Öhrlings

PRICEWATERHOUSECOOPERS

Jönköpings Kommun

Security Penetration Test

Mars 2007

Innehållsförteckning

1 Sammanfattning

1.1 Inledning

Öhrlings PricewaterhouseCoopers (ÖPwC) har på uppdrag av kommunrevisionen genomfört intrångstester mot delar av Jönköping kommuns system. Syftet med testerna var att utvärdera organisationens externa och interna IT-säkerhet. Skyddet mot angrepp från externa och interna hot har utvärderats och målen har varit kommunens verksamhetskritiska system.

Testerna har genomförts i tre faser där den första fasen utfördes från ÖPwC:s laboratorium i Stockholm och den andra fasen utfördes från kommunens lokaler i Jönköping. Den tredje fasen bestod av intervjuer med driftspersonal hos Jönköpings kommun.

Uppdraget har genomförts under januari och februari 2007. Ordföranden i kommunrevisionen har varit ansvarig kontaktperson mot ÖPwC.

1.2 Sammanfattning

Under uppdraget har bland annat kommunens externa tjänster, som är nåbara från Internet, granskats. Målet med testerna har varit att påvisa brister i för kommunen intressanta system på Internet och att komma åt organisationens interna IT-resurser från Internet. Den externa analysen påvisar ett stort informationsläckage från interna resurser vilket strider mot god praxis, på grund av tidspress har ÖPwC dock inte försökt att utnyttja denna information för att nå interna system. De tillkortakommanden som påträffades under testerna visar på att kommunen har brister avseende sitt skydd mot intrång från Internet.

Under uppdragets senare fas satt ÖPwC:s konsulter i kommunens lokaler i Jönköping. Hotbilden som illustreras i det här scenariot är intern, det kan t ex vara en missnöjd anställd, en konsult som jobbar för kommunen eller någon extern person som får tillgång till en dator som är kopplad till kommunens nätverk. De mål som definierades innan testerna, dvs. obehörig tillgång till verksamhetskritiska system har delvis uppfyllts.

Testerna har bevisat att sekretess, integritet och tillgänglighet på interna system ej varit tillfredsställande. ÖPwC anser att kommunen har en säkerhetsnivå som inte motsvarar god praxis. Det finns många brister i miljön men de huvudsakliga problemen grundar sig på svaga lösenord, bristfälligt uppdaterade och konfigurerade system samt avsaknaden av klara rutiner för installationer och konfigurering av nya system.

De intervjuer som genomfördes visade på att kommunens personal har en god förståelse för informations- och IT-säkerhet. Vid årsskiftet 2005/2006 hade Jönköpings kommun 8-9 olika IT-driftsorganisationer. Efter en utredning beslutades att kommunen skulle bilda en IT-avdelning där man bla skulle samla all drift av IT och telefoni. Som ett resultat av denna utredning beslutades även att man inom kommunen skulle ta fram strategier, riktlinjer och regelverk för en mängd olika områden, bla informationssäkerhet.

Vid vår granskning noterade vi dock att kommunen inte än börjat att utforma strategier och regelverk för informationssäkerhet. För att uppnå en jämn säkerhet som stödjer verksamheten på ett optimalt sätt måste organisationens ledning visa engagemang i frågan. Genom att ledningen ställer krav på säkerhet behövs en definierad roll som driver frågan i organisationen samt regelbundet rapporterar arbetets utveckling. En annan framgångsfaktor för informationssäkerhet är att man har en formell dokumentstruktur

som bland annat består av regelverk, instruktioner och riktlinjer. Utan ett fullt implementerat och kommunicerat ramverk för informationssäkerhet blir det svårare för kommunen att hitta en tillfredsställande balans mellan verksamhetens krav på säkerhet och den faktiska säkerheten.

Genom att inte ha rätt säkerhet ökar risken för exempelvis att sekretessbelagd information exponeras, att offentlig information förändras utan kommunens vetskap och/eller att system inte är tillgängliga vid behov.

I uppdragets inledningsfas valde kommunrevisionen nio system som mål för testerna. Målsystemen behandlar uppgifter som av kommunen anses vara kritiska ur både ett sekretess-, integritets- och tillgänglighetsperspektiv. Resultatet av analysen har visat att det är möjligt för en person utan behörighet till interna system att ta sig in på och erhålla åtkomst till ett av de specificerade målsystemen. Analysen förutsätter att attackerna genomförs från en av kommunen registrerad dator. ÖPwC har dock inom ramen för detta uppdrag inte analyserat konsekvenser eller möjligheter att förändra informationen i detta system.

En av orsakerna till att det är möjligt för en obehörig person att ta del av och kunna ändra konfidentiell information kan härledas till en obefintlig, alternativt icke kommunicerad, säkerhetspolicy. Detta kan också vara en anledning till att kommunen inte synes ha tillräckliga rutiner för att installera, konfigurera och uppdatera system. En otillräcklig säkerhetspolicy är sannolikt även anledningen till kommunens lösenordssituation. ÖPwC hittade ett antal lättgissade lösenord som ger högsta behörighet.

Under den period som testerna utfördes från Internet har vi inte sett några indikationer på att våra intrångsförsök har upptäckts, vilket kan vara ett tecken på att kommunen har brister i sin incidenthantering.

1.3 Konsekvenser

Kommunens nuvarande säkerhetsnivå kan få följande konsekvenser:

- Åtkomst till och troligtvis manipulation av information i system vilket skulle kunna innebära ekonomiska förluster och ett skadat förtroende för kommunen.

1.4 Slutsats

Under projektets interna fas kunde ÖPwC få tillgång till intern och sekretessbelagd information och anser därmed att man internt inte har något tillräckligt skydd som uppfyller god praxis.

De system man har på det interna nätverket har inte installerats med tillräcklig säkerhet och kommunen uppmanas att revidera sin miljö på ett sätt som säkrar den interna informationen på ett mer ändamålsenligt sätt. Arbetet med att säkra den interna miljön kommer troligtvis att ta lång tid och till stor del handla om att öka kunskapen och förståelsen för informationssäkerhet bland personalen. IT-säkerhetskrav bör byggas in i den grundläggande systemdesignen samtidigt som policys och riktlinjer bör utformas och kommuniceras.

ÖPwC anser att man genom relativt enkla förändringar kan öka säkerheten avsevärt inom organisationen.

2 Angreppssätt

2.1 Omfattning och mål

Syftet med de genomförda testerna var att granska IT-säkerhetsnivån inom kommunen samt komma med rekommendationer för att höja säkerheten. I enlighet med de nedan definierade scenarierna skulle sekretess, integritet och tillgänglighet testas på de definierade målsystemen. Utöver dessa områden har även viss utvärdering och bedömning av systemen och IT-miljön som helhet genomförts.

Scenario 1 – Externa tester via Internet

En extern hacker, utan djupare kunskaper om Jönköping kommuns, kartlägger organisationens närvaro på Internet. Målet är att bryta sig in i intressanta system exponerade på Internet, alternativt att försöka ta sig in i kommunens interna nätverk och störa tillgängligheten i systemen.

Under den inledande fasen av uppdraget, fastställde kommunrevisionen uppdragets omfattning i form av IP-adresser, alla adresser som har testats är registrerade på Jönköpings kommun.

Scenario 2 – Fysisk åtkomst från det interna nätverket

En person utan behörighet till Jönköping kommuns interna nätverk eller system får fysisk tillgång till det interna nätverket. Personen kartlägger nätverket och attackerar målsystemen. Målet är att få tillgång till och kunna ändra informationen, samt att störa systemens tillgänglighet.

Två nivåer av mål fastställdes innan uppdraget:

1. Att från Internet försöka erhålla obehörig tillgång till externa system exponerade mot Internet eller interna system, alternativt att identifiera sätt att störa systemens tillgänglighet.

2. Att från det interna nätverket försöka erhålla åtkomst till något av de verksamhetskritiska systemen

2.2 Begränsningar

Testerna har begränsats av följande faktorer:

- Tester har enbart genomförts mot utrustning relevant för att uppnå scenariots mål.
- Tester har endast skett mot de tjänster och system som upplevts mest sårbara. Denna bedömning har gjorts med hänsyn till tidsbegränsningar.
- Då ett stort antal system påträffats i nätverket, har endast tester gjorts på ett begränsat urval av dessa.
- Ingen kontroll av rutiner eller policys har genomförts.
- De tester som genomförts ger endast en ögonblicksbild av brister och säkerhetsnivå då testerna utfördes. Ingen hänsyn tas till aktiviteter genomförda före eller efter testperioden.
- För att undvika eventuella driftstörningar har ej tester genomförts där risken för att störa produktion bedömts som hög.

2.3 Genomförande

Uppdraget genomfördes i fyra steg: hotbildsanalys, generell informationsinsamling, intrångsförsök samt rapportering och sammanställning. Det externa steget genomfördes utan att driftspersonal hos kommunen varskoddes om den exakta tidpunkten för testerna. Hotbildsanalysen, där uppdragets scenarier definierades, genomfördes i samarbete med kommunens revisor.

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. Inga attacker eller intrångsförsök genomfördes i detta steg.

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 externa scenariot utfördes via Internet från Öhrlings PricewaterhouseCoopers laboratorium i Stockholm.

Under det interna scenariot genomfördes testerna från lokaler inom kommunen. Öhrlings PricewaterhouseCoopers fick fysisk åtkomst till det interna nätverket, varifrån målsystemen uppsöktes och attackerades.

Kommunrevisionen har godkänt varje steg av testerna innan de utfördes.

3 Resultat

Resultatet av de genomförda testerna har sammanfattats i en bilaga, som sekretessbelagts med stöd av sekretesslagen 5 kap § 2.