Hot- och riskanalys
SYSteam Cross Landstinget Västernorrland
RAPPORT

Fastställd av
Datum:
Sign:

INNEHÅLL

Bilagor

Bilaga 1 Scenarier, SYSteam Cross
Bilaga 2 Förteckning av hot mot Landstinget i Västernorrlands verksamhet (ej SYSteam Cross- specifik) som framkom vid hot- och riskanalyser 2009-12-01

1 INLEDNING

1.1 Bakgrund

Analysen är beställd och genomförd som ett led i säkerhetsarbetet inom ramen för fortsatt utveckling och förvaltning av systemet SYSteam Cross.

1.2 Bemanning

Namn:	Titel:	Tillhörighet:
Jonas Bylund	Systemförvaltare SYSteam Cross	Landstingsstaben IT
Micael Fichtel	Överläkare	Sundsvall
Jonas Hallberg	IT-tekniker	IT Drift och Support
Ronny Hedlund	Projektledare	Landstingsstaben IT
Gunnar Johansson	Överläkare med. Centrum	Örnsköldsvik
Staffan Magnusson	Överläkare	Sundsvall
Lennart Selander	IT-konsult DBA	IT Drift och Support
Bertil Svelander	Förvaltningsledare SYSteam Cross	Landstingsstaben IT
Leif Wennström	Huvudprojektledare	SC Projektet
Annica Wredenborg	IT-konsult	SC Förvaltning
Eva Ölund	Informationssäkerhetschef	
Ola Nilsson	Analysledare	Logica
Lars Rahm	Bitr analysledare	Logica

1.3 Allmänt

Hot- och riskanalysen genomfördes i konferensrum ”Ripan” i Landstinget Västernorrlands lokaler i Härnösand. Analysen påbörjades kl 0800 och avslutades ca kl 1800. Analysen genomfördes i god anda och samförstånd.

1.4 Genomförande

1.4.1 Redovisning av analyserat objekt

[

Innan analysen påbörjades genomförde Eva Ölund, Lars Bohlin och Stefan Alexandersson korta dragningar avseende bakgrunden till genomförandet av dagens hot- och riskanalys. Bertil Svelander föredrog uppbyggnaden av SYSteam Cross samt dess tekniska infrastruktur som inledning på analysen.

Förekomsten av insider diskuterades också. Med insider menas i detta sammanhang en person med logisk eller fysisk tillgång till systemet SYSteam Cross.

1.4.2 Hotframtagning i form av ”brainstorming”

”Brainstormingen” genomfördes enligt traditionell modell för scenariobaserad hot- och riskanalys. Deltagarna skrev ner hot och diskuterade sinsemellan och skapade därmed möjligheter att kvantifiera och verifiera flera befintliga hot mot systemet genom samverkan över olika delområden i systemets struktur, omgivande rutiner och processer.
Hot som tas fram i denna scenariobaserade hot- och riskanalys är indelade i sekretesshot (Se), riktighetshot (Ri), tillgänglighetshot (Ti) samt generella hot (Ge). Generella hot är hot som omspänner flera av föregående kategorier eller inte passar i någon av kategorierna.

1.4.3 Grovbedömning av sannolikhet och skada

Hoten grovbedömdes avseende sannolikhet och skadekonsekvens på tregradiga skalor. Bedömningen resulterade i ett riskvärde mellan 0 och 4 där 4 påvisar den allvarligaste risken.

Sannolikheten för skada angavs i tre steg enligt följande:

Sannolikhet	**Händelse som inträffar**
Hög sannolikhet	Hotet inträffar oftare än en gång per sex månader.
Medel sannolikhet	Hotet inträffar en gång under perioden sex till 24 månader.
Låg sannolikhet	Hotet inträffar färre än en gång per två år.

Skadekonsekvens angavs i tre steg enligt följande:

Konsekvens	**Exempel på skador**
Allvarlig skada	Strategisk förlust, fara för person, massiv eller kritisk sekretess-, riktighets- eller tillgänglighetsförlust.
Betydlig skada	Brott mot regelverk eller rättsliga krav. Märkbara konsekvenser, omprioriteringar nödvändiga.
Lindrig skada	Märks i den dagliga hanteringen, med inga eller små omprioriteringar som följd.

Allvarlig skada innebär strategiska förluster (förlust av sekretess, riktighet och tillgänglighet) exempelvis som följd av brand i datorhall där system går förlorade.

Betydlig skada innebär en skada som inte låter sig åtgärdas vare sig snabbt eller enkelt. Någon form av verksamhetsstörning, informationsförlust eller

motsvarande ska ha inträffat. Som riktmärke tillämpas normalt att samtliga överträdelser av vad som anges i författningar och bestämmelser är betydlig skada.

Lindrig skada innebär en skada som snabbt låter sig åtgärdas eller repareras exempelvis en server som går ner och måste startas om.

Utifrån angiven sannolikhetsfrekvens och skadekonsekvens får varje hot ett riskvärde enligt följande:

Sannolikhet				
	Hög	2	3	4
	Medel	1	2	3
	Låg	0	1	2
		Lindrig	Betydlig	Allvarlig
		Skada		

Grovbedömningen präglades genomgående av samförstånd mellan deltagarna. Viss diskussion föregick bedömningarna men konsensus nåddes i samtliga fall.

1.4.4 Detaljanalys av hoten och förslag till åtgärder

Diskussionen i gruppen rörande grovanalys med riskvärdering var mycket intensiv och tidkrävande. Detaljanalysen kom inte att genomföras i forum utan har i efterhand sammanställts av analysledaren. Diskussion har skett underhand med analysgrupppens medlemmar enskilt om detaljanalysens formuleringar och särskild vikt har lagts vid åtgärdsförslagen och att nå en gemensam uppfattning om dessa.
Samtliga hot/risker med ett riskvärde större än 2 detaljanalyserades och diskuterades med gruppen.

2 HOTREDOVISNING

2.1 Hot som har beaktats inom ramen för analysen

Nr	Kod	Risk	Hot
1	Ge	4	Systemfel i läkemedelslista.
2	Ri	4	Spärrar och rimlighetstester saknas vid medicinförskrivning och formulärinmatning.
3	Ri	4	Felaktig integration med folkbokföringsregister.
4	Ge	4	Remissbeställning och remissvar matchar inte varandra.
5	Se	4	Journalinformation skrivs ut på fel skrivare.
6	Se	4	Skyddad information röjs.
7	Ge	4	Mycket långa ledtider vid beställningar om förändringar i systemet.
8	Ge	4	Felkonsturerad lablista kan leda till felbehandlingar.
9	Ge	4	Administratör kan stänga av loggar i SC.
10	Ge	4	Funktionalitet ej fullständig vad gäller sammanhållen journalföring.
11	Ge	4	SC har ingen fungerande kontexthantering.
12	Se	4	Behörighetstilldelning ej fullständig enligt PDL.
13	Ge	4	Gruppering av laboratorieprover felaktig.
14	Ge	4	Felaktig information (indata) från tredje part.
15	Ge	4	Personuppgifter kan röjas vid kommunikation.
16	Ge	4	Felaktig behörighet leder till felbehandling.
17	Ge	4	Lösenord till databaser röjs.
18	Ge	4	Autenticeringsprocessen mellan databas och klient falerar.
19	Ge	4	Design och uppbyggnad av journalssystem innebär att felbehandling kan ske.
20	Ge	4	Dålig teknisk integration mellan flexlab och SC.
21	Ge	4	SC uppfyller inte kraven i PDL.
22	Ge	4	Signeringslista kopplas ej automatiskt till patient i systemet.
23	Ge	4	Personuppgifter riskerar att komma obehörig till del. Jfr 6 och 23.
24	Ge	4	Information från övriga källor blir inte tillgänglig och patient kan felbehandlas.
25	Se	4	Svaga lösenord leder till att patientuppgifter röjs.
26	Ge	4	Brister i moduler eller sammankoppling av moduler leder till systemkrascher.
27	Ge	3	Ej användarvänligt gränssnitt leder till felbehandling/felhantering.
28	Ge	3	SC tröghet leder till förseningar i handläggning.
29	Ge	3	Känslig information används i test.
30	Ge	3	Distribuerade transaktioner orsakar inkonsistenta databaser.
31	Ge	3	Organisationsförändringar inom landstinget leder till brister i hantering av SC.
32	Ge	3	Underbemanning i förvaltningsorganisation leder till förseningar och kvalitetsbrister.

33	Ge	3	Journalstruktur och innehåll i db inte samma vilket ger inkonsistena db.
34	Ge	3	Förändringar i produktionssmiljön ger störningar i verksamhetssystemen.
35	Se	3	Skrivbyråer anlitas för journalföring.

2.2 Hot som inte har beaktats inom ramen för analysen

Nr	Kod	Risk	Hot
36	Ge	2	Det saknas koppling mellan adressregister och brev.
37	Ge	2	Sorteringen av information i Kovis har stora brister.
38	Ge	2	Rättningar av fel sker med script.
39	Ge	2	Ronderande PC har låg batterikapacitet.
40	Ge	2	Ronderande PC tappar W-lankoppling under rond.
41	Ti	2	Planerat underhåll tar för lång tid.
42	Ge	2	Minibackup testas inte enligt rutin.
43	Ge	2	Makulering av recept sker endast i VS och inte på Apoteket.
44	Ge	2	Nätverkstimeout genererar noll svar vid utsökning av läkemedel.
45	Ge	2	Behovet av regressionstester ökar vid integration.
46	Ge	1	Dubbeldebitering kan ske vid utbyte mellan LISA och SC.
47	Ge	1	SC infört men används inte.
48	Ge	1	Brister i statistik.

2.3 Grafisk sammanställning riskvärden

Hög sannolikhet	**36,38,39,40,41,43,44,45**	**27,28,31,32,33,34,35**	**1,2,3,4,5,6,7,8,9,10,11, 12,13,14,15,16,17,18,19, 20,21,22,23,24,25,26**
Medel sannolikhet	**46,47,48**		**29,30**
Låg sannolikhet			**37,42**
	Lindrig skada	**Betydlig skada**	**Allvarlig skada**

Den grafiska sammanställningen över riskvärden visar hur dessa fördelar sig i sannolikhet och skada. Ju längre åt höger i matrisen som koncentrationen av värden ligger, ju allvarligare är den bedömda skadan. Ju högre upp i matrisen riskvärdena ligger, ju högre är sannolikheten att de inträffar. Således är en koncentration högt upp till höger det farligaste utfallet av en hot- och riskanalys.

Man kan här även göra en reflektion kring de risker som har getts ett riskvärde 2, som förekommer ofta men med en bedömd lindrig skada (hot nr 36,38,39,40,41,43,44 och 45). Att på sikt åtgärda även dessa kan vara av betydelse då de är så frekventa att de utgör tidtjuvar för verksamheten samt att de med tiden kan komma att utgöra betydande irritationsobjekt för verksamheten och även om skadan för verksamheten är lindrig kan landstingets oförmåga att hantera problemet leda till en ledningskris.

2.4 Särskilda beaktanden

I samband med analysen framkom en rad hot som rör Landstinget i Västernorrlands informationshantering i allmänhet. Dessa hot är i sig, i flera fall mycket allvarliga och kan om de inträffar tillfoga landstinget svåra skador, men även äventyra patienters säkerhet. Dessa hot är förtecknade i bilaga 2. Någon särskild redovisning av dessa risker görs ej här.

3 SAMMANFATTNING OCH SLUTSATS

3.1 Sammanfattning

Totalt framkom 48 hot mot SYSteam Cross under analysen. Av dessa bedömdes 36 med riskvärde 4 eller tre, 25 av dessa gavs riskvärde 4 och resterande 11 riskvärde 3. Bedömningen av dessa hot var således sådan att om de inträffar kommer de att allvarligt skada Landstinget i Västernorrland. De skadeverkningar som kan inträffa kan övergripande beskrivas som att:

- Patienter skadas;
- Verksamheten åsamkas ekonomiska förluster;
- Förtroendet för landstinget skadas.

Utifrån redovisningen av hot mot SYSteam Cross som framgår av bilaga 1 kan hoten översiktligt grupperas i tre grupper som bör åtgärdas. Dessa huvudgrupper är:

- Brister i teknik och funktionalitet;
- Brister i laguppfyllnad, PDL och PUL;
- Kunskap och medvetenhet.

Utöver hot tillhörande dessa grupper som sammmantaget utgör den större delen av hoten finns några enskilda hot som bedöms allvarligt kunna skada landstingets verksamhet. Dessa redovisas och diskuteras under pkt 3.1.3 Övrigt.

3.1.1Brister i teknik och funktionalitet

Med brister i teknik och funktionalitet menas här sådana hot som i allt väsentligt beror på att det finns brister i den tekniska lösningen bakom SYSteam Cross. Denna grupp av hot är i särklass störst. Bristerna är välkända i organisationen och man har i flera fall framtagna förslag till lösningar. De brister som konstaterats innebär exempelvis att information från provtagning ej på ett tillförlitligt sätt kan kopplas till rätt patient, att överdosering kan ske, att patienter kan felmedicineras eller felbehandlas. Bristerna utgörs exempelvis av att gränssnittet som vårdpersonalen arbetar i inte är användarvänligt eller begripligt, att kopplingen och kommunikationen mellan SYSteam Cross's olika moduler har brister och att rutiner kopplade till journalföringen är behäftade med brister. Likaså finns uppenbara brister i den interna ändringsrutinen gentemot SYSteam samt hur förbättringsförslag eller incidenthantering sker och hur dessa återkopplas till verksamheten. Vad gäller rapporteringsrutiner finns åtminstone två, dels i avtalet mellan landstinget och leverantör samt i förvaltningsorganisationens kommunikationsplan. Det har inte framgått om dessa är liktydiga eller redovisar olika processer och tidsförhållanden, däremot är det uppbart att de var för sig inte följs. Det är dessutom av vikt att förändringar i SYSteam Cross kan genomföras inom rimliga tidsförhållanden. Sammanfattningvis innebär dessa hot att patientsäkerheten kraftigt äventyras.

Att åtgärda dessa hot kan göras på flera sätt och parallellt. Att skärpa upp och följa ändringsrutier och återkopplingen till verksamheten kan bedömas som mycket väsentligt för att minska hoten. Dessutom, som nämndes ovan, är vetskapen om vad som tekniskt utgör problemen tämligen god inom förvaltningsorganisationen, varför det kan bedömas att man relativt snabbt kan ta fram såväl tekniska beskrivningar av dessa brister samt ta kravspecifikationer som underlag vid diskussion rörande förbättringar av SYSteam Cross med leverantör För två av hoten, nr 3 och 13 är lösningar framtagna och är på väg att implementeras. Dessutom pekar verksamheten på ett tydligt utbildningsbehov då systemet upplevs som svårt att använda samt att en del av hotbilden de facto genereras av handhavandefel beroende på kunskapsluckor hos personalen. Att därför tillhandahålla kontinuerlig utbildning för användargrupperna kan bedömas som en bra hotreducerande åtgärd.

3.1.2Brister i laguppfyllnad

Brister i laguppfyllnaden gäller såväl PUL som PDL samt möjligen Sekretess och offentlighetslagen (2009:400). Konsekvenserna som detta får är exempelvis att känslig information om patienter kan röjas samt att riktigheten och tillgängligheten till patientinformationen inte kan garanteras när vårdpersonalen behöver den. Bristerna står såväl att finna i den tekniska lösningen som rutiner, men även i brister i kunskap om gällande lagstiftning. Att ta fram en kravspecifikation avseende PDL och PUL gentemot SYSteam Cross är därför särskilt viktig.

3.1.3Övriga

Bland de övriga hoten finns några som initialt måste åtgärdas. Bland dessa är hot nummer nio särskilt allvarligt, det vill säga risken att en administratör kan stänga av loggar i SYStem Cross. Konsekvensen av detta skulle kunna vara förödande för landstinget, då man genom att kunna stänga av loggarna kan läsa, förändra eller ta bort information ur SYSteam Cross utan att det upptäcks. Särskilt allvarlig är bristen dessutom utifrån det perspektiv att bristen är spridd inom landstinget.

Andra hot som i detta sammanhang lyfts fram och som rekommenderas att landstinget åtgärdar rör organisationen kring SYSteam Cross, hot nr 31 och 32. Av dessa hot framgår det att organisationsförändringar liksom underbemanning inom landstinget får negativa konsekvenser för såväl förvaltning som utveckling av systemet. Konsekvenserna är att förseningar av leveranser kommer att inträffa, bristande funktionalitet kommer att finnas kvar under onödigt lång tidsperiod och fortsätta skapa irritation inom verksamheten.

3.2 Slutsats

Slutsatsen som kan dras är att SYSteam Cross har allvarliga brister som ytterst äventyrar patientsäkerheten och allvarligt kan skada förtroendet för Landstinget i Västernorrland. Skulle hoten inträffa kommer de allvarligt att skada landstingets verksamhet och varumärke.

De åtgärder som föreslås påbörjas under 2010:

- Att upprätta en detaljerad åtgärdsplan med en till verksamheten kommunicerad tidplan över de åtgärder som är nödvändiga för att komma till rätta med de brister som är kopplade till systemets teknik och funktionalitet.
- Att upprätta en detaljerad åtgärdsplan över de brister som är kopplade till brister i laguppfyllnad, såväl PUL som PDL samt möjligen Sekretess och offentlighetslagen (2009:400). Jfr Ernst & Young's granskning.
- Omöjliggöra att administratörer kan stänga av och radera loggar.
- Kontinuerligt utbilda användare i SYSteam Cross.
- Utbilda verksamheten i hantering av sekretessbelagd information.
- Se över ändringsrutin avseende fel och brister i systemet samt förbättra information och återkoppling till verksamheten.
- Skapa arbetsro för förvaltningsgruppen kring SYSteam Cross.