Landstingsrådsberedningen

SKRIVELSE
2017-03-22

LS 2015-1326

Landstingsstyrelsen

Landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter

Föredragande landstingsråd: Daniel Forslund

Ärendebeskrivning

Återrapportering av landstingsstyrelsens uppdrag till landstingsdirektören att utarbeta en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter.

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att godkänna återrapporteringen av förslag till landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter

att uppdra åt landstingsdirektören att, efter utvärdering och justering, fastställa en landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter i enlighet med promemoria bilagd landstingsdirektörens tjänsteutlåtande.

Landstingsrådsberedningens motivering

Stockholms läns landsting ska vara väl rustat för att upptäcka och hantera IT-säkerhetsrelaterade hot och incidenter. Den snabba IT-utvecklingen, komplexa system och ökad informationsdelning ställer höga krav på landstingets förmåga inom området. Som en del i detta arbete har ett förslag utarbetats kring en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter.

Informationssäkerhetsincidenter är händelser som påverkar eller kan komma att påverka säkerheten negativt för landstingets informationstillgångar. Det kan till exempel vara driftstörningar till följd av

skadlig kod, dataintrång eller obehörigt användande av information. Inom landstinget används i dag flera olika modeller för hur informationssäkerhetsincidenter klassas. En landstingsgemensam klassificeringsmodell med gemensamma nivåer och beskrivningar underlättar kommunikationen kring och bedömningen av incidenten så att rätt åtgärder vidtas så snabbt som möjligt.

Beslutsunderlag

Arbetsutskottets protokollsutdrag den 21 februari 2016
Innovationsberedningens protokollsutdrag den 15 februari 2016
Landstingsdirektörens tjänsteutlåtande den 2 februari 2017
Promemoria Förslag kring landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter. Bedömning av skadeverkan samt prioritering av informationssäkerhetsincidenter

Irene Svenonius

Daniel Forslund

Gustaf Drougge

§ 23
Landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter

LS 2015-1326

Ärendebeskrivning

Återrapportering av landstingsstyrelsens uppdrag till landstingsdirektören att utarbeta en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter.

Underlag

Landstingsdirektörens tjänsteutlåtande den 2 februari 2017
Promemoria Förslag kring landstingsgemensam Klassificeringsmodell för informationssäkerhetsincidenter - Bedömning av skadeverkan samt prioritering av informationssäkerhetsincidenter

Arbetsutskottets beslut

Arbetsutskottet beslutar

att lägga ärendet om klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter till handlingarna

---

Beslutsexpediering:
Akt

§ 8
En landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter

LS 2015-1326

Ärendebeskrivning

Återrapportering av landstingsstyrelsens uppdrag till landstingsdirektören att utarbeta en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 2 februari 2017
Promemoria Förslag kring landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter Bedömning av skadeverkan samt prioritering av informationssäkerhetsincidenter

Förslag och yrkande

Ordförandes förslag om bifall till landstingsdirektörens förslag

Proposition

Innovationsberedningens beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att godkänna återrapporteringen av förslag till landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter

att uppdra åt landstingsdirektören att, efter utvärdering och justering, slutligen fastställa en landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter i enlighet med promemoria bilagd landstingsdirektörens tjänsteutlåtande.

Beslutsexpediering:
Arbetsutskottet
Akt

Landstingsstyrelsens förvaltning
SLL Strategisk IT
SLL Informationssäkerhet

TJÄNSTEUTLÅTANDE
2017-02-02

LS 2015-1326

Handläggare:
Henrik Brodin

Landstingsstyrelsens
innovationsberedning

Landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter

Ärendebeskrivning

Återrapportering av landstingsstyrelsens uppdrag till landstingsdirektören att utarbeta en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 2 februari 2017
Promemoria Förslag kring landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter Bedömning av skadeverkan samt prioritering av informationssäkerhetsincidenter

Förslag till beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att godkänna återrapporteringen av förslag till landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter

att uppdra åt landstingsdirektören att, efter utvärdering och justering, slutligen fastställa en landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter i enlighet med promemoria bilagd landstingsdirektörens tjänsteutlåtande.

Förvaltningens förslag och motivering

Sammanfattning
I tjänsteutlåtandet klarläggs förutsättningarna för en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av incidenter med påverkan på informationssäkerheten. Den samlade bedömningen är att en landstingsgemensam modell kan tillämpas i den betydelsen att incidenter klassificeras utifrån gemensamma nivåer för skada och prioritering. Ett förslag på landstingsgemensam klassificeringsmodell har tagits fram och beskrivs i bilagd promemoria. Det rekommenderas att den föreslagna modellen, efter att den utvärderats och justerats, slutligen fastställs av landstingsdirektören.

Bakgrund
Landstingsdirektören genomförde under år 2015 en översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor etableras gällande IT-säkerhetsåtgärder och hantering av IT-säkerhetsrelaterade incidenter, LS 1404-0548. I samband med översynen konstaterades att det i landstinget förekommer flera olika modeller för hur informationssäkerhetsincidenter klassas. Ett förslag i utredningen var därför att klarlägga förutsättningarna för en landstingsgemensam modell för fastställande av landstingsdirektören, i syfte att ytterligare stärka förutsättningarna att hantera IT-säkerhetsrelaterade incidenter inom landstingets förvaltningar och bolag.

Överväganden
Förutsättningarna för en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av incidenter med påverkan på informationssäkerheten har utretts. En landstingsgemensam klassificeringsmodell med gemensamma nivåer och beskrivningar av dessa skulle underlätta kommunikation kring och bedömning av IT-incidenter med säkerhetspåverkan så att rätt åtgärder vidtas så snabbt som möjligt.

Utredningen har genomlyst vilka primära målgrupper som bör känna till hur incidenter klassificeras och identifierat vilka behov dessa målgrupper har. Exempel på målgrupper är landstingets stödjande funktion inom IT-säkerhet, SLL SOC (eng: information security operations center), parter med vilka SLL SOC för dialog (exempelvis SLL IT som sköter driften av stora delar av central IT-infrastruktur i landstinget och övriga IT-driftorganisationer inom landstinget) samt lokala krisledningar (staber).

Utredningen har vidare identifierat tre existerande klassificeringsmodeller inom landstinget. De finns inom Karolinska universitetssjukhuset, trafikförvaltningen och landstingsstyrelsens förvaltning/SLL IT. De tre modellerna är utformade för att framför allt hantera incidenter där *tillgängligheten* till information är påverkad. Två av modellerna utgår från verksamhetspåverkan och går därför att tillämpa även för incidenter där informationens *riktighet* befaras vara påverkad. Den tredje modellen utgår från perspektivet IT-system. Den är inskriven i avtal med driftleverantör och kan ändras först i samband med att nytt avtal skrivs. Ingen av modellerna är direkt tillämpbara på incidenter där information befaras vara *röjd för obehörig*.

Ett förslag till landstingsgemensam klassificeringsmodell med nivåer avseende skada och prioritering gällande informationssäkerhetsincidenter har tagits fram och redovisas närmare i bilagd promemoria. Föreslagen modell utgår från SLL IT:s incidentmodell avseende verksamhetspåverkan. Tillägg i nivåerna har gjorts för att omfatta incidenter där skyddsvärd information befaras ha röjts. Hänsyn har även tagits till landstingets modell för riskbedömning gällande informationssäkerhet samt till landstingets modell för informationssäkerhetsklassificering så att föreslagna nivåer inte avviker allt för mycket från de fastställda konsekvensnivåerna i dessa modeller.[1]

Utredningens samlade bedömning och rekommendation är att landstingsdirektören, efter utvärdering och erforderlig justering, beslutar om landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter, samt slutligen fastställer den i en till riktlinjerna hörande tillämpningsanvisning enligt förslaget i bilagd promemoria. Utvärdering och justering föreslås ske av landstingets stödjande funktion inom IT-säkerhet, SLL SOC, och avser främst att säkerställa att modellen blir ändamålsenlig i förhållande till identifierade målgruppers behov.

Det konstateras samtidigt att det finnas en påtaglig risk att identifierade vinster med en gemensam klassificeringsmodell uteblir om inte samtidigt en landstingsgemensam process för uppföljning av avvikelser och incidenter införs och stärkande styrningsåtgärder vidtas inom informationssäkerhetsområdet. Det rekommenderas därför att dessa åtgärder utvärderas och prioriteras.

---

[1] Tillämpningsanvisningarna LS 2016-0067 Hantering av informationstillgångar samt LS 2016-0067 Riskhantering.

Förtydligande avseende uppdraget till landstingsdirektören att fastställa en landstingsgemensam klassificeringsmodell för informationssäkerhets-incidenter

Landstingsstyrelsen och landstingsfullmäktige antog år 2013 en informationssäkerhetspolicy och riktlinjer för informationssäkerhet, LS 1112-1733[2]. Landstingsfullmäktige delegerade då viss beslutskompetens till landstingsstyrelsen som bemyndigades att i sin tur vidaredelegera beslutanderätten till landstingsdirektören. Beslutanderätten avser att besluta om ändringar eller tillägg till riktlinjer för informationssäkerhet samt att utarbeta tillämpningsanvisningar för beslut om styrdokument inom informationssäkerhetsområdet i Stockholms läns landstings nämnder, styrelser och bolag. Beslutanderätten beskrivs närmare i förvaltningens bakomliggande tjänsteutlåtande den 7 februari 2013.

Informationssäkerhetsincidenter är oavsiktliga eller avsiktliga händelser som påverkar eller kan komma att påverka säkerheten negativt för landstingets informationstillgångar. Exempel på sådana incidenter driftstörningar till följd av skadlig kod, dataintrång eller obehörigt användande av information. Krisberedskapsplanen för Stockholms läns landsting anger att varje nämnd och styrelse är ytterst ansvarig för planering och organisering av krisberedskap inom sitt verksamhetsområde, LS 1406-0750. Föreliggande förslag om landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter utgör ett stöd så att informationssäkerhetsaspekter kan integreras i detta arbete på ett likvärdigt sätt.

Mot bakgrund av detta föreslås landstingsdirektören i detta ärende ges mandat att efter utvärdering och justering att slutligen fastställa en landstingsgemensam klassificeringsmodell för informationssäkerhets-incidenter i enlighet med till detta tjänsteutlåtande bilagd promemoria.

Ekonomiska konsekvenser av beslutet

Ekonomiska konsekvenser av beslutet att införa en landstingsgemensam klassificeringsmodell bedöms vara förknippade med ev. behov av att reglera gemensamma nivåer i avtal. Kostnader bedöms även kunna uppstå till följd av delvis förändrade arbetsätt och utbildningsinsatser. Bland de positiva effekterna som bedöms uppstå till följd av beslutet finns vinster i form av mer effektiv uppföljning av informationssäkerhetsincidenter och på sikt en

[2] Reviderad version med i kap 6, kap 12 samt bilaga genomfördes år 2016, LS 2016-0646.

mer effektiv hantering av informationssäkerhetsincidenter med kortare ledtider.

Kostnader som kan uppstå ska rymmas inom respektive verksamhets budget. Beslutet omfattar personella resurser och utbildningsinsatser och motsvarar de krav som redan ställs på landstingets verksamheter. Kostnader för ett gemensamt systemstöd för rapportering av avvikelser och incidenter kommer att utredas innan eventuellt beslut om införande föreslås fattas.

Malin Frenning
Landstingsdirektör

Mats Nomberg
Tillförordnad direktör
Strategisk IT

Stockholms läns landsting

Landstingsstyrelsens förvaltning
SLL Strategisk IT
SLL Informationssäkerhet

PM
2017-02-02

LS 2015-1326

Förslag till landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter

Bedömning av skadeverkan samt prioritering av informationssäkerhetsincidenter

Innehållsförteckning

Sammanfattning 3

1. Bakgrund 4

2. Begrepp 5

3. Metod 6

4. Nulägesanalys 7
4.1 Nivåer vid Karolinska sjukhuset 7
4.2 Nivåer vid SLL IT 8
4.3 Nivåer vid trafikförvaltningen 10

5. Analys av behov och förutsättningar 11
5.1 Syfte 11
5.2 Omfattning på prioritetsnivåer 11
5.3 Målgrupper och behov 11
5.4 Analys av existerande modeller 13
5.5 Slutsats och rekommendation 13

6. Förslag på nivåer avseende skada och prioritering för informationssäkerhets-incidenter 16
6.1 Nivåer – informationssäkerhet 16
6.2 Nivåer kopplat till IT-säkerhet 17
6.3 Åtgärder kopplat till nivå 18

7. Referenser 19

Sammanfattning

I promemorian klarläggs förutsättningarna för en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av incidenter med påverkan på informationssäkerheten. En klassificeringsmodell med gemensamma nivåer och beskrivningar av dessa underlättar kommunikation kring och bedömning av IT-säkerhetrelaterade incidenter så att rätt åtgärder kan vidtas så snabbt som möjligt.

Utredningens samlade bedömning är att en landstingsgemensam modell kan tillämpas i den betydelsen att incidenter klassificeras utifrån gemensamma nivåer för skada och prioritering. I promemorian ges ett förslag på modell med nivåer.

Utredningens rekommendation är att landstingsdirektören, efter utvärdering och erforderlig justering, fastställer föreslagen landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter. Utvärdering och justering föreslås genomföras av landstingets stödjande funktion inom IT-säkerhet, SLL SOC (eng: information security operations center), och avser främst att säkerställa att modellen blir ändamålsenlig i förhållande till identifierade målgruppers behov.

Utredningen konstaterar samtidigt att det finnas en påtaglig risk att identifierade vinster med en gemensam klassificeringsmodell uteblir om inte samtidigt en landstingsgemensam process för uppföljning av avvikelser och incidenter införs och stärkande styrningsåtgärder vidtas inom informationssäkerhetsområdet. Det rekommenderas därför att dessa åtgärder prioriteras.

1. Bakgrund

I landstingsdirektörens översyn av roller och ansvar gällande hantering av IT-säkerhetsincidenter som genomfördes år 2015 [5] föreslås att en landstingsgemensam klassificeringsmodell för bedömning av IT-säkerhetsincidenter tas fram:

"Några av de största utmaningarna gällande hantering av informationssäkerhetsincidenter 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."

Bakgrunden till utredningens förslag var bland annat att ytterligare stärka förutsättningarna att hantera IT-säkerhetsrelaterade incidenter inom landstingets förvaltningar och bolag. En landstingsgemensam klassificeringsmodell med gemensamma nivåer och beskrivningar av dessa underlättar kommunikation kring och bedömning av IT-incidenter med säkerhetspåverkan så att rätt åtgärder kan vidtas så snabbt som möjligt.

Denna promemoria innehåller en närmare utredning och förslag för att bereda frågan. Promemorian har tagits fram av avdelning SLL Informationssäkerhet inom landstingsstyrelsens förvaltning.

2. Begrepp

Begrepp	Förklaring	Källa
Avvikelse	icke-uppfyllande av ett krav	SS-ISO/IEC 20000-1:2011 [4]
Händelse (event)	förekomst eller förändring av särskilda omständigheter	SIS-TR 50:2015 [9]
Incident	oplanerat avbrott i en tjänst, en minskning i kvaliteten hos en tjänst eller en händelse som ännu inte har påverkat leveransen av en tjänst till kunden	SS-ISO/IEC 20000-1:2011 [4]
Informations-säkerhet	bevarande av konfidentialitet, riktighet och tillgänglighet hos information	SIS-TR 50:2015 [9]
Informations-säkerhetsincident	enskild eller flera oönskade eller oväntade informations-säkerhetshändelser som har negativa konsekvenser för verksamheten och dess in-formationssäkerhet	SIS-TR 50:2015 [9]
IT-säkerhet	IT-relaterade tekniska säker-hetsåtgärder för att upprätthålla informationssäkerhet	SIS-TR 50:2015 [9]
Konfidentialitet	skydd mot obehörig insyn	SIS-TR 50:2015 [9]
Riktighet	skydd mot oönskad förändring	SIS-TR 50:2015 [9]
Sårbarhet	brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot	SIS-TR 50:2015 [9]
Tillgänglighet	åtkomst för behörig person vid rätt tillfälle	SIS-TR 50:2015 [9]

3. Metod

Uppdraget genomfördes genom en kartläggning av förekommande klassificeringsmodeller samt interna möten (i workshop-form) som genomfördes under hösten 2016. Mötena inriktades mot diskussion om nuläge och behov. Syftet var även att säkerställa att den kunskap som finns internt inom landstinget togs tillvara.

Datum	**Deltagare**
2016-06-10 *(5 personer)*	Landstingsstyrelsen förvaltning • Informationssäkerhet • IT-säkerhet
2016-09-26 *(3 personer)*	Karolinska Universitetssjukhuset • Informationssäkerhet • IT-säkerhet
2016-10-05 *(4 personer)*	Landstingsstyrelsens förvaltning/SLL IT • Incidenthantering • IT-säkerhet
2016-10-18 *(4 personer)*	Trafikförvaltningen • Informationssäkerhet • IT-säkerhet • Incidenthantering

Följande frågor diskuterades under mötena:

- Vilka nivåer används idag?
- Hur ser deltagarna på behoven av att ensa nivåer inom SLL?
  - Vilka är fördelarna med att ensa nivåer?
  - Vilka är nackdelarna med att ensa nivåer?
- Gäller behovet av nivåer i så fall infosäkerhetsincidenter i stort eller bara IT-säkerhetsincidenter?
- Syfte med gemensamma incidentnivåer.
- Målgrupp för gemensamma incidentnivåer.

Avslutningsvis analyserades och sammanställdes den insamlade informationen, och ett förslag till inriktning togs fram.

4. Nulägesanalys

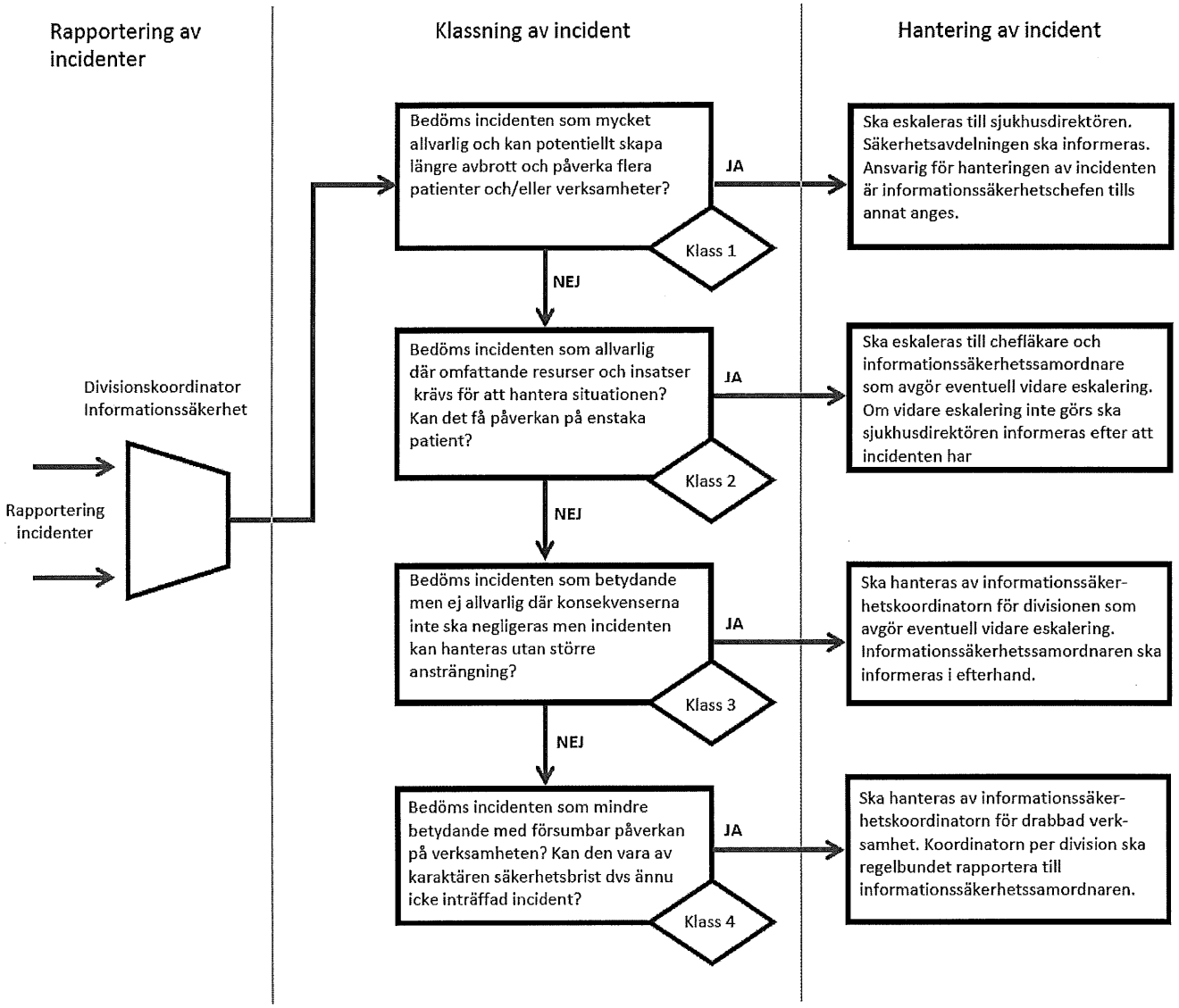
Under arbetet har tre klassificeringsmodeller med tillhörande nivåer identifierats inom landstinget. Dessa beskrivs nedan. Några ytterligare modeller och nivåer som används inom landstingets verksamheter har inte framkommit.

4.1 Nivåer vid Karolinska sjukhuset

I bilaga 21 till Karolinska sjukhusets lokala riktlinjer för informationssäkerhet [2] beskrivs sjukhusets modell för hantering av informationssäkerhetsincidenter:

Rapporterade incidenter ska värderas mot följande fyra klasser:

Klassning av incident		*Hantering av incident*
Klass 1	Bedöms incidenten som mycket allvarlig och kan potentiellt skapa längre avbrott och påverka flera patienter och/eller verksamheter?	Ska eskaleras till sjukhusdirektören. Säkerhetsavdelningen ska informeras. Ansvarig för hanteringen av incidenten är informationssäkerhetschefen tills annat anges
Klass 2	Bedöms incidenten som allvarlig där omfattande resurser och insatser krävs för att hantera situationen? Kan det få påverkan på enstaka patient?	Ska eskaleras till chefläkare och informationssäkerhetssamordnare som avgör eventuell vidare eskalering. Om vidare eskalering inte görs ska sjukhusdirektören informeras efter att incidenten har inträffat.
Klass 3	Bedöms incidenten som betydande men ej allvarlig där konsekvenserna inte ska negligeras men incidenten kan hanteras utan större ansträngning?	Ska hanteras av informationssäkerhetskoordinatorn för divisionen som avgör eventuell vidare eskalering. Informationssäkerhetssamordnaren ska informeras i efterhand.
Klass 4	Bedöms incidenten som mindre betydande med försumbar påverkan på verksamheten? Kan den vara av karaktären säkerhetsbrist dvs. ännu icke inträffad incident?	Ska hanteras av informationssäkerhetskoordinatorn för drabbad verksamhet. Koordinatorn per division ska regelbundet rapportera till informationssäkerhetssamordnaren



4.2 Nivåer vid SLL IT

Inom SLL IT vid landstingsstyrelsens förvaltning finns en fastställd incidentprocess som beskrivs i en processbeskrivning [3]:

Prioritering sker i Servicedesk genom att ange ärendets påverkan och en bedömning om hur brådskande ärendet är. Denna kan justeras av Incident Manager vid behov. Prioritetsnivåerna 1 – Kritisk eller 2 – Hög sätts vanligen i samråd med Incident Manager (IM).

Dessa prioriteringskoder ska associeras med lämpliga åtgärdstider (enl. SLA):

Prioriteringsmatris

	Mycket stor	Stor	Begränsad	Liten
Kritisk	**1**	**2**	**3**	**4**
Hög	**2**	**2**	**3**	**4**
Medel	**2**	**3**	**4**	**4**
Låg	**3**	**3**	**4**	**4**

Hur akut	**Prio 1 Kritisk**	**Prio 2 Hög**	**Prio 3 Medel**	**Prio 4 Låg**
Påverkan	En mycket stor störning som drabbat ett stort antal kunder eller en affärsenhet. Kritiska verksamhetsprocesser kan inte genomföras. Det kan även innebära att det finns en förhöjd risk att patientsäkerheten äventyras. Medför finansiella skador, negativ medie-exponering och/eller brott mot lagstadgade föreskrifter.	System eller applikation användbar, men med stora begränsningar. Prestanda allvarligt begränsad. Det kan även innebära att det finns en förhöjd risk att patientsäkerheten äventyras. Medför finansiella skador, negativ medie-exponering och/eller brott mot lagstadgade föreskrifter.	Incidenter som drabbar ett mindre antal användare och som påverkar kundens produktivitet. Måste lösas skyndsamt, men har ingen negativ finansiell effekt på SLA. Standardprioritering.	Incidenter som drabbar en enskild användare, och som inte direkt påverkar kundens produktivitet. Tillfällig lösning finns framtagen och är tillgänglig.
Insats	Alla inom SLL IT vid behov.	Alla nödvändiga resurser	Prioriterat mot övriga öppna ärenden.	När resurser är tillgängliga.

4.3 Nivåer vid trafikförvaltningen

Trafikförvaltningen har i avtal med av trafikförvaltningen upphandlad driftsleverantör fastställt nivåer för prioritering av händelser [1]:

Varje Incident tillskrivs en Prioritet. Prioritet används för att kunna prioritera Incidenter samt för att följa upp avvikelser i IT-driften.

Prioritet	Beskrivning	Åtgärdstid
P1	Kritisk påverkan, funktion ej tillgänglig, ingen temporär lösning finns tillgänglig	Direkt (akut åtgärd)
P2	Betydande påverkan, del av funktion ej tillgänglig, ingen temporär lösning finns tillgänglig	Direkt (akut åtgärd)
P3	Påverkan, del av funktion ej tillgänglig, temporär lösning finns tillgänglig	Planerad åtgärd
P4	Ringa påverkan, stör ej funktionalitet i applikation/Funktion	Planerad åtgärd

Leverantören ansvarar för att:

- *vid Incident av Prioritet 1 och 2 omedelbart informera SLs Incident Manager dessutom ska en Incidentrapport levereras till SL inom 24 timmar*
- *vid Incident av Prioritet 3 och 4 informera SLs Incident Manager om Leverantören anser det nödvändigt. Incidentrapport ska skrivas om Leverantören eller SL anser det nödvändigt.*

5. Analys av behov och förutsättningar

5.1 Syfte

Vid mötet med landstingets stödjande funktion inom IT-säkerhet, SLL SOC (eng: information security operations center), diskuterades vilka fördelarna skulle kunna vara med att ha en landstingsgemensam klassificeringsmodell med gemensamma prioriteringsnivåer. En syftesbeskrivning för prioriteringsnivåer definierades enligt följande:

Alla tolkar allvarligheten på samma sätt. Detta leder till samma prioritering görs vilket kortar ner ledtider och säkerställer att adekvata resurser tillsätts för att hantera incidenter.

Vid övriga möten framkom inga invändningar mot denna syftesbeskrivning.

5.2 Omfattning på prioritetsnivåer

Under mötena diskuterades frågan om prioritetsnivåer bör omfatta incidenter som rör informationssäkerhet eller enbart IT-säkerhet. Begreppet informationssäkerhet innebär skyddet av informationstillgångar oavsett var den lagras eller hanteras. Begreppet kan exempelvis även inbegripa information i form av kunskap hos enskilda medarbetare. Begreppet IT-säkerhet är en delmängd av informationssäkerheten och handlar om skyddet av information som lagras och hanteras med hjälp av informationsteknik, IT.

Under mötena konstaterades att det är relevant med prioriteringsnivåer som omfattar informationssäkerhetsincidenter, det vill säga det vidare begreppet. Det är dock troligt att de mest allvarliga incidenterna, med störst konsekvenser, kommer att vara IT-säkerhetsrelaterade incidenter, det vill säga sådana som berör information som hanteras med hjälp av IT.

5.3 Målgrupper och behov

Under mötena diskuterades vilka grupper, funktioner och personer inom landstinget som bör känna till hur incidenter klassificeras och som skulle kunna ha nytta av gemensamma prioriteringsnivåer. Nedan redovisas de målgrupper som identifierades och de identifierade behoven.

5.3.1 Mottagare av IT-säkerhetsmeddelanden

SLL SOC arbetar för närvarande med att etablera en tjänst som innebär utskick av relevanta IT-säkerhetsmeddelanden till landstingets förvaltningar och bolag. Meddelanden kommer att innehålla aktuell information om sårbarheter som prioriterats samt rekommenderade åtgärder och förhållningssätt i syfte att förebygga säkerhetsrelaterade incidenter.

I samband med sådana utskick skulle det underlätta om sårbarheter kunde kommuniceras utifrån gemensamma prioriteringsnivåer.

5.3.2 Tjänsteman i beredskap

Landstinget är enligt socialstyrelsens föreskrifter [8] skyldig att bemanna rollen tjänsteman i beredskap[1], TiB.

En prioriteringsnivå skulle kunna underlätta TiB:s kommunikation med verksamheten i samband med incidenter. Tjänsteman i beredskap har dock behov att förstå exakt hur verksamhetspåverkan ser ut för att kunna bedöma behovet av åtgärder. Kommunikation utifrån enbart prioriterings-nivåer är därför inte tillräcklig. Behovet av landstingsgemensamma prioriteringsnivåer för TiB finns men bedöms inte vara stort. TiB har ett större behov av att det finns i förväg utarbetade kontinuitetsplaner i verksamheten.

5.3.3 Lokal krisledning (staber)

Lokal krisledning vid landstingets verksamheter, framförallt vård och trafik, skulle kunna vara en målgrupp för prioritetsnivåer av informationssäkerhetsincidenter. Vid incidenter av de slag att lokal krisledning kopplas in är det troligt att mer information än enbart prioritetsnivåer måste kommuniceras med både IT-driftsanasvariga, tjänsteman i beredskap och SLL SOC.

5.3.4 Funktion för incidenthantering vid IT-drift

Funktion för incidenthantering vid organisationer med IT-drift inom landstinget bedöms ha behov av att använda definierade nivåer i sin kommunikation med SLL SOC. Funktion för incidenthantering utgör också troligen mottagare av IT-säkerhetsmeddelanden enligt avsnitt 5.3.1.

5.3.5 Chefläkare

Samma resonemang som kring lokal krisledning, se avsnitt 5.3.3 ovan.

---

[1] 1 § I varje landsting ska det finnas en funktion som ständigt är bemannad och som vid allvarlig händelse eller vid risk för sådan händelse har till uppgift att

1. ta emot larm,
2. verifiera uppgifter,
3. larma vidare,
4. initiera och samordna det inledande arbetet och
5. informera om händelsen.

Funktionen ska benämnas tjänsteman i beredskap.
Allmänna råd
Landstinget bör fastställa rutiner med kriterier för när en operatör vid en larmcentral ska kontakta tjänsteman i beredskap.
Vid ett larm bör tjänsteman i beredskap ha befogenhet att fatta de beslut som krävs för att initiera och samordna det inledande arbetet.

5.3.6 Systemägare och systemförvaltare

Systemägare definieras i landstingets riktlinjer för informationssäkerhet [6] på följande sätt:

"För varje IT-system och nätverk ska det utses en systemägare, med uppdrag att ansvara för informationssäkerheten rörande det system uppdraget gäller. Systemägaren ska besluta om nyutveckling, vidareutveckling och avveckling. Systemägaren ska vid behov utse systemförvaltare som ges uppdraget att inom givna ekonomiska ramar ta det funktionella ansvaret för systemet."

Systemägarroll innehas ofta av objektägare eller objektägare IT i landstinget.

Prioriteringsnivåer skulle kunna underlätta systemägares och system-förvaltares kommunikation med SLL SOC i samband med incidenter.

5.3.7 Beställarfunktioner för IT

För denna målgrupp skulle nivåer för skademedömning framför allt vara intressant ur uppföljningssyfte.

5.3.8 Verksamhetsägare

För denna målgrupp skulle nivåer för skadebedömning framför allt vara intressant ur uppföljningssyfte.

5.4 Analys av existerande modeller

Under arbetet har tre modeller identifierats. En modell är framtagen för klassificering av informationssäkerhetsincidenter (Karolinska Universitetssjukhuset). Två modeller används för prioritering av IT-incidenter (landstingsstyrelsens förvaltning/SLL IT samt trafikförvaltningen). Trafikförvaltningens prioriteringsnivåer är inskrivna i avtal med driftleverantör och kan ändras först i samband med att nytt avtal skrivs.

Samtliga tre modeller är utformade för att framför allt hantera incidenter där *tillgängligheten* till information är påverkad. Nivådefinitioner från Karolinska universitetssjukhuset och SLL IT utgår från verksamhets-påverkan och går därför att tillämpa även för incidenter där informationens *riktighet* befaras vara påverkad. Nivådefinitionerna från trafikförvaltningen å andra sidan utgår från perspektivet IT-system. Ingen av nivådefinitionerna är direkt tillämpbara på incidenter där information befaras vara *röjd för obehörig*.

5.5 Slutsats och rekommendation

Utredningen konstaterar att en landstingsgemensam modell kan tillämpas i den betydelsen att incidenter klassificeras utifrån gemensamma nivåer för

skada och prioritering. Utredningen har tagit fram ett förslag till klassificeringsmodell med nivåer avseende skada och prioritering gällande IT-säkerhetsrelaterade incidenter. Förslaget utgår från den modell som används inom SLL IT vid landstingsstyrelsens förvaltning. Förslaget redovisas närmare i kapitel 6.

Föreslagna nivåer föreslås utvärderas och färdigställas av landstingets stödjande funktion inom IT-säkerhet, SLL SOC (eng: information security operations center). SLL SOC har i uppdrag att minska omfattning och skadeverkan av IT-säkerhetsrelaterade hot och incidenter genom att stödja landstingets förvaltningar och bolag att upptäcka och hantera dessa. När nivåerna är tillräckligt utprovade och förädlade av SLL SOC föreslås att landstingsdirektören fastställer dessa i en tillämpningsanvisning. Utvärdering och justering avser främst att säkerställa att modellen blir ändamålsenlig i förhållande till identifierade målgruppers behov.

Det har i tidigare uppföljningsarbete [7] konstaterats att det systematiska informationssäkerhetsarbetet inom landstinget fortfarande är i ett utvecklingsskede och att brister finns i viktiga styrningsprocesser. För närvarande saknas det dessutom en landstingsgemensam process för uppföljning av avvikelser och incidenter inom informationssäkerhet. Mot denna bakgrund är bedömningen att det finnas en påtaglig risk att den avsedda effekten av en gemensam klassificeringsmodell uteblir om inte samtidigt en landstingsgemensam process för uppföljning av avvikelser och incidenter införs och stärkande åtgärder avseende styrning och uppföljning vidtas inom informationssäkerhetsområdet.

Negativa konsekvenser av att införa en landstingsgemensam klassificeringsmodell med fastställda nivåer rör ekonomiska konsekvenser som är förknippade med ev. behov av att reglera gemensamma nivåer i avtal. Kostnader bedöms även kunna uppstå till följd av delvis förändrade arbetsätt och utbildningsinsatser.

Bland de positiva effekterna finns vinster i form av mer effektiv uppföljning av informationssäkerhetsincidenter och på sikt en mer effektiv hantering av informationssäkerhetsincidenter med kortare ledtider. Framförallt underlättar en sammanhållen struktur med tydliga nivåer SLL SOC:s dialog med förvaltningar och bolag kring it-säkerhetsrelaterade incidenter. För att dessa vinster ska falla ut till fullo rekommenderas att det införs ett landstingsgemensamt system för rapportering av avvikelser och incidenter inom informationssäkerhet samt att stärkande styrningsåtgärder vidtas inom området.

Utredningens samlade bedömning och rekommendation är att landstingsdirektören, efter utvärdering och erforderlig justering, beslutar om

fastställande av landstingsgemensam klassificeringsmodell för informationssäkerhetsincidenter enligt förslaget i denna promemoria. Utvärdering och justering föreslås ske av landstingets stödjande funktion inom IT-säkerhet, SLL SOC, och avser främst att säkerställa att modellen blir ändamålsenlig i förhållande till identifierade målgruppers behov.

6. Förslag på nivåer avseende skada och prioritering för informationssäkerhets-incidenter

Utifrån analysen av identifierade behov och förutsättningar i kapitel 6 redovisas nedan ett förslag på klassificeringsmodell med nivåer för bedömning av informationssäkerhetsincidenter respektive IT-säkerhets-incidenter. Föreslagna nivåer föreslås utvärdas och vid behov justeras av landstingets stödjande funktion inom IT-säkerhet, SLL SOC (eng: information security operations center) innan fastställande av landstingsdirekören. Utvärdering av modellen behöver också ske avseende uppföljning av avvikelser.

6.1 Nivåer – informationssäkerhet

Föreslagna nivåer utgår från formuleringar som används i SLL IT:s incidentmodell avseende verksamhetspåverkan. Dessa nivåer har använts en längre tid inom SLL IT och är väl beprövade. För SLL SOC är det viktigt att dialog kring nivåer fungerar bra med SLL IT som sköter driften av stora delar av central IT-infrastruktur i landstinget.

Tillägg i nivåerna har gjorts för att omfatta incidenter där skyddsvärd information röjs. Hänsyn har även tagits till landstingets modell för riskbedömning gällande informationssäkerhet samt till landstingets modell för informationssäkerhetklassificering[2]. Nivåerna bör inte avvika allt för mycket från fastställda konsekvensnivåerna i dessa modeller.

[2] Tillämpningsanvisningarna LS 2016-0067 Hantering av informationstillgångar samt LS 2016-0067 Riskhantering.



Prio 4 – Låg

Påverkar inte verksamhetens produktivitet. Tillfällig lösning finns framtagen och är tillgänglig.

Misstänkt röjande av information orsakar mindre problem eller mindre olägenheter för verksamheten.



Prio 3 – Medel

Påverkar verksamhetens produktivitet. Tillfällig lösning ej framtagen.

Misstänkt röjande av information som orsakar problem i verksamheten.



Prio 2 – Hög

Produktivitet allvarligt begränsad.

Misstänkt röjande av information som har en betydande kortsiktig effekt på verksamheten eller taktiska mål.



Prio 1 -Kritisk

Kritiska verksamhetsprocesser kan inte genomföras.

Misstänkt röjande av information har en allvarlig inverkan på långsiktiga strategiska mål eller äventyrar kritiska verksamhetsprocesser.

6.2 Nivåer kopplat till IT-säkerhet

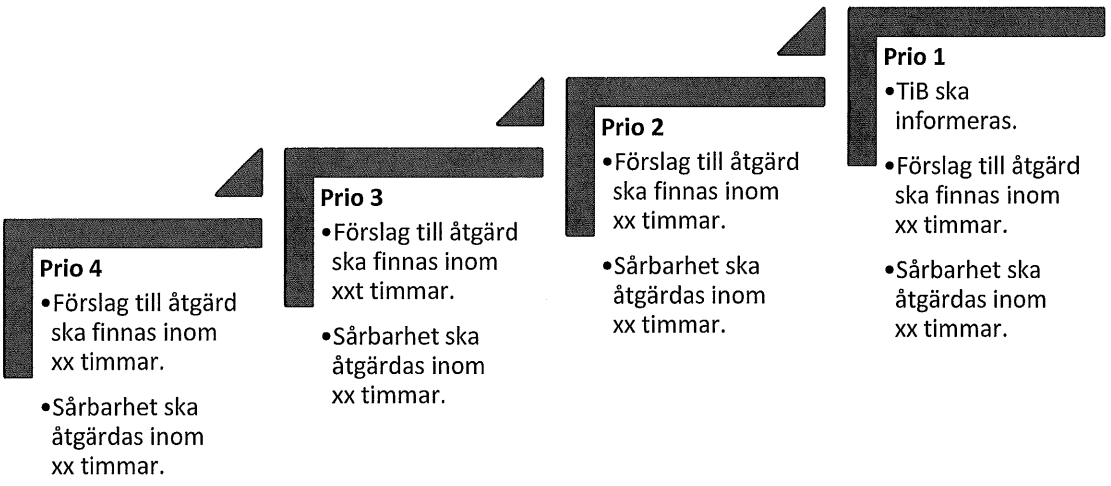
I tabellen nedan ges ett förslag till konkretisering av de föreslagna nivåerna till specifika typer av IT-säkerhetsrelaterade incidenter (skadlig kod, sårbarheter i IT-system samt tillgänglighets-attacker). Förslaget behöver ytterligare utprovning av SLL SOC och vid behov justering för att säkerställa att de fungerar i relation till landstingets förvaltningar och bolag.

Prio 1 - Kritisk	Skadlig kod med omfattande spridning.
	Sårbarhet som får en eviromental score enligt CVSS* definieras som critical (>9).
	DDOS attack mot verksamhetskritiska system.
Prio 2 – Hög	Skadlig kod med flertalet drabbade användare.
	Sårbarhet som får en eviromental score enligt CVSS* definieras som high (7,0-8,9).
	DDOS attack med risk för spridning mot verksamhetskritiska system.
Prio 3 – Medel	Skadlig kod som är intressant för SLL SOC (eng: information security operations center.
	Sårbarhet som får en eviromental score enligt CVSS* definieras som medium (4.0-6.9).
Prio 4 – Låg	Skadlig kod som drabbat en användare.
	Sårbarhet som får en eviromental score enligt CVSS* definieras som low (0,1-3,9).

**The Common Vulnerability Scoring System, CVSS.*

6.3 Åtgärder kopplat till nivå

I figuren nedan ges ett förslag till struktur gällande åtgärdstider kopplat till nivåerna. Strukturen behöver ytterligare utprovning av SLL SOC och åtgärdstider fastställas för att säkerställa att de är implementerbara i landstingets förvaltningar och bolag.



7. Referenser

[1] Avtal DIT09 – Driftupphandling IT 2009 – Bilaga 2 Servicenivåer och viten – 2009-06-10 – Diarienummer: SL-2007-3627-018
[2] Bilagor till riktlinjer informationssäkerhet – 2016-03-29 – Dokumentnr: STAB0508
[3] Incidenthantering inom SLL IT – Processbeskrivning - Processbeskrivning_Incident_Management_V3.1.1_2016-04-26.doc
[4] Informationsteknik – Ledningssystem för tjänster –Del 1: Krav (ISO/IEC 20000-1:2011, IDT)
[5] Översyn av roller och ansvar gällande hantering av it-säkerhetsincidenter, LS 1404-0548
[6] Riktlinjer för informationssäkerhet inom Stockholms läns landsting, LS 2016-0646, daterad 2015-11-03
[7] Efterlevnad av landstingets riktlinjer för informationssäkerhet – strategisk nivå. Uppföljning år 2015. LS2015-1394.
[8] Socialstyrelsens föreskrifter och allmänna råd om (SOSFS 2013:22) katastrofmedicinsk beredskap
[9] Terminologi för informationssäkerhet - SIS-TR 50:2015