Revisionsrapport

Övergripande säkerhetsgranskning av kommunens säkerhet angående externa och interna dataintrång

Klippans kommun

Björn Johrén,
Säkerhetsspecialist
Juni 2013

pwc

Innehållsförteckning

1. Inledning

1.1. Bakgrund

Hanteringen av risker inom IT-området får allt större betydelse då verksamheten blir allt mer beroende av stöd från IT-system.
En effektiv och framgångsrik riskhantering bygger på ett helhetstänkande. Kvaliteten, säkerheten och effektiviteten i organisationens interna processer ökar och organisationen skyddas mot till exempel obehöriga dataintrång samtidigt som beredskapsmedvetandet stärks inom organisationen.

1.2. Revisionsfråga och kontrollfrågor

Granskningen ska besvara följande revisionsfråga:

Är den interna säkerheten ändamålsenlig när det gäller övervakning, uppföljning och beredskap av obehörigt dataintrång?

Granskningen inriktas mot följande kontrollfrågor:

- Följs kommunens policys/riktlinjer för dataintrångshantering?
- Har kommunen ett ändamålsenligt arbetssätt rörande riskhantering inom IT-området?
- Är roller och ansvar i processen för risk-/dataintrångshantering inom IT-området tydligt definierade?
- Inkluderar processen effektiv kommunikation mot samtliga intressenter?
- Adresserar kommunens riskhanteringsprocess de mest väsentliga riskerna vid dataintrång?

1.3. Metod och avgränsning

Inom ramen för uppdraget har PwC genomfört intervjuer med utvalda personer på Klippans kommun och genomfört analys av dokumentation samt en verifikation av kontohantering och säkerhetsinställningar på server-och operativsystemnivå. Rapporten har övergripande fokuserat på IT generellt och journalsystemet mer specifikt.

Intervjuer har genomförts med följande personer:

- IT-chef
- Medicinsk ansvarig sjuksköterska

Rapporten har varit föremål för sakgranskning av samtliga intervjuade.

2. Observationer och påverkan

2.1. Följs kommunens policys/riktlinjer för dataintrångshantering?

Det finns inom kommunen riktlinjer och policys för IT-säkerhet. Det har dock framkommit i intervjuer att användare kan avvika från riktlinjerna. Exempelvis klickar användare ibland på osäkra länkar i mejl. Dock är IT-avdelningens uppfattning att användare ofta frågar IT när de är osäkra.

Det finns en informell process för hur kommunen hanterar incidenter av intrång eller avbrott i sin IT-miljö. De incidenter som inte löses på en gång, dokumenteras i en loggbok som analyseras och som slutligen leder till en rapport med rekommendationer för framtida lösningar.

Vår kontoanalys visar att behörighetsnivåerna på IT-personalens användarkonton är förhöjda, vilket tyder på att IT själva inte följer riktlinjerna för hantering av konton. Vidare visar analysen att kommunen inte följer internationell standard för lösenordslängd, det vill säga man har 6 stycken tecken istället för rekommenderade 8.

Om avvikande beteenden inte rapporteras till IT kan det innebära att kommunen exponeras för onödiga risker som i slutändan kan leda till ett intrång.

En formell process är enklare att följa upp och mäta.

Om många användare har förhöjda behörigheter, i kombination med svaga lösenord, underlättar det för en obehörig användare att få åtkomst till känslig information inom kommunen.

2.2. Har kommunen ett ändamålsenligt arbetssätt rörande riskhantering inom IT-området?

Vid incidenter av intrång eller avbrott, som inte löses på en gång, skrivs en loggbok och en rapport med rekommendationer för framtida lösningar. Rapporten innehåller bakgrund, händelseförlopp och en summering.

Det saknas en formell process gällande kontroller och uppföljning av obehörig åtkomst till kommunens journalsystem, vilket strider mot patientdatalagen då ”… Vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter…”. Det finns idag ett förslag på en formell process för kontroll och uppföljning på remiss inom kommunen.

Utan en formell process försvåras uppföljning och mätning samt att individberoendet kan öka.

Utan en formell process för uppföljning av åtkomst i journalsystemet innebär det att kommunen kan bryta mot patientdatalagen.

2.3. Är roller och ansvar i processen för risk- / dataintrångshantering inom IT-området tydligt definierade?

Ansvaret för IT-säkerhet och integritetsskydd ligger på IT-säkerhetsansvariga och är definierat i kommunens säkerhetspolicy. Säkerhetspolicyn blev godkänd 2001 och har inte uppdaterats sedan dess.

Det har vid intervjuer framkommit att ett individberoende existerar inom kommunen, kring ansvar för IT-säkerheten. Vidare saknas vissa formella processer inom området, som till exempel en eskaleringsprocess vid incidenter.

Det har även framkommit att det inte genomförs några regelbundna intrångstester eller sårbarhetsanalyser på kommunens IT-miljö, inklusive journalsystemet.

Ej uppdaterade styrande dokument kan leda till mindre effektiva aktiviteter och otydligt ansvar. Det kan i slutändan leda till felaktiga rutiner och processer.

Formella processer kan följas upp, mätas och jämföras för att kunna utvärdera processen.

Utan regelbundna sårbarhetsanalyser eller intrångstester ökar risken för intrång i kommunens IT-miljö.

2.4. Inkluderar processen effektiv kommunikation mot samtliga intressenter?

Vid intervjuer har det framkommit att det saknas en formaliserad eskaleringsprocess vid incidenter. Vid en incident informeras idag IT-chefen och övriga berörda parter, vilket tyder på att den informella processen fungerar.

Vid intervjuer har det framkommit att den informella processen vid genomgång av obehörig åtkomst av en journal i journalsystemet är effektiv. Den sker på individnivå och enligt uppgift har endast berörda parter information om ärendet, vilket är positivt ur sekretess- och kommunikationsaspekt.

Utan en formaliserad process kan intressenter som berörs missa att få informationen alternativt att informationen kommer sent, vilket kan ha en negativ påverkan på hur snabbt organisationen kan vidta åtgärder.

Formella processer kan följas upp, mätas och jämföras för att kunna utvärdera processen.

2.5. Adresserar kommunens riskhanteringsprocess de mest väsentliga riskerna vid dataintrång?

Det finns totalt 23 906 konton inom Klippans kommun, varav 21 662 är aktiva. Utav dessa konton finns ett stort antal användare, cirka 18 000, som inte loggat på inom 90 dagar, vilket motsvarar 76 procent. Av dessa är det dessutom cirka 15 000 konton som aldrig loggat på i systemet, vilket motsvarar över 60 procent.

Vi har även noterat att det finns ett stort antal konton, 21 539 stycken, som är definierade att inte behöva byta lösenord överhuvudtaget.

Det finns totalt 31 konton med administrativa rättigheter, 22 stycken är domänadministratörer och 3 stycken ”Enterprise Admin”. Dessa konton har de högsta behörigheterna i hela IT-systemet.

I journalsystemet genomför kommunen cirka två gånger per år en genomgång av konton för att ta bort inaktiva konton. Denna process är informell och beroende på individer.

Att inte ha kontroll på sin kontohantering samt att användare inte behöver byta lösenord innebär en förhöjd risk för intrångsförsök och förenklar avsevärt vid eventuella intrångsförsök.

Formella processer kan följas upp, mätas och jämföras för att kunna utvärdera processen och kan nyttjas för extern och intern hjälp utan att kommunen tappar lika många upplärningstimmar.

3. Revisionell bedömning och rekommendationer

Granskningens revisionsfråga var: *Är den interna säkerheten ändamålsenlig när det gäller övervakning, uppföljning och beredskap av obehörigt dataintrång?*

Efter att ha granskat kontrollfrågorna bedömer vi att den interna säkerheten inte fullt ut är ändamålsenlig och att det finns en förbättringspotential inom samtliga områden.

Vår granskning har visat att vissa av de informella processerna idag fungerar för kommunen, men att det kan ändras vid en större incident.

Nedan följer våra bedömningar och rekommendationer utifrån granskningens kontrollfrågor.

Följs kommunens policys/riktlinjer för dataintrångshantering?

- *IT-avdelningen bör regelbundet uppdatera användare med information om gällande regler och riktlinjer för IT-användning.*
- *IT-avdelningen bör ta fram en formaliserad incidentprocess för intrång.*
- *IT-avdelningen bör analysera om alla administrativa och domänadministrativa konton är nödvändiga och framförallt om de innehar rätt behörighetsnivå.*

Har kommunen ett ändamålsenligt arbetssätt rörande riskhantering inom IT-området?

- *IT-avdelningen bör etablera en formell process för intrångsincidenter.*
- *Socialnämnden bör skyndsamt implementera processen för kontroller och uppföljning i journalsystemet när den är godkänd från remissinstanserna.*

Är roller och ansvar i processen för risk-/dataintrångshantering inom IT-området tydligt definierade?

- *IT-avdelningen bör se över och uppdatera styrande dokument inom IT-säkerhetsområdet och formalisera processerna för dataintrångshantering.*
- *IT-avdelningen bör genomföra regelbundna sårbarhetsanalyser för att på så sätt säkerställa att en hög IT-säkerhetsnivå finns inom kommunen.*
- *Sårbarhetsanalyser bör genomföras både på interna och externa IT-miljöer och på de applikationer som hanterar känslig information, som till exempel journalsystemet.*

Inkluderar processen effektiv kommunikation mot samtliga intressenter?

- *Processerna för IT och för socialnämnden gällande kommunikation bör formaliseras för att ha tydlighet i åtgärdsstegen och vara behjälplig vid eventuella insatser, både interna och externa, i syfte att förtydliga ansvar och intressenter som berörs.*

Adresserar kommunens riskhanteringsprocess de mest väsentliga riskerna vid dataintrång?

- *IT-avdelningen bör uppdatera behörighetsprocessen inom kommunen och genomföra regelbundna uppföljning av densamma.*

- *IT-avdelningen bör analysera om säkerhets- inställningarna för kommunens konton följer kommunens policy samt utvärdera om policyn ska ändras för att följa god praxis gällande säkerhetsinställningar för konton.*

Utifrån granskningsresultatet och vår riskbedömning rekommenderar vi att Kommunstyrelsen börjar med följande tre åtgärder:

- *Uppdatera behörighetsprocessen inom kommunen och genomföra regelbundna uppföljningar av densamma.*

- *Skyndsamt implementera den formella processen för kontroll och uppföljning av obehörig åtkomst för journalsystemet, som är på remiss vid denna rapportframtagning.*

- *Analysera om säkerhetsinställningarna för kommunens konton följer kommunens policy samt utvärdera om policyn ska ändras för att följa god praxis gällande säkerhetsinställningar för konton.*

- *En uppföljning till våren 2014 för att kontrollera att ovanstående har genomförts.*

2013-06-13

Björn Johrén, Projektledare

Alf Wahlgren, Uppdragsledare