-/bolagschef samt landstingets chefläkare, behöver framgå i ”Arbetsordningar, reglementen och delegationsordning” för Stockholms läns landsting.
- Beslutsmandatet ska tydliggöras i riktlinjerna för informationssäkerhet eller tillämpningsanvisning.

6.1.3 Mandat för beslut om it-säkerhetsåtgärder

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 landstingsövergripande perspektiv.

Utredningen har granskat hur beslutskedjorna för it-säkerhetsåtgärder ser ut i dagsläget och om de behöver förändras. Utredningens slutsats är att ansvaret för att besluta om it-säkerhetsåtgärder i första hand är systemägarens[11]. Enligt landstingets gemensamma förvaltningsstyrningsmodell som utgår på pm3 innebär detta att ansvaret är objektägare-IT:s, OÄ-IT. Beroende på åtgärd kan det även uppstå situationer där ansvaret är OÄ:s och OÄ-IT:s gemensamt. Om mer än en verksamhet påverkas så föreslås att mandat att besluta om it-säkerhetsåtgärder finnas på central nivå, hos landstingsdirektören eller person som denne utser.

Det föreslår att en utredning genomförs utifrån riskbedömning huruvida den centrala styrningen av central it-infrastruktur kan stärkas.

Utredningen föreslår följande:

- I landstingets riktlinjer för informationssäkerhet ska tydliggöras att det är systemägaren som har ansvaret att besluta om it-säkerhetsåtgärder

[11] Begreppet systemägare motsvaras av objektägare och objektägare-IT enligt landstingets förvaltningsstyrningsmodell (som baseras på modellen pm3).

- I rollbeskrivningarna för landstingets gemensamma förvaltnings-styrningsmodell som utgår från pm3 ska tydliggöras att ansvaret för att besluta om it-säkerhetsåtgärder ligger hos objektägare-IT och i förekommande fall gemensamt hos objektägare och objektägare-IT.
- Om mer än en verksamhet påverkas ska mandat att besluta om it-säkerhetsåtgärder finnas på central nivå, förslagsvis hos landstingsdirektören eller den som landstingsdirektören utser.
- En utredning genomförs utifrån riskbedömning huruvida den centrala styrningen av central it-infrastruktur kan stärkas.

6.1.4 Mandat att genomföra uppföljning av it-säkerhet

I gällande riktlinjer för informationssäkerhet, punkt [3.1.3] framgår det att landstingsdirektören ska utse en informationssäkerhetschef med ansvar för samordning och övergripande uppföljning av informationssäkerhetsarbetet inom landstinget. Behov av justering av mandat i detta avseende föreligger således ej. Dock föreslås att en kontrollplan tas fram för uppföljningar hos vårdgivare, även privata.

7 Förslag på justering i befintliga riktlinjer

7.1 Förslag på justering om kontrollåtgärder

Reglerna för kontrollåtgärder anges i pkt [6.9.1]-[6.9.4] i riktlinjer för informationssäkerhet inom Stockholms läns landsting. Översynen visar att nuvarande skrivningar gällande kontrollåtgärder behöver tydliggöras. Utredningen föreslår att justeringar görs genom att ersätta nuvarande pkt [6.9.1]-[6.9.7] med följande skrivningar:

Utredningens förslag: [6.9.1] Information om vad som sker på en användares dator lagras centralt och i enskild dator, s.k. loggning. Loggning görs för driftövervakning och felsökning men kan även göras för uppföljning av att gällande regler och riktlinjer följs samt för att identifiera hot (t.ex. intrångsförsök och skadlig kod) som kan utgöra en fara för landstingets IT-miljö och/eller informationstillgångar.

Kommentar: Sker lämpligen genom att ha en informationsruta om detta vid inloggning. Förvaltningar, bolag eller privata aktörer ansvarar för att deras medarbetare som arbetar i landstingets it-miljö informeras om att loggning sker av vad man gör i it-miljön.

Utredningens förslag: [6.9.2]Medarbetares användning av landstingets IT-system kan komma att följas upp vid misstanke om brott mot lag eller landstingets styrande regelverk.

Utredningens förslag: [6.9.3]Förvaltningschef/VD eller motsvarande, eller person med delegation därifrån, beslutar om kontroll av medarbetares användning ska ske och om några åtgärder ska vidtas i det enskilda fallet i samband med överträdelser. Förvaltningschef/VD ska fastställa instruktioner för hur sådan kontroll ska genomföras.

Kommentar: Kontrollen sker mot specifik individ, t.ex. med hjälp av loggkontroller.

Utredningens förslag: [6.9.4]Förvaltningschef/VD eller motsvarande, eller person med delegation därifrån, beslutar om kontroll ska ske av trafiken i lokala nätverk. Förvaltningschef/VD ska fastställa instruktioner för hur sådan kontroll ska genomföras.

Kommentar: Kontrollen kan ske generellt, t.ex. med hjälp av loggkontroller. Syftet med denna skrivning är att skapa tydliga möjligheter för kontroll i syfte att upptäcka hot, sårbarheter och avvikelser i lokala nätverk. Kontrollen utförs lämpligen genom att loggar skickas till centralt verktyg för logguppföljning där uppföljning utförs av SLL SOC.

Utredningens förslag: [6.9.5] Landstingsdirektören, eller den som landstingsdirektören utser, beslutar om kontroll ska ske av loggar i central it-infrastruktur i syfte att identifiera och oskadliggöra hot mot landstingets IT-miljö eller informationstillgångar. Landstingsdirektören, eller den som landstingsdirektören utser, fastställer instruktioner för hur sådan kontroll ska genomföras. Landstingets förvaltningar och bolag samt privata vårdgivare och andra som genom avtal är bundna av dessa riktlinjer är skyldiga att bistå i detta arbete.

Kommentar: Syftet med kontrollen är inte att kontrollera enskild användares aktiviteter i it-miljön.

Utredningens förslag: [6.9.6]Medarbetares tillgång till landstingets it-system kan stängas av vid misstanke om brott mot lag eller landstingets styrande regelverk eller då användningen utgör en allvarlig risk för landstingets it-miljö och/eller informationstillgångar.

Kommentar: Anger när exempelvis SAM-konton i landstingets distans-tjänst får stängas av.

Utredningens förslag: [6.9.7] Anslutning till SLLnet kan komma att stängas av då anslutningen utgör hot mot landstingets IT-miljö och/eller informationstillgångar. Beslut om sådan avstängning ska fattas av systemägaren för SLLnet, eller person med delegation därifrån. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats.

7.2 Förslag på justering om incidenthantering

Reglerna för incidenthantering anges i [12.1.1]-[12.1.4] i riktlinjer för informationssäkeret inom Stockholms läns landsting. Översynen visar att nuvarande skrivningar behöver kompletteras. Utredningen föreslår att justeringar görs genom att ersätta nuvarande pkt[12.1.1]-[12.1.2] med följande skrivningar:

Utredningens förslag: [12.1.1] om incidentstyrning:
Informationssäkerhetsincidenter ska hanteras enligt samma process som andra verksamhetsstörningar.

Kommentar: Processer och rutiner för krisberedskap ska inkludera hantering av informationssärhetsincidenter.

Utredningens förslag: [12.1.2] om incidentstyrning: Medarbetare ska rapportera avvikelser som kan utgöra ett hot mot landstingets informationstillgångar enligt anvisad rutin. Förvaltningschef/VD ska fastställa rutin för hur sådan rapportering ska genomföras.

Kommentar: Rapportering bör ske på samma sätt som för övriga avvikelser, t.ex. genom landstingets it-stöd HändelseVis. Kravet på rapportering av avvikelser omfattar anställda och andra som arbetar på uppdrag av landstinget och som har tillgång till landstingets informationstillgångar och IT-system.

8 Slutsatser och rekommendationer

Uppdraget från landstingsstyrelsen var att göra en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras för t.ex. upptäckt, eskalering, åtgärder och kommunikation gällande it-säkerhetsåtgärder och incidenthantering. Uppdraget innebär att utreda förutsättningarna för en ambitionshöjning inom informationssäkerhetsområdet. Slutsatser och rekommendationer redovisas nedan.

8.1 Process för styrning vid säkerhetsincidenter

Utredningen slår fast att it- och informationssäkerhetsincidenter ska hanteras i enlighet med gällande krisberedskapsplan för landstinget. Det är avgörande för hantering av alla typer av incidenter att krisberedskapsplanen är implementerad i verksamheterna.

Verksamheterna ska, i enlighet med gällande krisberedskapsplan, ha inarbetade processer och rutiner för upptäckt, eskalering, beslut om åtgärder och kommunikation av incidenter. Det är nödvändigt att informationssäkerhetsincidenter integreras i dessa processer. Utredningen ser behov av att implementering av lokal krisberedskap sker skyndsamt och att resurser tillsätts för detta.

Samtidigt behöver den övergripande styrningen av it-säkerhetsincidenter förtydligas i en till riktlinjerna hörande tillämpningsanvisningar. Utredningen ser det som nödvändigt att gränssnitt etableras mellan framför allt tjänsteman i beredskap, förvaltningar och bolags beredskaps-funktioner och krisledningsgrupper samt säkerhetsoperativt center, SLL SOC.

Rapportering av informationssäkerhetsincidenter ska ske enligt samma process som andra verksamhetsstörningar.

Rapporteringen av informationssäkerhets-avvikelser bör ske på samma sätt som för övriga avvikelser, t.ex. genom it-stödet HändelseVis.

8.2 Nya beslutsmandat

Utredningen har genomfört en översyn av beslutsmandaten i olika slags styrande dokument och analyserat dem i förhållande till identifierade typfall, se

kapitel 3. Utredningen konstaterar att följande nya beslutsmandat behöver ges för att tydliga beslutskedjor ska kunna etableras och synliggöras:

- Mandat att besluta om kontroller
- Mandat att stänga av anslutningar
- Mandat att besluta om it-säkerhetsåtgärder

Mandat gällande uppföljning/revision av it-säkerhet beskrivs redan i riktlinjerna för informationssäkerhet och behöver ej justeras. Dock föreslås att en plan tas fram för uppföljningar/revision hos vårdgivare, även privata.

8.3 Justering av riktlinjerna

En översyn av roller och ansvar i tjänstemannaorganisationen har genomförts. Översynen visar på vissa brister i nödvändiga beslutsmandat. Mot denna bakgrund finns behov av att utveckla landstingets styrande dokument för informationssäkerhet. Det är i första hand reglerna för kontrollåtgärder och incidenthantering i riktlinjer för informationssäkerhet inom Stockholms läns landsting som förslås justeras i syfte att åstadkomma ökad tydlighet.

8.4 Klassificering av it-säkerhetsincidenter

Några av de största utmaningarna gällande hantering av informations-säkerhetsincidenter handlar om att förändra arbetssätt. En av dem gäller klassificering av it-säkerhetsincidenter. Utredningen konstaterar att det inom landstinget förekommer olika modeller för hur informationssäkerhetsincidenter ska klassas. Utredningen föreslår därför att en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering tas fram och fastställs av landstingsdirektören i en tillämpningsanvisning.

8.5 Övning

Utredningen önskar framhålla vikten av stärka landstingets förmåga att hantera it-säkerhetsrelaterade kriser och incidenter genom övningar. Det föreslås att övning av hantering av informationssäkerhetsincidenter genomförs för att träna samarbete mellan landstingets olika verksamheter i hanteringen av informationssäkerhetsincidenter. Inte minst är det viktigt att träna kommunikationsåtgärder vid olika slags oönskade händelser.

Referenser

[1] Tjänsteutlåtande Förslag på kort- och långsiktiga lösningar för bättre och tydligare IT-säkerhet, LS LS 1311-1456

[2] Principer för ny tjänstemannaorganisation under landstingsstyrelsen med anledning av den nya politiska organisationen, LS 1411-1350

[3] Myndigheten för samhällsskydd och beredskap: Informationssäkerhet– trender 2015.

[4] Prioritering it-säkerhetshändelser, 2015-04-24, SLL SOC

[5] Riktlinjer för informationssäkerhet inom Stockholms läns landsting, LS 1112-1733

[6] http://www.intranat2.sll.se/Global/SLLIT/Dokument/Styrdokument/Processbeskrivningar/Processbeskrivning_Incident_Management_V3.0.pdf , IM incidenthanteringsprocess

[7] Plan krisberedskap Stockholms läns landsting. Planeringsinriktning inför allvarlig händelse samt Plan för krisledningsnämnden vid extraordinära händelser, LS 1406-0750

[8] ”Arbetsordningar, reglementen och delegationsordning” för Stockholms läns landsting, 2015-02-17.

Dokumenthistorik

Datum	Författare	Kommentar
2015-08-21	Tiina Loukusa Anna-Lena Hallgren Henrik Brodin Sofia Burendahl Vesna Lucassi	Första versionen
2015-08-28	Sofia Burendahl	Uppdateringar
2015-09-03	Vesna Lucassi	Justeringar
2015-09-07	Vesna Lucassi	Språkliga rättningar