Revisionsrapport

IT-säkerhet

Internt intrångstest

Tyresö kommun

Janne Swenson

Maj 2015

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.