Mjölby Kommun

Kommunstyrelsen

För kännedom
Kommunfullmäktige

Granskning av IT-säkerhet

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

Revisorerna har med hänsyn till risk och väsentlighet uppdragit till PwC att granska IT-säkerheten med inriktning på externt intrångstest.

Vår sammanfattande bedömning är att kommunen uppnår en tillräcklig IT-säkerhet för att minimera risker för obehörigt intrång från internet.

Det är dock viktigt att lägga extra fokus på IT-säkerhet och kravställning avseende säkerhetsgranskningar gentemot tredjepartsleverantör. Detta med tanke på den känsliga information som Mjölby kommun hanterar gällande medborgarna och den ökade risken för cyberhot.

Vi rekommenderar att genomföra en riskanalys samt åtgärdsrapport baserat på angivna iakttagelser och rekommendationer i denna rapport. De åtgärder som genomförs bör också revideras och granskas efter införandet för att säkerställa att effekten av åtgärden uppnås.

Vid granskningen gjorda iakttagelser, bedömningar och rekommendationer redovisas i sekretessbelagd rapport, som kommer att kommuniceras med IT-enheten. Granskningens övergripande resultat redovisas i bifogad presentation.

Kommunens revisorer emotser ett skriftligt svar från kommunstyrelse med kommentarer och förslag till åtgärder med anledning av rapporten senast 15 oktober 2016.

För att skapa rätt förutsättningar för en riktig information till och eventuell diskussion i KF ska svar samtidigt tillställas KF.

Mjölby Kommun

För Mjölby kommuns revisorer

2016-06-23

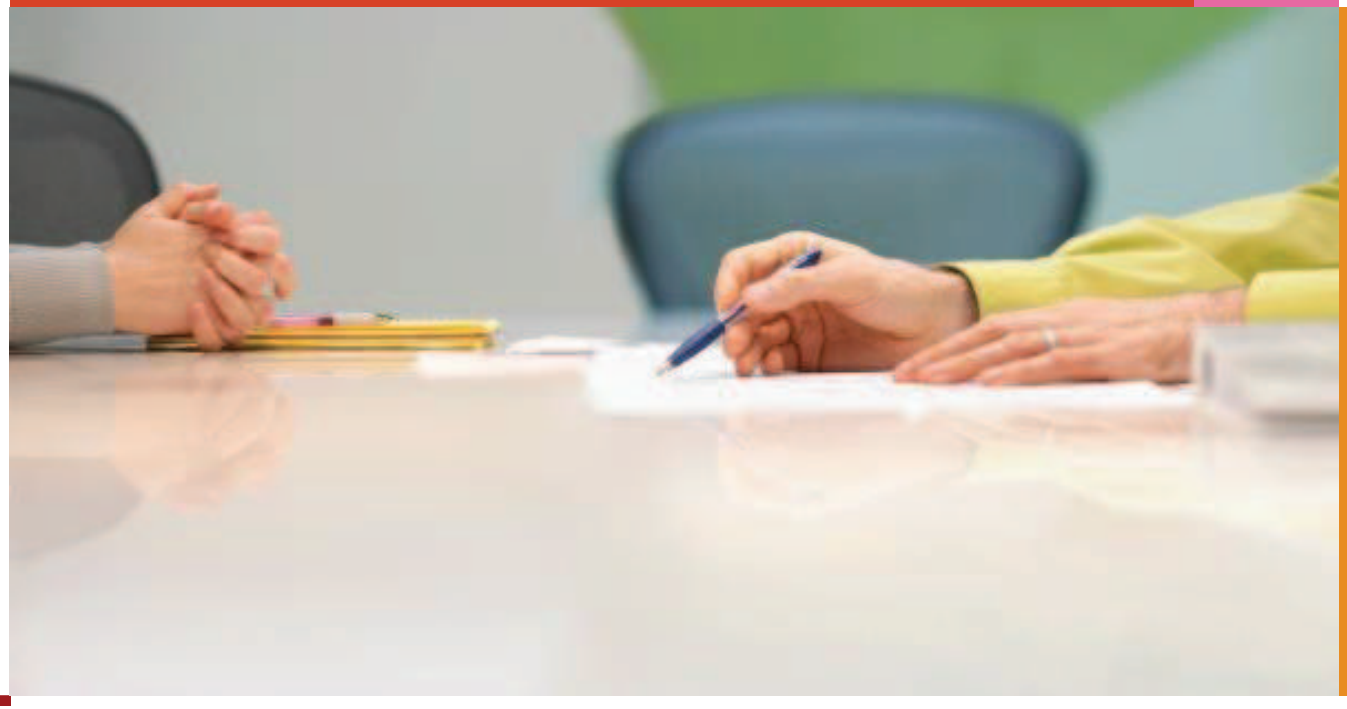
Yngve Welander
Ordförande

Yngve Nilsson
Vice ordförande

www.pwc.com/se

IT-säkerhet
Externt intrångstest

Mjölby kommun
April 2016



pwc

Revisionsfråga

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

För att uppnå granskningens syfte är följande kontrollmål styrande för granskningen:

- *Kommunen har en informations- och IT-säkerhet som anses uppfylla krav enligt god praxis.*
- *Det finns en tillräcklig och tydlig styrning av kommunens informationssäkerhet.*
- *Kommunen har tillfredställande rutiner avseende åtkomst, patch och incidenthantering.*
- *En eventuell attack upptäcks och hanteras av IT-personalen på ett rimligt tillvägagångssätt.*
- *Kommunens externa säkerhetsåtgärder förhindrar eventuella angripare att ”enkelt” få åtkomst till kritisk information utifrån Internet.*

Angreppssätt

Scenario – Extern intrångstest

- En person utan behörighet till kommunens system får via Internet tillgång till kommunens känslig information.
- Hotbilden som illustreras är en extern s.k. ”hacker” som försöker erhålla åtkomst till intern information.

Avgränsningar

Testerna har begränsats av följande faktorer:

- Tester har enbart genomförts mot en begränsad mängd av externa servrar och tjänster. Målsystem har specificerats av kommunen.
- I de fall sårbarheter har detekteras, har fördjupade försök att utnyttja dessa gjorts.
- Endast de mest allvarliga sårbarheterna har verifierats och utnyttjas.
- 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 produktionen bedömts som hög, exempelvis s.k. DDoS attacker (belastningsattacker).

Sammanfattande bedömning

Vi bedömer säkerheten avseende det externa penetrationstestet som strax över medel i jämförelse med liknande testresultat i jämförbara verksamheter.

- De sårbarheter som upptäcktes var av generell karaktär och kan tillsammans bilda en hög risk, med det kräver lång tid och hög budget för att utnyttja.

Resultatet för intrångsförsöket visar att det finns några tveksamma tjänster som bör genomgå en grundligare översyn ex VPN-lösningen, FRI4-systemet m.fl.

12 sårbarheter har identifierats på de granskade IT-systemen. Följande områden innefattar de huvudsakliga säkerhetsbristerna.

- Åtkomst till styrningssystem Solar web
- Bristfällig webbsäkerhet med tanke på användning av https

Det noterades även att Kommunen använder sig av många tredjepartslösningar som inte omfattats av granskningen.

Exempel på sårbarheter

Fronius – Skänninge Idrottshall (kritisk)

- En angripare kan komma åt admin-gränssnittet i lösningen
- Inställning- och inloggningsmöjligheter

Inloggning över http (medel)

- Webbtjänster skickas över http vilket inte rekommenderas

SSL/TLS konfiguration (medel)

- Servrar som använder http är felkonfigurerande

Informationsläckage vid felmeddelande (låg)

- Felmeddelanden som innehåller utförlig information på produktionsservrarna

Slutsats och rekommendation

Vår sammanfattande bedömning är att kommunen uppnår en tillräcklig IT-säkerhet för att minimera risker för obehörigt intrång från internet**.**

Det är dock viktigt att lägga ett extra fokus på IT-säkerhet och kravställning avseende säkerhetsgranskningar gentemot tredjepartsleverantör. Detta med tanke på den känsliga information som Mjölby Kommun hanterar gällande sina medborgare och den ökande risken för cyberhot.

PwC rekommenderar kommunen att genomföra en riskanalys samt åtgärdsanalys baserat på de angivna iakttagelserna och rekommendationerna i denna rapport. 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

Avslutning - frågor