Revisionsrapport

IT-säkerhet

Externt och internt intrångstest

Tierps kommun

Älvkarleby kommun

Kerem Kocaer

Juni 2014

pwc

Innehållsförteckning

Inledning

Revisorerna i Tierps kommun och Älvkarleby kommun 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 kommunernas system. Granskningen har utförts under vår 2014.

Bakgrund

Kommunerna blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker. Kommunikationen med omvärlden ökar i omfattning och system blir mer integrerade såväl inom kommunerna som med andra intressenter. Detta ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Information måste skyddas mot obehörig åtkomst samtidigt som den skall finnas tillgänglig och dessutom vara tillförlitlig - *rätt information i rätt tid och för rätt personer*.

Sedan 2011-2012 finns det en gemensam IT-nämnd, ”IT-Centrum”, mellan Tierps kommun och Älvkarleby kommun. IT-Centrum har som uppdrag att ”förse användarna med verktyg för att hantera och förenkla vardagens processer.”

Om IT-Centrum 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 kommunernas trovärdighet ifrågasätts, såväl som till ekonomiska förluster och förlorat anseende.

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

Mot bakgrund av detta har kommunerna bedömt att en granskning av informations- och IT-säkerheten behöver genomföras.

Revisionsfråga

Granskningens syfte är att bedöma om IT-säkerheten, ur ett övergripande perspektiv, är tillräcklig.

Revisorerna önskar svar på följande revisionsfråga:

- **Är kommunernas 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:

- 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 kommunernas 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 två delar;

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

- **Internt intrångstest**
  I de interna testerna granskades kommunernas 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 kommunernas lokaler. Hotbilden är liknande om en persondator som drabbas av skadlig kod (exempelvis ett trojanprogram) ansluts till det interna nätverket.

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. Vidare ger testerna endast en ögonblicksbild av IT-säkerhetsnivån och är således ingen garanti för att nivån är densamma i framtiden.

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 kommunernas 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 Tierps kommun, varifrån målsystemen uppsöktes och attackerades.

Rapporten har sakgranskats av berörda tjänstemän.

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.