Tyresö kommun
Konsult- och servicekontoret
Urban Petrén

Diarienummer
2015/KS 0323 016

Kommunstyrelsen

Svar på revisionsrapport om IT-säkerhet i form av internt intrångstest

Förslag till beslut

- Konsult- och servicekontorets skrivelse antas som svar på revisionsrapporten IT-säkerhet i form av internt intrångstest.

Ann-Catrine Hagner
Chef konsult- och servicekontoret

Urban Petrén
IT-chef

Beskrivning av ärendet

PWC genomförde i april 2015 ett internt intrångstest på uppdrag av kommunens revisorer. I den rapport som presenterats efter intrångstestet finns ett antal identifierade risker i kommunens IT-miljö. I uppdraget att genomföra intrångstestet ingick inte att vidare analysera de identifierade riskerna, dess möjliga konskevens eller sannolikhet att inträffa för kommunens specifika IT-miljö. Med anledning av de listade riskerna ser revisorerna att det finns en risk att arbetet med kommunens informationssäkerhet innehåller brister gällande rutiner kring säkerhetskonfigurering, behörighetskontroll och övervakning.

I skrivelsen till kommunstyrelsen finns ett antal rekommendationer kring arbetet med informationssäkerheten:

- genomföra en risk- och åtgärdsanalys av de identifierade riskerna
- genomföra ett externt penetrationstest

Svar på revisorernas skrivelse har tagits fram i samråd med Säkerhetsenheten.

Nuvarande arbete med informationssäkerhet

IT-avdelningen har successivt arbetat för att höja kvaliteten på arbetet med informationssäkerheten. I IT-avdelningens verksamhetsplan för 2014 anges att intrångstest ska genomföras för kommunens IT-miljö. Dessa tester, internt och externt intrångstest, genomfördes i slutet av 2014. De i testerna identifierade riskerna är analyserade och åtgärdsplan med prioritering kring riskerna finns för det fortsatta informationssäkerhetsarbetet.

Under 2014 infördes rutiner för att öka det proaktiva arbetet kring att förebygga risker. Bland annat finns automatiska system som övervakar och identifierar möjliga risker. Alla rapporterade risker analyseras inför kommande releasefönster (1 gång/kvartal) och beslut fattas om vilka av riskerna som ska åtgärdas. Risker som inte hanteras inom IT-avdelningens ansvarsområde vidareförmedlas till berörd systemförvaltare.

Rekommendation: Risk- och åtgärdsanalys

IT-avdelningen inom konsult- och servicekontoret har tagit del av PWC:s rapport och analyserat samtliga risker som anges i rapporten.

Kommentar från konsult- och servicekontoret:
De identifierade riskerna var sedan tidigare, med några få undantag, kända risker och därmed även hanterade i tidigare risk- och åtgärdsanalyser. En förnyad risk- och åtgärdsanalys har genomförts utifrån de risker som identifierats och även de nya riskerna har riskvärderats och åtgärdsanalyserats. Analysen är utifrån ett helhetperspektiv där hänsyn tas till såväl konsekvens som sannolikhet kring respektive risk. Detta har resulterat i en risk- och sårbarhetsanalys med åtgärdsanalys för de identifierade riskerna.

Rapporten från PWC innehåller en mängd listade risker. Utifrån en gruppering på risktyp och påverkade system blir det 29 grupperingar av risker. Av dessa är det 6 risker som bedöms som möjliga att inträffa och samtidigt har en måttlig konskevens. Övriga risker bedöms ha en lägre sannolikhet att inträffa alternativt en lägre konsekvens. 6 st av 29 grupperingar berör inte produktionssystem utan berör fristående lab- eller testmiljöer som inte har koppling till produktionsmiljön. Några av riskerna gäller system där Tyresö kommun köper IT-funktionen som tjänst. Där har leverantören ett helhetsansvar gällande tillgänglighet och säkerhet.

Av de i rapporten identifierade riskerna var 2 risker okända för IT-avdelningen.

En summerad bedömning utifrån ovanstående är att de redan införda rutinerna ger en i praktiken god informationssäkerhet samt en god kännedom av de risker som finns i kommunens IT-miljö.

Arbete och rutiner kring informationssäkerhet behöver kontinuerligt utvecklas och förbättras. Arbetet med den operativa informationssäkerheten har fokuserat på att få fram rutiner i det praktiska arbetet för att säkerställa informationssäkerheten i IT-miljön.

I det fortsatta arbetet med att förbättra informationssäkerheten ska åtgärdsutvärderingen inför varje releasefönster dokumenteras då det idag saknas fullgod dokumentation. Förbättrad kravställning vid upphandling av IT-tjänster ska utarbetas, där leverantörerna får ett tydligt krav på återkoppling kring åtgärder och riskbedömningar kring de levererade IT-tjänsterna.

Rekommendation: Externt intrångstest

Kommentar från konsult- och servicekontoret:
I verksamhetsplaneringen för 2014 ingick att genomföra intrångstester för kommunens IT-miljö. För att genomföra denna typ av tester anlitades ett fristående säkerhetskonsultföretag som under november och december 2014 genomförde intrångstester för såväl det interna som externa nätverket. Om inga

större förändringar genomförs av IT-miljön, bedöms förnyade intrångstest vara relevant att genomföra 2016/2017.

De genomförda testerna resulterade i ett antal identifierade risker som har analyserats och resulterat i en åtgärdsplan.

Intrångstester är ett av många bra verktyg för att upprätthålla en bra informationssäkerhet och även få en bild av hur kommunens arbete med informationssäkerhet fungerar i praktiken.

Intrångstester bör genomföras med jämna mellanrum. Utifrån hur den kontinuerliga informationssäkerheten övervakas av olika system, bedöms ett rimligt intervall för denna typ av tester i Tyresö kommuns IT-miljö vara 3 år.