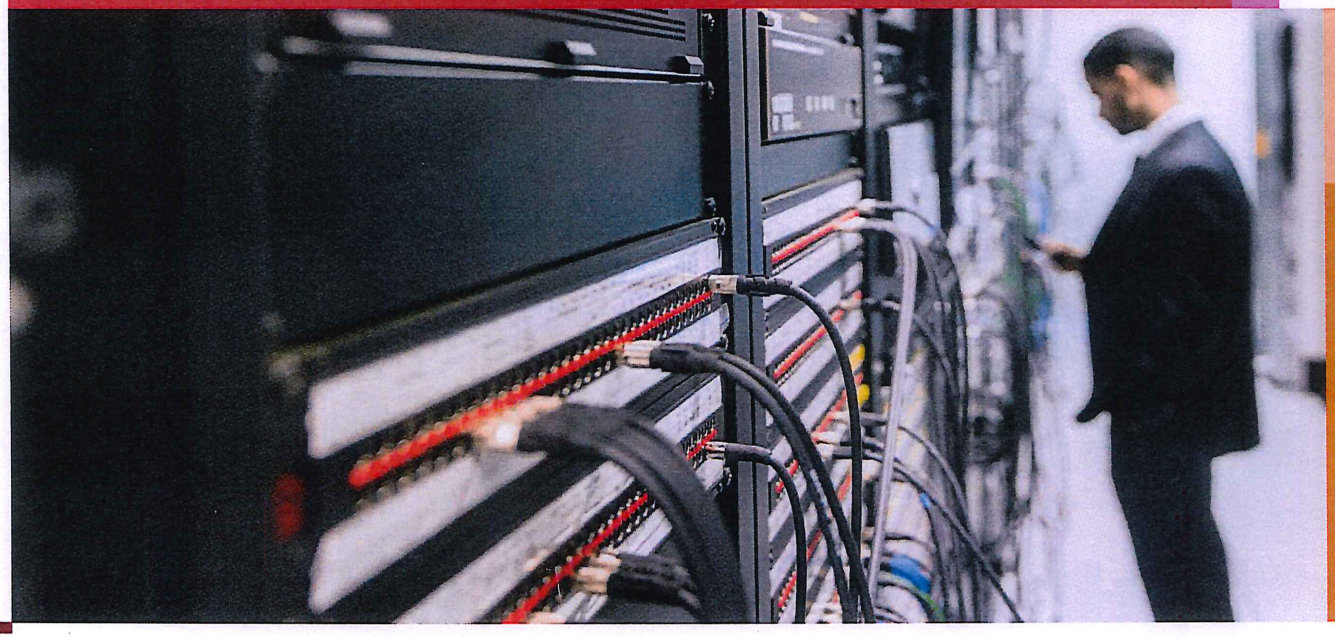
www.pwc.com/se

Region Halland

Granskning: IT-säkerhet - hälsokontroll ITM och Cybersecurity

17 augusti 2018



pwc

Innehåll

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Halland genomfört en översiktlig granskning av regionens IT-säkerhet. Granskningen omfattar regionens IT-enhet (IT- och serviceavdelningen) såväl som IT-verksamheten inom ett urval av regionens verksamheter. Syftet har varit att granska huruvida Region Hallands styrelse säkerställt att regionen arbetat systematiskt och ändamålsenligt med IT-säkerhet.

Rapporten avser att belysa följande övergripande revisionsfrågor:

1. Finns en tillfredställande intern styrning och kontroll för en effektiv och säker hantering av IT?
2. Har regionstyrelsen säkerställt att nuvarande tekniska IT- säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

Vår övergripande bedömning är att revisionsfråga 1 till viss del är uppfylld medan fråga 2 ej är uppfylld.

De främsta observationerna (och rekommendationerna):

- [redacted] Detta arbeta bör ledas av en arkitekt eller annan likande roll med övergripande ansvar för denna fråga.
- [redacted]
- [redacted] Det finns en avvecklingsplan men arbetet behöver intensifieras.
- [redacted]

Sammanfattning (forts.)

Det finns utvecklingspotential inom ett flertal områden;

- Rollen Informationssäkerhetsstrateg ligger i dag under IT-direktören, detta är olämpligt när informationssäkerhetsarbetet är kravställare på IT-organisationen. Rollen bör flyttas.
- I dag leds regionens informationssäkerhetsarbete av informationssäkerhetsstrategen som är sammankallande för ISSO-gruppen (består av representanter från olika förvaltningar). ISSO-gruppen tar fram underlag, rutiner och riktlinjer för beslut av direktören för aktuellt område.
- Efter vår granskning och efter att ha tagit del av rapporten "Stabilt IT Region Halland" är vår rekommendation att det genomförs en komplettering av den klassning som finns av regionens information för att ta fram en matris att knyta information och system till SLA:er, redundans, backuper, återläsningstider och IT-säkerhet m.m. Detta arbete kan med fördel ledas av informationssäkerhetsansvarig men genomföras av verksamheten.
- Regionens IT-verksamhet är utifrån granskningens perspektiv välfungerande. Att stora delar av driften sköts internt ses som positivt då detta borgar för en säker IT-miljö med möjlighet att ha större kontroll över den än vid outsourcing. Intern drift av IT-miljön minskar även beroendet mot externa aktörer. Ledningen bör säkerställa att medarbetare på IT-avdelningen ges möjlighet och förutsättningar till kompetensutveckling samt att resursbehov är tillgodosedda.

Sammanfattande bedömning

Uppfyllt
Delvis uppfyllt
Ej uppfyllt

	Kontrollmål	Bedömning
1	Finns aktuella och ändamålsenliga styrande dokument samt riktlinjer som är tillräckligt införda, implementerade och kända av organisationen?	
2	Sker uppföljning kring efterlevnad av de styrande dokumenten?	
3	[redacted]	
4	[redacted]	
5	[redacted]	
6	[redacted]	
7	Finns adekvat förmåga att hantera säkerhetsincidenter som har inträffat?	
8	Har regionen en godtagbar förmåga att återställa IT-stödet efter en incident?	
9	[redacted]	
10	Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?	

Bakgrund och syfte

Inledning

PwC har på uppdrag av revisorerna i Region Halland genomfört en översiktlig granskning av regionens IT-verksamhet med fokus på IT-säkerhet. Granskningen omfattar regionens IT-enhet samt IT-verksamheten inom ett litet urval av regionens verksamheter.

Resultatet av granskningen presenteras i denna rapport.

Bakgrund

Ett fungerande IT-stöd är av stor betydelse för Region Hallands verksamhet. Den moderna informationsteknologin ger möjligheter att höja kvalité, säkerhet och effektivitet i de olika verksamheterna samt sprida och öka tillgängligheten till information. IT är en förutsättning för att verksamheten skall fungera på ett effektivt och säkert sätt. Ett av de mest verksamhetskritiska systemen är vårdinformationssystemet Cosmic.

Rörligheten bland IT-användare är stor och önskan om tillgång till IT-tjänster från allmänhet och olika yrkesgrupper ökar. Den snabba utvecklingen av tekniken innebär att det kommer nya risker som måste beaktas genom ökat användande av mobiltelefoner, läsplattor, appar, sociala medier m.m. Brister i IT-säkerheten medför även risker att verksamheten och dess kunder och intressenter kan påverkas mycket negativt.

Mot bakgrund av ovanstående har regionens revisorer utifrån sin risk-och väsentlighetsbedömning beslutat sig för att genomföra en granskning av IT-säkerhet inom ramen för revisionsplanen för år 2018.

Syfte

Syftet med granskningen är att klargöra vilka eventuella områden som Region Halland behöver utveckla för att uppnå en balanserad IT-säkerhet.

Övergripande revisionsfrågor

Rapporten avser att belysa följande övergripande revisionsfrågor:

1. Finns en tillfredställande intern styrning och kontroll för en effektiv och säker hantering av IT?
2. Har regionstyrelsen säkerställt att nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

För att besvara de övergripande revisionsfrågorna, har 10 kontrollmål definierats, se nästa sida.

Kontrollmål

Kontrollmål

1. Finns aktuella och ändamålsenliga styrande dokument samt riktlinjer som är tillräckligt införda, implementerade och kända av organisationen?
2. Sker uppföljning kring efterlevnad av de styrande dokumenten?
3. Är IT-driften och användningen av IT tillräckligt fri från störningar och incidenter för att anses vara ändamålsenlig?
4. Finns det mekanismer för identifiering av säkerhetsrelaterade hot mot IT-miljön?
5. Har regionen infört tillfredställande skyddsåtgärder mot interna och externa hot?
6. Har regionen skapat rätt förutsättningar i form av processer och kunskap i organisationen för att upptäcka säkerhetsincidenter?
7. Finns adekvat förmåga att hantera säkerhetsincidenter som har inträffat?
8. Har regionen en godtagbar förmåga att återställa IT-stödet efter en incident?
9. Hur är IT-säkerheten avseende intrång av aktör innanför det fysiska skyddet?
10. Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?

Metod och fokus

Granskningen har genomförts enligt ITM-metoden. ITM-metoden bygger på fem områden som tillsammans representerar och sammanfattar IT-verksamheten inom en organisation. Metoden tar även hänsyn till så kallad "good practice" inom IT generellt och jämför erhållet resultat med hur IT hanteras hos andra organisationer.

Resultatet bygger på intervjuer med identifierade nyckelpersoner i regionen, (se intervjulista, bilaga 1) samt inläsning och genomgång av tillgänglig dokumentation och styrande dokument.

Grad av fokus

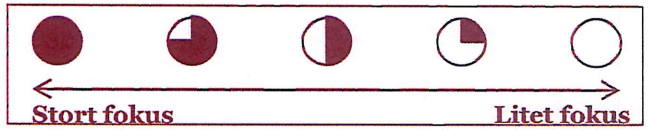
Informationssäkerhet
- Finns det en tydlig målbild och ansvarsfördelning för arbetet med informationssäkerhet? Hur arbetar man med att klassificera och kategorisera data samt känslig information? Är kravställningen mot IT-drift och IT-säkerhet tydlig?

Teknisk säkerhet
- Hur arbetar organisationen med att utveckla och hålla sig á jour med den tekniska säkerheten? Hur säkerställer man säkerheten hos interna och externa system? Sker det löpande uppdatering av tekniska komponenter? Sårbarhetsscannas systemen regelbundet? Finns det system som kan detektera intrång?

Drift
- Hur ser den dagliga driften ut? Hur ser processer, rutiner, dokumentation samt loggföring ut för driftorganisationen?
- Är driftorganisationen ordentligt rustad för att klara ett systemhaveri?

Organisation och Personal
- Hur ser rollfördelningen ut inom organisationen? Finns det en tydlig ansvarsfördelning? Är bemanningen i driftorganisationen samt service-desk tillräcklig och har de rätt kompetens? Är organisationen strukturerad och uppbyggd för att inte hamna i beroende till nyckelpersoner?

Utveckling och framtid
- Hur arbetar organisationen med förändringsarbete, utveckling och målsättningar? Finns det planer och strategier för att leda organisationen framåt? Finns tydliga mål och visioner från ledningen uppsatta och dokumenterade?



Revisionell bedömning

Övergripande revisionsfrågor

1. ***Finns en tillfredställande intern styrning och kontroll för en effektiv och säker hantering av IT?***
2. ***Har regionstyrelsen säkerställt att nuvarande tekniska IT- säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?***

Bedömning

Vår övergripande bedömning är att regionen till viss del uppfyller innebörden i revisionsfråga 1 [redacted]

[redacted]

Fråga 1: Den interna styrningen och kontrollen som finns i Region Halland är till viss del tillfredställande för att skapa en effektiv och säker hantering av IT. Det finns en tydlig roll och ansvarsfördelning gällande IT-säkerhet samt en medvetenhet inom regionen av vikten av säker hantering av IT. Avsaknad av intern kontroll och tydlig kravställning mot IT gällande klassning och informationssäkerhet innebär att det inte finns tydliga krav från verksamheten om vilken nivå av IT-säkerhet som bör uppnås. Detta försvårar besvarandet av frågan eftersom det saknas en beskrivning av vilka behov som finns.

Vid penetrationstester uppmärksammades allvarliga brister gällande hantering av IT vilket innebär en stor säkerhetsrisk för regionens IT. Det som bland annat kan nämnas är avsaknad av process för hantering av inaktiva konton, svårigheter att genomföra tester av IT-miljön samt hantering av dokumentation vilka samtliga har påverkan på hur effektiv och säker hanteringen av IT är.

Regionstyrelsen har inte säkerställt att nuvarande tekniska IT-säkerhet är tillräcklig och tillfredställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Genomförda penetrationstester visade på att när en obehörig får tillgång till det interna nätet är det lätt att ta sig mellan system utan att bli upptäckt. Detta beror dels på bristfällig segmentering av nätet, dels på att verktyg som skulle kunna detektera denna typ av intrång inte finns.

[redacted]

Detaljerad analys

Observationer och rekommendationer

Kontrollmål 1 -

Finns aktuella och ändamålsenliga styrande dokument samt riktlinjer som är tillräckligt införda, implementerade och kända av organisationen?

Observationer

- Region Halland har policys både gällande IT och säkerhet framtagna. För säkerhetspolicyn finns även riktlinjer framtagna för att finnas som stöd för implementering av policyn i verksamheten.
- Vid intervjuer med verksamheten framkommer det att verksamheten inte känner till att IT-organisationen har checklistor som skall användas bl.a. vid upphandling och implementering av nya system (IT-tekniskförväntan på leverantörens lösning). Detta tyder på att det finns brister i kommunikationen mellan IT-organisationen och verksamheten.
- Sedan förändringen av intranätet för ett par år sedan har IT och verksamheten haft en utmaning med tillgång till dokument då de inte har åtkomst till varandras lagringsplatser. I intervjuer med IT framkom att detta lett till att samma dokument måste lagras och uppdateras på flera ställen för att samtliga som har behov av dokumentet skall ha åtkomst till det. Ett exempel på detta är riktlinjer gällande säkerhet för MT och IT.
- Riktlinjer gällande säkerhet ligger inte bara sparade på olika ställen, vid intervjuer har framkommit att de dessutom inte alltid är samstämmiga vilket kan innebära problem och samarbetssvårigheter mellan avdelningarna.
- Det finns en upplevd otydlighet kring processer och strukturer för dokumentation och ansvaret ligger hos individen att se till att hålla dokument uppdaterade.
- Vid intervjuer framkom att det finns ett antal riktlinjer för olika områden, dock kan det vara svårt att veta vilken som är den senast uppdaterade. Ett exempel som framkom i samband med detta var riktlinjer för kommunikation mellan IT och verksamheten.

Bedömning

- Region Halland har styrande dokument kring IT och säkerhet, bland annat policys och riktlinjer för dessa områden. Det finns dock utrymme för att förtydliga dessa samt bryta ner dem ytterligare för att underlätta för verksamheterna att använda sig av dem.
- De dokument som finns används sporadiskt av verksamheten och det finns ett stort personberoende gällande vilka riktlinjer och dokument som följs. Genomgång av riktlinjers riktighet och tydlighet kan med fördel genomföras för att öka tydligheten för organisationen vad de skall förhålla sig till.

Kontrollmål 2 -
Sker uppföljning kring efterlevnad av de styrande dokumenten?

Observationer

- Revision av dokumentation på verksamhetsnivå sker, men i olika utsträckning och inte alltid enligt de riktlinjer som finns. Tidsbrist anges vara en stor anledning till bristande dokumentation eller till att revidering av befintliga dokument släpar efter.
- Systemdokument skall uppdateras löpande vid förändringar, detta är med som en del av "change-processen". Dock framkommer vid intervjuer att det inte finns någon kontroll att detta görs.
- För systemdokumentation blir kvalitén ofta i förhållande till storleken på systemet. Dokumentation av mindre system prioriteras ner och kvalitén blir därefter.
- IT-organisationen använder Sharepoint som dokumenthanteringssystem och där finns en inbyggd versionshantering, Dock har den begränsningar och det är svårt att se annat än när den senast ändrades. Det saknas mer information som ger en bättre bild av status på dokumentet, är dokumentet dessutom utskrivet i pappersform saknas all spårbarhet.
- Då checklistor från IT till verksamheterna är bristande minskar följsamheten från verksamheterna vilket innebär konsekvenser för IT vid upphandling, implementering och uppdatering av system.

Bedömning

- Bristande uppföljning av dokument och riktlinjer beror till största delen på resursbrist/tidsbrist. Det bör säkerställas att verksamheterna (inkl. IT) har tillräckliga resurser för att följa upp och revidera den dokumentation som krävs för att bibehålla en säker informations- och IT-hantering inom organisationen. Idag kan verksamheten inte vara säker på att den dokumentation som finns är riktig, vilket dels skapar merarbete, dels ökar risken för fel.
- Kontrollfunktion (LIS) finns för att kontrollera efterlevnaden av dokumentationen men det finns brister i processen. Detta gör att det i dag finns en del brister i efterlevandet av dokumentationen.

Kontrollmål 3 -
Är IT-driften och användningen av IT tillräckligt fri från störningar och incidenter för att anses vara ändamålsenlig?

Observationer

- Relativt få störningar har uppmärksammats enligt intervjuerna med IT-avdelningen och vissa verksamheter.
- De störningar som uppmärksammas av verksamheten beror till viss del på dålig kommunikation mellan IT och verksamheterna. Exempelvis att utrustning installerats utan att kommunicera med IT, vilket innebär att de utan förvarning har stängt av tillgång till nätet för utrustningen då de uppmärksammat för dem okända system eller utrustning.
- Att kommunikationen mellan IT och verksamheterna upplevs bristfällig i vissa delar, bland annat att verksamheten inte har dokumenterat konkreta behov och krav. Detta har även uppmärksammats i projekt Stabilt IT Region Halland.*

Bedömning:

- IT är ändamålsenligt ur aspekten att det är få störningar och incidenter. Översyn kring processen för implementering av ny utrustning för att säkerställa god kommunikation mellan IT-avdelningen och verksamheterna kan förbättra detta ytterligare.

*Se projektrapport Stabilt IT Region Halland, version 1, 20180626

Kontrollmål 4 -
Finns det mekanismer för identifiering av säkerhetsrelaterade hot mot IT-miljön?

Observationer

- [redacted]
- Vid PwC:s PEN-tester uppmärksammades ett flertal starka säkerhetsmekanismer och skydd, samt ett påtagligt säkerhetstänk som tycktes genomsyra många delar.
- Skalskyddet innehåller flera säkerhetslösningar för att försvåra ett otillåtet intrång.
- Insamling av loggar sker.
- Region Halland har satt ut ett flertal larm som har för avsikt att varna om någon obehörig försöker ta sig in i IT-miljön, till exempel upptäcktes det när PwC försökte lägga till domänadministratörsrättigheter för en testanvändare.
- [redacted]
- Utvalda personer på IT-avdelningen genomför omvärldsbevakning i syfte att vara à jour med vad som händer inom området.
- Inte alla tjänsteansvarigas rollbeskrivningar innehåller krav på att hen skall genomföra relevant omvärldsbevakning för att kunna fånga upp hot inom sitt område.

Bedömning

- [redacted]
- Omvärldsbevakning sker idag inte av alla som borde genomföra detta. Det sker mer sporadiskt och utifrån personligt intresse vilket kan innebära att viktiga områden missas. Ett mer strukturerat genomförande samt kontinuerlig informationsdelning internt ökar markant värdet av omvärldsbevakningen.
- [redacted]

Kontrollmål 5 -
Har regionen infört tillfredställande skyddsåtgärder mot interna och externa hot?

Observationer

- [redacted]
- [redacted]
- Alla SQL 2008-databaser når ”end of life” under 2019, idag finns ingen plan för hur uppgradering till nyare version av dessa skall genomföras.
- Det saknas en plan för hur man skall uppdatera regionens stora bestånd av Windows Server 2008-maskiner innan dessa når ”end of life”.
- [redacted]
- [redacted]
- [redacted]
- Ett flertal gamla, inaktiva, domänadministratörskonton ligger kvar. De är inaktiverade men har fortfarande kvar domänadministratörsrättigheter.
- [redacted]
- Det pågår ett arbete med att få igång en intern sårbarhetsscanning och detta arbete planeras att genomföras i egen regi.
- [redacted]

Kontrollmål 5 -
Har regionen infört tillfredställande skyddsåtgärder mot interna och externa hot?

Bedömning

- Region Halland har inte infört tillfredsställande skyddsåtgärder mot interna och externa hot.
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Arbetet med intern sårbarhetsscanning behöver intensifieras för att få kontroll över de sårbarheter som finns i Region Hallands system.
- [redacted]
- [redacted]

*Se exempelvis IIS rapport "Lösenord för alla – Statistik, råd och rekommendationer för bättre säkerhet"

Kontrollmål 6 -

Har regionen skapat rätt förutsättningar i form av processer och kunskap i organisationen för att upptäcka säkerhetsincidenter?

Observationer

- Region Halland har tydliga processer och riktlinjer för ärendehantering. Dock finns tydliga brister i ett antal andra processer, bland annat för genomgång och borttagning av inaktiva konton samt för genomgång av de insamlade loggarna.
- [redacted]
- [redacted]
- Informationssäkerhetssamordnarna är ansvariga för att ta fram relevanta utbildningar inom IT-säkerhet. HR är ansvariga för den övergripande kompetensutvecklingen inom organisationen. Vid intervjuer framkom att samtlig personal inom IT-avdelningen inte hinner med att utbilda sig eller hålla sig uppdaterade på ett önskvärt sätt, vilket innebär kompetenstapp då IT är ett område som snabbt förändras.
- Samtliga incidenter skall hanteras av Incident Manger. Kvällar och helger finns beredskap med rullande schema fördelat på [redacted] samband med incidenter skall ITIL-processen följas. En påtalad brist är att verksamheten inte alltid vet vem de bör kontakta vilket kan skapa problem för att de ringer ”fel” sorts tekniker.
- Verksamheterna har ett intresse av att få en större förståelse för IT, IT-säkerhet och informationssäkerhet. IT-säkerhetsansvarig får många förfrågningar om att presentera IT-säkerhetsfrågan vid verksamhetsmöten och liknande.
- I syfte att utbilda och uppmärksamma verksamheten på hur en phishingattack kan gå till planeras ett genomförande av en sådan från IT-avdelningen.

Kontrollmål 6 -

Har regionen skapat rätt förutsättningar i form av processer och kunskap i organisationen för att upptäcka säkerhetsincidenter?

Bedömning

- [redacted]
- I samband med implementering av framtida detekteringssystem samt system för logghantering bör det skapas processer och rutiner för hur säkerhetsincidenter skall upptäckas och hanteras.
- För att behålla en adekvat kunskapsnivå hos personalen måste ledningen säkerställa att de som arbetar med IT- och informations-säkerhetsfrågor har förutsättningar att vidareutbilda sig.
- Ledningen bör säkerställa att samtliga medarbetare inom Region Halland har en baskunskap gällande IT- och informationssäkerhet. Gällande det senare finns planer för hur detta kan genomföras vilket är positivt.
- Genomgång av befintliga processer samt analys av processer som saknas bör genomföras. Bland annat finns behov av en process för genomgång av inaktiva konton.

Kontrollmål 7 -
Finns adekvat förmåga att hantera säkerhetsincidenter som har inträffat?

Observationer

- De incidenter som har inträffat i Region Halland har hanterats bra enligt tillfrågade personer.
- IT-avdelningen upplever begränsade möjligheter att testa incidenter och/eller återläsning. Vid intervjuer framkom att det finns ett motstånd inom verksamheten vilket gör det svårt att få tillfällen att genomföra tester.
- Det finns en jourberedskap, se kontrollmål 6.

Bedömning

- IT-avdelningen har en adekvat förmåga att hantera de säkerhetsincidenter och haverier som inträffat. IT-avdelningen har i de incidenter som skett agerat i enlighet med framtagna processer. Incidenterna har registreras och Incident Manager tagit ansvar för incidenten.
- Fler tester ger möjlighet att säkerställa förmågan att kunna hantera de incidenter som sker. Det upplevda motståndet som finns idag kan förklaras av okunskap inom verksamheterna, dels vad det innebär rent praktiskt dels vad konsekvenserna kan bli av uteblivna möjligheter till att testa.

Kontrollmål 8 -
Har regionen en godtagbar förmåga att återställa IT-stödet efter en incident?

Observationer

- [redacted]
- Regionen har inte tagit fram en övergripande prioriteringslista för samtliga verksamheter gällande upptagning av servrar och system i samband med incidenter.
- Idag finns dokumentationen om hur system skall startas upp och i vilken ordning endast online och/eller i systemet.

Bedömning

- Den tekniska förmågan att återställa IT-stödet efter en incident finns bland personalen på IT-avdelningen. Men avsaknad av tydliga rutiner och prioriteringar kan dock leda till att återställning tar onödig lång tid eller görs i fel ordning vilket skapar lång nertid för kritiska system.
- Möjlighet att genomföra tester är en förutsättning för att undvika konsekvenserna av att servrar går ner oförutsett [redacted]
- Brister i den ej kompletta övergripande klassning av information och system gör att IT-avdelningen inte har någon prioriteringsordning att utgå ifrån vid incident. Detta kan få stora konsekvenser för verksamheterna som riskerar att behöva vänta onödigt länge på tillgång till kritiska system.
- I händelse av serverhaveri måste nödvändig dokumentation finnas tillgänglig off-line samt off-site beroende på hur lösningen ser ut för att säkerställa att dokumentationen alltid finns nåbar.

Kontrollmål 9 -
Hur är IT-säkerheten avseende intrång av aktör innanför det fysiska skyddet?

Observationer

- [redacted]
- Tele2 som är operatör har ansvar för stora delar av nätverket, både det trådade och det trådlösa samt linor till och från regionen. Tele2 är även drivande i frågor kring hur nätet bör segmenteras. Upphandling av nätleverantör pågår och innan det är på plats kommer inget internt arbete med segmentering av nätet påbörjas.
- IT-säkerhetsgrupperingen har nyligen nyanställt och består idag av två heltidstjänster samt två på 50% av heltid.
- Idag finns ingen formell gruppering med kompetenser från fler avdelningar som driver IT-säkerhetsfrågor inom regionen. Tjänsteansvarig för IT-säkerhet håller ihop en informell gruppering som arbetar med dessa frågor.
- [redacted]
- I dag finns det 5 aktiva domänadministratörskonton [redacted]

Bedömning

- [redacted]
- Avsaknad av en nätverksarkitekt som tillsammans med IT-säkerhetsavdelningen kan ta fram design [redacted] Detta är en roll som bör skapas och tillsättas snarast.
- Ansvar för och kompetens om nätverk och segmentering bör finnas internt i större utsträckning än vad det finns idag.
- En gruppering för IT-säkerhetsfrågor bör formaliseras för att säkerställa att samtliga delar inom IT inkluderas samt ge grupperingen en större tyngd internt.
- [redacted]
- Resultatet av nyanställningen inom IT-säkerhetsgruppen går ännu inte att utvärdera då de nyanställda precis påbörjat sin anställning.
- 5 aktiva domänadminstratörskonton kan anses vara en rimlig mängd konton med dessa rättigheter. [redacted]

Kontrollmål 10 -
Finns det en tydlig roll- och ansvarsfördelning i frågor kring den övergripande IT-säkerheten?

Observationer

- IT-direktören är ytterst ansvarig för IT-säkerheten i Region Halland. Ansvaret är delegerat till IT- och tele-chefen som delegerat det till IT-driftansvarig. Operativt ansvarig är tjänsteansvarig för IT-säkerhet tillsammans med sin grupp.
- Vid intervjuer framkom ett stort personberoende inom regionen vilket påverkar möjligheten för personal att ta ledigt.
- På IT-avdelningen hålls forumet Techtalk månatligen, där möjlighet finns att lyfta IT-relaterade frågor. Där lyfts även frågor som rör IT-säkerhet, men det finns inget eget formellt forum för IT-säkerhet.
- E-rådet är det beredande organet i frågor rörande IT- och informationssäkerhet medan beslutmandat ligger hos IT-direktören i informationssäkerhetsfrågor som gäller IT.
- Inom regionstyrelsen planeras för en ny organisation, IT-styrning och samordning, som kommer verka direkt under IT-direktören. Denna organisation kommer bestå av bland annat chefsarkitekt och IT-strateg. Detta kommer troligtvis bli bra om det finns tydliga rollbeskrivningar och gränsdragningar.

Bedömning

- Tydligt att IT-direktören är ytterst ansvarig för IT-säkerhet. Mycket ansvar är delegerat. Rollbeskrivningar ibland otydligt/generellt skrivna med en del tolkningsmån. Vid uppstart av ny organisation bör fokus läggas på tydliga roller och gränsdragning mot övriga verksamheter för att skapa förutsättningar för den nya enheten att vara ett komplement till befintlig organisation.
- Avsaknad av tydlig beställare/kravställning gällande informationssäkerhet leder till att frågan faller mellan stolarna. Varken IT-drift, IT-säkerhet eller verksamheterna har regler att förhålla sig till gällande vilken nivå på säkerhet, tillgänglighet eller upptid som olika system bör hålla. Brist på kravställare samt kontrollområden för hur IT skall skydda information och system.
- ISSO-gruppen bör ges en tydligare roll, genomlysning av hur denna grupp kan skapa maximal nytta i organisationen bör genomföras.

Övrigt

- IT-avdelningen uppger att de har svårt att få till servicefönster mot verksamheten, en tydligare process för detta har tagits fram men inte riktigt satt sig än. Detta kan med fördel utvärderas kontinuerligt tills processen kan anses väl implementerad hos både IT och verksamheten.
- Inom regionen finns ett behov av bättre sammanhållning inom IT och teknikplattformar. Den nya organisationen – IT-styrning och samordning – kan med fördel ha fokus på strategi, målstyrning och verksamhetsplanering för att skapa förutsättningar för bättre samanhållning. För att uppnå detta bör gruppen innehålla bland annat IT-säkerhetsansvarig, övergripande arkitekt och informationsansvarig.
- För att IT-säkerhet och IT-drift skall fungera på ett tillfredställande och säkert vis behöver dessa grupper någon som kravställer utifrån:
  - **Tillgänglighet** – IT-miljön skall vara tillgänglig för behöriga på den plats, vid den tidpunkt och på det sätt informationen behövs.
  - **Riktighet** – Korrekt information med rätt kvalité genom hela dess livscykel.
  - **Konfidentialitet** – Åtkomstbegränsning för obehöriga som inte har rätt att ta del av informationen.
  - **Spårbarhet** – Vid behov möjlighet att se vem som har gjort vad med informationen, när det skedde och hur de hade tillgång.
- En informationssäkerhetsansvarig i regionen har möjlighet att ställa krav på verksamheten att klassa sina system och information efter ovan nämnda områden. Detta synkroniseras till en matris över vilka system som behöver en viss skyddsnivå eller vilka system som behöver tas upp igen efter ett större haveri. Matrisen blir en karta för IT-avdelningen att hålla sig till vid haveri, eller vid uppsättning av system, segment m.m. Utan klassning och matris blir det godtyckligt vilken nivå av säkerhet eller återställning som behövs hållas på regionens system.
- En tydlig bild av vad som skall uppnås med säkerhetssystemen gällande redundans, kraft, infrastruktur m.m. underlättar äskande av medel i budgetförhandlingar. Det ger också möjlighet att sätta mål och genomföra systematisk uppföljning av målen.
- Projektet ”Uppföljning stabilitet Region Hallands IT-miljö” visar på brister i kommunikationen mellan IT och verksamheten. Bland annat finns ingen konkret dokumentation kring krav och behov samt kvalité och leverans, vilket påverkar på IT- och informationssäkerheten i regionen.
- Det pågår en implementation av en DLP-lösning i regionen, ett arbete som initierats och drivits av IT-säkerhetsgrupperingen och involverat både ISSO och E-rådet. Vid intervjuer har framkommit att ägandet av DLP fortfarande inte är klarlagt vilket är olyckligt. En DLP-lösning bör driftas av IT men ägas av en beställare av informationssäkerhet så som informationssäkerhetsansvarig eller i Region Halland ISSO-gruppen.
- IT-avdelningen är ISO 27000-certifierad. Under granskningen har framkommit synpunkter på behovet av att övriga delar av regionen certifierar sig. Det bör därmed påpekas att det är eftersträvansvärt att ha ett strukturerat arbete med informationssäkerhet oavsett certifiering eller ej. En stark rekommendation som ett första steg mot att arbeta strukturerat med informationssäkerhet är att tillsätta en informationssäkerhetsansvarig med övergripande ansvar i hela regionen.

Penetrationstest

PwC har som en del av denna granskning genomfört ett penetrationstest. Detta test utfördes av PwC Offensive Securitys säkerhetsexperter med avsikten att hitta kritiska sårbarheter i Region Hallands IT-miljö.

Det huvudsakliga målet med testet var att utvärdera IT-säkerheten hos Region Halland, att hitta sårbarheter med hög riskfaktor samt att föreslå åtgärder som Region Halland kan vidta för att öka säkerheten i organisationen. PwC:s konsulter utgår från det administrativa nätverket som har tillgång till samtliga/en stor del av systemen i Region Hallands IT-miljö, ett nätverk som vanligtvis endast är tillgängligt för IT-personal och annan administrativ personal.

Under arbetet utsattes Region Hallands IT-miljö för angrepp och tester vilka utformats på så vis att de i möjligaste mån efterliknar de reella hot som organisationen kan utsättas för. Detta innebär att PwC Offensive Securitys säkerhetsexperter har försökt angripa systemet genom manuellt testande, så kallad ”black-box testing”, utefter en väl beprövad metodik mot en delmängd av Region Hallands IT-system.

PwC:s team utforskade under testperioden en omfattande IT-struktur med ett flertal starka säkerhetsmekanismer och skydd, samt ett påtagligt säkerhetstänk som tycktes genomsyra många delar. PwC:s bedömning är att Region Hallands IT-miljö består av ett stort antal system och webbapplikationer vilka tillhandahåller kritiska resurser för dess personal och invånare. IT-miljön innehar känslig data, såsom personuppgifter och journaler.

Avslutning

2018-08-17

Uppdragsledare

Projektledare

Bilaga 1

Intervjulista

Namn	Roll	Verksamhet
Danijela Huskic	Tjänsteansvarig Nätverk	IT/Tele-Service
Thomas Persson	Tjänsteansvarig Server	IT/Tele-Service
Henrik Ljungberg	Tjänsteprotföljsanvarig	IT/Tele-Service
Måns Anrup	IT-direktör	Regionkontoret Stab
Fredrik Gustavsson	AC Server & kommuniktation samt IT-säkerhetsansvarig	IT/Tele-Service
Lasse Sjöberg	Tjänsteansvarig IT-säkerhet	IT/Tele-Service
Christina Nilsson	Objektledare systemförvaltning fam. Vårdsystem	Hälso- och sjukvården
Marie Rosengren	Objektledare systemförvaltning fam. Vårdsystem	Hälso- och sjukvården
Hendrik Pedersen	Informationssäkerhetsstrateg	IT/Tele-Service

Bilaga 2

Ordlista 1/2

Ord	Beskrivning
SQL	SQL är namnet på Microsofts databashanterare.
Databas	Databas är en lagringsplats för information som används av ett eller flera program/system.
DLP	DLP, Data Loss Prevention, är en typ av verktyg som försöker förhindra att en organisations interna information kommer i orätta händer. Det sker genom att verktyget försöker känna igen olika typer av information där den finns sparad, när den skickas eller när den används i ett program. DLP-verktyg kan arbeta passivt och bara övervaka användningen av information, eller aktivt och kontrollera hur information används.
IT	IT står för informationsteknik. Oftast pratar man om tekniken – alla datorer, maskiner, nätverk och programvaror som används för att skapa ett företags IT-lösning. Men egentligen är det i:et, alltså informationen, som är det viktiga. De flesta företag är i dag helt beroende av att skapa och använda information.
Patcha	Patcha, är att uppdatera till senaste versionen av programmet/mjukvaran. Kan vara för att införa förbättringar eller att stänga säkerhetshot.
Switch	Nätverkskomponent som styr datatrafik mellan olika noder och system i ett nätverk.
802.1X	IEEE 802.1X är en standard för portbaserad nätverksåtkomstkontroll. Det tillhandahåller en autentiseringsmekanism för enheter som vill och är betrodda att ansluta till ett LAN eller WLAN.
UPS	UPS, Uninterruptible Power Supply, är en elektrisk apparat som tillhandahåller en hög kvalité på lik- eller växelspänning till elförbrukare, även då ett strömavbrott eller andra störningar uppstår. Apparaten installeras mellan den ingående kraftmatningen ("vägguttaget") och elförbrukaren (exempelvis en dator).
End of life	End of life innebär att det inte kommer några nya sårbarhetsuppdateringar efter det datum som anges som sistadatum.

Bilaga

Ordlista 2/2

Ord	Beskrivning
Fysiskt skydd	Tillgång till lokaler, nätverksuttag och dyl.
Nätverkssegmentering	Nätverkssegmentering innebär uppdelning av regionens nätverk för att höja säkerheten. System inom olika segment kan då endast kommunicera genom kontrollerade kanaler medan system inom samma segment fortfarande kan kommunicera fritt med varandra. För att ytterligare höja säkerheten kan brandväggar upprättas mellan olika segment. Syftet med segmentering är att minimera onödiga kontaktytor mellan system som inte behöver kommunicera. Systemen kan grupperas på olika sätt vid segmentering, exempelvis utifrån verksamhet eller utifrån skyddsnivå.
Nätverksarkitet	Ansvarig för utformningen av regionens infrastruktur, nätverk, systemlösningar och IT-säkerhetslösningar mm.
Windows Server 2003	Windows Server 2003 är ett serveroperativsystem från mjukvarutillverkaren Microsoft. Det släpptes på marknaden 24 april 2003. Microsoft har därefter släppt ett antal nyare versioner av sitt serveroperativsystem t.ex. server 2008, 2008 R2, 2012, 2012 R2 och 2016.
Brandvägg	En brandvägg ansluts mellan två eller flera nätverk, vanligen mellan Internet (WAN) och ett privat nätverk (ett eller flera LAN). En brandvägg analyserar inkommande och utgående trafik och blockerar obehöriga IP-paket. För att avgöra vilken trafik som är behörig eller ej arbetar den efter regler, bestämda av brandväggens programvara och av dess systemadministratör.