Landstingsrevisionen

Landstingsstyrelsen

Granskning av IT-säkerheten inom Landstinget i Jönköpings län

Landstingets revisorer har, med hjälp av sakkunnigt biträde, gjort en granskning av informations- och IT-säkerheten inom landstinget. Syftet med granskningen är att bedöma om landstingets IT-säkerhet, ur ett övergripande perspektiv, är tillräcklig. Begreppet IT-säkerhet inbegriper i granskningen även informationssäkerhet. Landstingets revisorer har beslutat att ställa sig bakom revisionsrapporten.

Resultatet av granskningen redovisas övergripande i bifogad revisionsrapport ”IT-säkerhet – externt och internt intrångstest samt granskning av IT-säkerhetsprocesser”, daterad september 2013.

Revisorernas bedömning

Granskningen visar att det finns en övergripande styrning av informations- och IT-säkerheten med processer, rutiner och dokumentation som stöd. Landstingets riktlinjer för informationssäkerhet är under uppdatering för att säkerställa att kraven enligt patientdatalagen beaktas.

Resultatet av genomförda tester visar på brister i IT-säkerheten och att landstinget därmed inte når upp till en adekvat säkerhetsnivå. Bedömningen är dock att landstinget på en övergripande nivå har en god medvetenhet om behovet av att arbeta med IT- och informationssäkerhet. Säkerhetsmedvetandet och ambitionen hos berörd personal bedöms vara hög, vilket positivt bedöms bidra till det fortsatta förbättringsarbetet avseende IT-säkerhet.

Landstingets kansli
Landstingsrevisionen
Hermansvägen 7
Box 1024
551 11 Jönköping

Telefon 036-32 40 01
E-post landstinget@lj.se
Hemsida www.lj.se

Plusgiro: 10 50 00-4
Bankgiro: 5216 2849
Orgnr: 232100-0057

Revisorernas rekommendationer

Revisorerna rekommenderar landstingsstyrelse att se till

- att arbetet med genomförd riskanalys och åtgärdsanalys fortsätter och följs upp samt baseras på de iakttagelser och rekommendationer som redovisas i granskningsrapporten

- att fokus i detta arbete läggs på att åtgärda de mest kritiska riskerna, särskilt i den interna IT-miljön, varefter resterande iakttagelser prioriteras

- att de åtgärder som genomförs granskas och revideras efter införandet, för att säkerställa att avsedda effekter uppnås.

Revisorernas uppföljning av vidtagna åtgärder

Revisorerna avser följa upp genomförandet och resultatet av ovanstående rekommendationer i samband med träff med landstingsstyrelsen.

Doris Johansson
Ordförande

Arnold Carlzon
Vice ordförande

Revisionsrapport

IT-säkerhet

Externt och internt intrångstest samt granskning av IT-säkerhetsprocesser

Landstinget i Jönköpings län

Kerem Kocaer
Johan Elmerhag
Jean Odgaard

September 2013

pwc

Innehållsförteckning

Inledning

Revisorerna i Landstinget i Jönköpings län har beslutat att genomföra en granskning av IT-säkerheten. PwC har fått uppdraget att genomföra granskningen, vilken utförts i form av intrångstester mot delar av landstingets system samt granskning av IT-säkerhetsprocesser. Granskningen har utförts under våren 2013.

Bakgrund

Landstingen blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker. Kommunikationen med omvärlden ökar i omfattning och systemen blir mer integrerade såväl inom landstinget som med andra intressenter. Ofta används system och applikationer av externa aktörer såväl som att medborgare har tillgång till information som kommer från journalsystem. Ett aktuellt exempel är att det nu i Uppsala går att nå sin journal på nätet och att detta ska lanseras som en nationell tjänst för alla landsting.

Detta ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Informationen måste skyddas mot obehörig åtkomst samtidigt som den skall finnas tillgänglig och dessutom vara tillförlitlig - *rätt information i rätt tid och för rätt personer*.

Om landstinget inte har ett väl fungerande säkerhetsarbete och ett strukturerat arbetssätt för att hantera IT-säkerheten finns risker att känslig information, t ex personuppgifter, kan läcka ut till obehöriga. Utöver detta finns det även risk för att det uppstår fel i kritiska processer p g a att information är felaktig eller inte finns tillgänglig. Sammantaget kan detta leda till att landstingets trovärdighet ifrågasätts såväl som till ekonomiska förluster och förlorat anseende.

Genom granskning av säkerhet avseende teknik, identifieras eventuella riskområden där skydd av landstingets information saknas.

Mot bakgrund av detta har landstingets revisorer bedömt att en granskning av informations- och IT-säkerheten behöver genomföras. I detta dokument används termen IT-säkerhet för såväl informationssäkerhet som IT-säkerhet.

Revisionsfråga

Revisorerna önskar svar på följande revisionsfråga:

- **Är landstingets nuvarande IT-säkerhet tillräcklig och ansvarsförhållanden tydliga för att minimera risker för obehörigt intrång?**

För att besvara granskningens övergripande revisionsfråga har följande kontrollmål varit styrande för granskningen:

- Finns det en adekvat övergripande styrning av informations- och IT-säkerheten?
- Finns det styrande dokument, såsom policy och riktlinjer för informations- och IT-säkerhet?
- Finns ändamålsenliga rutiner för behörighet och lösenord?
- Hanteras icke önskvärda incidenteter på ett ändamålsenligt sätt?
- Hur är säkerheten avseende intrång av extern aktör?
- Hur är säkerheten avseende intrång av intern aktör?

Angreppssätt

Syfte, omfattning och avgränsning

Syftet med testerna och granskningen var att utvärdera landstingets interna och externa IT-säkerhet, att identifiera potentiella säkerhetsbrister samt att ge rekommendationer för riskreducerande åtgärder. Vidare har utvärdering och bedömning av systemen och IT-miljön som helhet genomförts, baserat på observationer under testets genomförande.

Uppdraget har utförts i tre delar, externa respektive interna intrångstester samt granskning av processer inom IT-säkerhet.

- **Externt intrångstest**
  I de externa testerna, vilka utfördes från PwC:s säkerhetslaboratorium, granskades landstingets tjänster som är nåbara från Internet. Hotbilden som illustreras var en extern så kallad hacker som försöker erhålla åtkomst till intressant information.

- **Internt intrångstest**
  I de interna testerna granskades landstingets interna IT-miljö på plats från det ordinarie interna nätverket. Hotbilden som illustreras i dessa tester är exempelvis en missnöjd anställd, konsult eller annan person som får tillgång till ett nätverksuttag i landstingets lokaler. Hotbilden är liknande om en persondator drabbas av skadlig kod (exempelvis ett trojanprogram) ansluts till det interna nätverket.

- **Granskning av IT-säkerhetsprocesser**
  I denna del av uppdraget granskades processer avseende IT-säkerhet inom landstinget. Granskningen innefattade även viss fokus på det bredare begreppet informationssäkerhet avseende övergripande styrning och styrande dokument. Resultaten från de externa och interna intrångstesterna användes också som bakgrund i de intervjuer som hölls.

De s.k. intrångstesterna har endast omfattat tester av en begränsad mängd servrar och tjänster. Målsystem, där t ex känslig information behandlas samt vilka IP-adresser som ingår i testerna, har specificerats i detalj under uppdragets första fas.

Metodik

Både de externa och interna intrångstesterna genomfördes i fyra steg: hotbildsanalys, generell informationsinsamling, intrångsförsök samt rapportering och sammanställning.

Ett flertal verktyg användes inledningsvis för att kartlägga resurserna på landstingets nätverk. Samtliga resurser som omfattades av testerna kartlades och identifierades. Avslutningsvis testades även de identifierade systemen och tjänsterna för eventuella säkerhetsproblem och brister. Detta för att kartlägga och bestämma de olika sätt som systemen kunde angripas på.

Efter insamling av information, utarbetades planer för hur det fortsatta arbetet skulle kunna genomföras, i enlighet med de scenarier som tidigare definierats. Under intrångssteget försökte vi erhålla behörighet eller på annat sätt kringgå säkerheten i de testade systemen. Samtliga tester i det första scenariot utfördes via Internet från PwC:s laboratorium i Stockholm.

Under det interna scenariot genomfördes testerna från lokaler inom Landstinget i Jönköpings län, varifrån målsystemen uppsöktes och attackerades.

Granskningen av processer inom IT-säkerhet utfördes genom intervjuer med berörda personer samt granskning av ett urval av relevant dokumentation. Följande roller intervjuades: IT-direktör, Områdeschef Systemförvaltning, Drift- och IT-säkerhetschef, Teamledare Systemutveckling, Enhetschef Applikation och infrastruktur samt Enhetschef Kundcenter. De huvuddokument som ingått i granskningen av IT-processer är:

Riktlinjer för informationssäkerhet, Krisplan för IT-centrum, Systemförvaltningsplan, samt processbeskrivningar inom ett antal område.

Rapporten har sakgranskats av berörda tjänstemän.

Resultat

Mot bakgrund av tekniska detaljer i rapporten har resultatet sammanfattats i en bilaga som är sekretessbelagd med stöd av sekretesslagen 2009:400 kapitel 18 paragraf 8.

Sammanfattande bedömning

Våra slutsatser är kopplade till de övergripande frågorna som föranlett denna granskning. Följande kontrollfrågor har varit styrande för granskningen.

- *Finns det en adekvat övergripande styrning av informations- och IT-säkerheten?*

  Ja, en övergripande styrning avseende informations- och IT-säkerhet finns på plats med processer, rutiner och dokumentation som stöd.

- *Finns det styrande dokument, såsom policy och riktlinjer för informations- och IT-säkerhet?*

  Ja, styrande dokument finns för övergripande styrning mot verksamheten avseende informations- och IT-säkerhet. Landstingets riktlinjer för informationssäkerhet är baserad på Ledningssystem för informationssäkerhet SS-ISO 17799. Riktlinjerna är under uppdatering för att säkerställa att kraven enligt patientdatalagen tas i beaktan.

- *Finns ändamålsenliga rutiner för behörighet och lösenord?*

  Ja, för vanliga användare finns tydliga och etablerade processer samt rutiner för hantering av behörigheter och lösenord. Dock bör rutiner för uppföljning av behörighetsnivåer kring priviligierade konton såsom användare med administrativa rättigheter stärkas (vilket noterats vid den tekniska säkerhetsgranskningen).

- *Hanteras icke önskvärda incidenteter på ett ändamålsenligt sätt?*

  Ja, etablerade och ändamålsenliga rutiner finns för hantering och uppföljning av incidenter. Landstinget har även en etablerad problemprocess för uppföljning och analys av uppkomna incidenter.

- *Hur är säkerheten avseende intrång av extern och intern aktör?*

  Resultatet av intrångstesterna visar tydligt vad effekterna av de identifierade bristerna i IT-säkerheten medför. Genom bristande rutiner kring säkerhetsuppdateringar, behörighetskontroll och konfiguration når landstinget inte upp till en adekvat IT-säkerhetsnivå avseende skydd mot obehörigt intrång. Positivt är att det finns en övervakningsfunktion som bidrar till att reducera sannolikheten för att ett intrång sker oupptäckt.

Är landstingets nuvarande IT-säkerhet tillräcklig och ansvarsförhållanden tydliga för att minimera risker för obehörigt intrång?

Vi bedömer att det finns en övergripande styrning avseende informations- och IT-säkerhet. Det finns tillräckliga processer, rutiner och dokumentation som stöd för detta. Dock visar resultatet av intrångstesterna en del svagheter i den tekniska IT-säkerheten.

Landstinget bedöms på en övergripande nivå ha en god medvetenhet om behovet av att arbeta med IT- och informationssäkerhet. Dessutom är säkerhetsmedvetandet och ambitionen hos IT-personalen hög, vilket bidrar positivt till framtida förbättringsarbete avseende IT-säkerhet.

PwC rekommenderar landstinget att fortsätta och följa upp genomförd riskanalys samt åtgärdsanalys baserat på de i denna rapport angivna iakttagelser och rekommendationer. Fokus bör vara att åtgärda de mest kritiska riskerna, särskilt i den interna IT-miljön, för att sedan prioritera resterande iakttagelser.

De åtgärder som genomförs bör revideras och granskas efter införande för att säkerställa att effekten av åtgärden är uppnådd. Detta kan exempelvis göras genom analys av utförda åtgärder, nya penetrationstester eller manuella kontroller.

2013-09-10

Kerem Kocaer	***Jean Odgaard***
Projektledare	***Uppdragsledare***