UTDRAG

§ 133

Dnr 2015/KS 0323 016

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

Kommunledningsutskottets förslag till kommunstyrelsen

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

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 skrivelsen till kommunstyrelsen finns rekommendationer kring arbetet med informationssäkerheten om att genomföra en risk- och åtgärdsanalys av de identifierade riskerna samt att genomföra ett externt penetrationstest.

Ett förslag till svar på revisorernas skrivelse har tagits fram av IT-enheten på konsult- och servicekontoret i samråd med säkerhetsenheten.

Bilagor

Tjänsteskrivelse Svar på revisionsrapport om IT-säkerhet i form av internt intrångstest.pdf
IT-säkethet i form av internt intrångstest.pdf

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 Hägner
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 vidarefördelas 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.

TYRESÖ KOMMUN
Revisorerna

2015-05-28

Kommunstyrelsen

IT-säkerhet i form av internt intrångstest

De förtroendevalda revisorerna i Tyresö kommun har givit PwC i uppdrag att genomföra en granskning av ovanstående område.

Efter genomförd granskning är vår sammanfattande bedömning är att kommunen inte uppnår en tillräcklig IT-säkerhet för att minimera risker för obehörigt intrång av en intern aktör. Resultatet av det interna intrångstestet visar vilka potentiella effekter identifierade brister i processer kring IT-säkerhet medför. Genom bristande rutiner kring säkerhetskonfiguration, behörighetskontroll och övervakning når kommunens interna nätverk inte upp till en adekvat IT-säkerhetsnivå avseende skydd mot obehörigt intrång.

Vi rekommenderar kommunen att genomföra en riskanalys samt åtgärdsanalys baserat på de i denna rapport angivna iakttagelserna och rekommendationerna. Fokus bör vara att omgående åtgärda de mest kritiska riskerna för att sedan prioritera resterande iakttagelser.

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

Vi rekommenderar även kommunen att genomföra ett penetrationstest av sitt externa nätverk. Hotbilden som illustreras i dessa tester är en extern hacker som, utan kunskap om kommunens IT-miljö, kartlägger organisationens närvaro på Internet. Fokus är att bryta sig in i intressanta system exponerade på Internet, med det slutliga målet att försöka ta sig in i kommunens interna nätverk.

Revisorerna översänder rapporten och önskar skriftligt få del av styrelsens yttrande med anledning av granskningsresultatet senast 2015-11-16. Yttrandet tillställs revisorerna via Tyresö kommuns kanslifunktion inom kommunledningskontoret.

För Tyresö kommuns revisorer

Claes-Göran Enman
Ordförande

För kännedom
Kommunfullmäktiges presidium

Revisionsrapport

IT-säkerhet

Internt intrångstest

Tyresö kommun

Janne Swenson

Maj 2015

pwc

Innehållsförteckning

Inledning

Bakgrund

Kommunen 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 inom kommunen samt med andra intressenter. Detta ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Informationen måste skyddas mot obehörig åtkomst samtidigt som den ska finnas tillgänglig och dessutom vara tillförlitlig - *rätt information i rätt tid och för rätt personer.*

Enligt säkerhetsexperter inom IT-området är det idag fullt möjligt, och även vanligt, att göra intrång i olika organisationers nätverk. Dessa intrång kan i värsta fall medföra stor skada för såväl kommunen som enskilda individer.

Revisionsfråga

Granskningen syftar till att identifiera sårbarheter i kommunens interna nätverk genom tekniska tester.

För att uppnå granskningens syfte kommer följande kontrollmål att vara styrande för granskningen:

- *Är kommunens nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av intern aktör?*
- *Uppfyller kommunen kraven för vad som anses som god praxis gällande teknisk IT-säkerhet?*

Väsentlighets- och riskanalys

Om kommunen inte har ett väl fungerande säkerhetsarbete och ett strukturerat arbetssätt för att hantera IT-säkerheten finns risk för 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 kommunens trovärdighet ifrågasätts, såväl som till ekonomiska förluster och förlorat anseende.

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

Angreppssätt

Omfattning och mål

Syftet med testerna och granskningen var att utvärdera kommunens 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. I följande stycken beskrivs kort omfattning och utgångspunkt för uppdraget.

Det interna intrångstestet utgår från ett scenario som definieras nedan.

Scenario – Internt intrångstest
En person utan behörighet till kommunens system får fysisk tillgång till det interna nätverket. Personen kartlägger nätverket och attackerar viktiga interna system. Målet är att få tillgång till och kunna ändra information, alternativt att störa systemens tillgänglighet.

Metodik

PwC har en väl etablerad internationell metod för intrångstester, Security Penetration Testing Methodology. Metoden inför ett systematiskt angreppssätt för alla faser av uppdraget. Syftet med metoden är att minimera riskerna med intrångstester samt att uppnå en effektivitet i testarbetet.

Testerna genomfördes i fyra steg; generell informationsinsamling, sårbarhetsanalys, intrångsförsök, sammanställning och rapportering.

Ett flertal verktyg användes inledningsvis för att kartlägga resurserna på kommunens 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 det scenario som tidigare definierats. Under intrångssteget försökte vi erhålla behörighet eller på annat sätt kringgå säkerheten i de testade systemen. Samtliga tester utfördes från lokaler inom Tyresö kommun, varifrån målsystemen uppsöktes och attackerades.

Rapporten har sakgranskats av berörda tjänstemän.

Avgränsningar

Testerna har begränsats av följande faktorer:

- Tester har enbart genomförts mot relevant utrustning inom kommunens nätverk för att uppnå scenariots mål.
- Tester har, på grund av tidsbegränsningar, skett mot ett urval av de tjänster och system som varit tillgängliga. Det innebär sannolikt att det finns fler brister än de som identifierats och redogörs för i denna rapport.
- De tester som genomförts ger endast en ögonblicksbild av brister och säkerhetsnivån för det aktuella tillfället då testerna utfördes.
- För att undvika eventuella driftstörningar har tester inte genomförts där risken för att störa produktion bedömts som hög, exempelvis DoS attacker (tillgänglighetsattacker).

Resultat

Mot bakgrund av tekniska detaljer i rapporten har resultatet sammanfattats i en bilaga. PwC rekommenderar att bilagan sekretessbeläggs med stöd av sekretesslagen 2009:400 kapitel 18 paragraf 8.

Sammanfattande bedömning

Vår sammanfattande bedömning är att kommunen inte uppnår en tillräcklig IT-säkerhet för att minimera risker för obehörigt intrång av en intern aktör. Resultatet av det interna intrångstestet visar vilka potentiella effekter identifierade brister i processer kring IT-säkerhet medför. Genom bristande rutiner kring säkerhetskonfiguration, behörighetskontroll och övervakning når kommunens interna nätverk inte upp till en adekvat IT-säkerhetsnivå avseende skydd mot obehörigt intrång.

PwC rekommenderar kommunen att genomföra en riskanalys samt åtgärdsanalys baserat på de i denna rapport angivna iakttagelserna och rekommendationerna. Fokus bör vara att omgående åtgärda de mest kritiska riskerna för att sedan prioritera resterande iakttagelser.

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

PwC rekommenderar även kommunen att genomföra ett penetrationstest av sitt externa nätverk. Hotbilden som illustreras i dessa tester är en extern hacker som, utan kunskap om kommunens IT-miljö, kartlägger organisationens närvaro på Internet. Fokus är att bryta sig in i intressanta system exponerade på Internet, med det slutliga målet att försöka ta sig in i kommunens interna nätverk.

Datum	2015-09-24
Tid	09:00–10:35
Plats	Sammanträdesrummet Bollmora
Beslutande	Se närvarolista
Övriga deltagare	Se närvarolista
Justeringens plats och tid	Kommunkansliet 2015-09-28
Paragrafer	130 - 142

Sekreterare
Hillevi Elvhage

Ordförande
Fredrik Saweståhl

Justerande
Anita Mattsson

ANSLAG / BEVIS

Protokollet är justerat. Justeringen har tillkännagivits genom anslag.
Observera att anslagstiden inte är samma sak som överklagandetiden.

Organ	Kommunledningsutskottet
Sammanträdesdatum	2015-09-24
Datum då anslaget sätts upp	2015-09-29
Datum då anslaget tas ned	2015-10-21
Förvaringsplats för protokollet	Kommunkansliets arkiv plan 6

Underskrift
Hillevi Elvhage

	Utdragsbestyrkande

Närvarolista

Beslutande

Fredrik Saweståhl (M), ordförande
Mats Lindblom (FP), 1:e vice ordförande
Anita Mattsson (S), 2:e vice ordförande
Helen Dwyer (C), tjänstgörande ersättare för Ulrica Riis-Pedersen
Leif Kennerberg (KD)
Kristjan Vaigur (S)
Marie Åkesdotter (MP)

Ersättare

Andreas Jonsson (M)
Anna Steele (FP)
Anna Lund (KD)
Anders Linder (S)
Marcus Obligado (V)

Övriga

Bo Renman, kommundirektör, kommunledningskontoret
Sigbrith Martinsson, ekonomichef, kommunledningskontoret
Jonas Jansfors, tf HR-chef, kommunledningskontoret
Catarina Stavenberg, kvalitetschef, kommunledningskontoret
Karin Hassler, kommunikationschef, kommunledningskontoret, till och med § 136
Ann-Catrine Hagner, chef konsult- och servicekontoret, konsult- och servicekontoret, till och med § 133
Ulrika Josephson Westberg, chef kommunkansliet, kommunledningskontoret
Eva Nilsson, kommunjurist, kommunledningskontoret
Hillevi Elvhage, kommunsekreterare, kommunledningskontoret
Urban Petrén, IT-chef, konsult- och servicekontoret, till och med § 133

Frånvarande

Ulrica Riis-Pedersen (C)
Karin Ljung (S)