Deloitte.

TIMRÅ KOMMUN
Kommunledningskontoret
2016 -03- 09
Kf3/2016
Dnr. 84 Dpl. 004

Rapport
Hantering av IT-säkerhet

Timrå kommun

Februari 2016

Innehåll

Sammanfattning

Uppdrag och bakgrund

En god intern kontroll är viktig för att kunna uppnå och upprätthålla en hög IT-säkerhetsnivå och minimera riskerna för att verksamheten ska drabbas av allvarliga störningar.
På uppdrag av de förtroendevalda revisorerna har Deloitte granskat IT-säkerhet i kommunen.

Syfte

Syftet med granskningen är att bedöma om den interna kontrollen avseende IT-säkerhetsarbetet är tillräcklig.

Revisionskriterier

Underlag för bedömning är i huvudsak

- Kommunallagen 6 Kap, 7 §
- Interna styrdokument

Svar på revisionsfrågan

Vår bedömning är att den interna kontrollen avseende kommunens IT-säkerhet inte är tillräcklig och bör förbättras.

Iakttagelser

Det finns en dokumenterad ansvarsfördelning. De övergripande dokumenten är inte i alla delar aktuella och behöver uppdateras. Det pågår ett arbete med riskanalyser för de prioriterade systemen i kommunen och det arbetet bör färdigställas. Det bör också förtydligas när riskanalyser ska göras och att kontrollmoment som ska genomföras årligen som en del av den interna kontrollen baseras på en riskbedömning.

Kommunstyrelsen har det övergripande ansvaret för IT-säkerheten. För verksamhetssystemen är kontroller utlagda på systemägare och systemförvaltare vid respektive förvaltning. Vår bedömning är att centrala IT bör ha en mer aktiv roll i att säkerställa att det finns en tillräcklig intern kontroll, även ute vid förvaltningarna.

Rekommendationer

- Färdigställ riskanalyser av prioriterade system och förtydliga vid vilka tillfällen riskanalyser ska göras.
- Se till att de vägledande råden är aktuella.
- Utred om ansvarsfördelningen är ändamålsenlig, exempelvis genom att se till att minst två personer har kännedom om system och rutiner vid varje förvaltning.
- Säkerställ att det finns skriftliga rutiner för exempelvis behörighetshantering och att de rutinerna är ändamålsenliga.
- Se till att det genomförs regelbundna kontroller med avseende på IT-säkerhet och att de kontrollerna baseras på en riskbedömning. Kommunstyrelsen som är övergripande ansvarig för IT säkerheten bör regelbundet inhämta information om vilket arbete som bedrivs vid förvaltningarna.
- Utred om det finns något sätt att automatiskt få en överblick över de anställdas samtliga behörigheter. I dagsläget hålls en manuell förteckning av systemförvaltarna.

Timrå 20 februari 2016
DELOITTE AB

Marianne Harr	Veronica Blank
Certifierad kommunal revisor	Certifierad kommunal Revisor

1. Inledning

Uppdrag och bakgrund

Kommunstyrelsen har det yttersta ansvaret för IT-säkerheten. Nämnderna har ansvaret för IT-säkerheten inom sina verksamhetsområden.

En god intern kontroll är viktig för att kunna uppnå och upprätthålla en hög IT-säkerhetsnivå och minimera riskerna för att verksamheten ska drabbas av allvarliga störningar. På uppdrag av de förtroendevalda revisorerna har Deloitte granskat IT-säkerhet i kommunen.

Syfte och revisionsfråga

Syftet med granskningen är att bedöma om den interna kontrollen avseende IT-säkerhetsarbetet är tillräcklig.
I granskningen ska följande frågor besvaras:

- *Är ansvarsfördelningen för kommunens IT-system aktuell, klarlagd och dokumenterad?*
- *Finns ändamålsenliga rutiner för behörighet och lösenord?*
- *Granskas användandet av kommunens IT-system systematiskt?*
- *Hanteras icke önskvärda incidenteter på ett ändamålsenligt sätt?*
- *Görs riskanalyser regelbundet och på ett systematiskt sätt?*

Revisionskriterier

Underlag för bedömning är i huvudsak:

- Kommunallagen, 6 kap 7 §
- Interna styrdokument

Avgränsning

Granskningen avgränsas till kommunstyrelsen.

Metod

Granskningen har genomförts genom att intervjua ansvarig personal vid kommunledningsförvaltningen och IT avdelningen samt genom att granska dokument. För att få en uppfattning om hur det fungerar har vi också intervjuat systemförvaltare.

2. Granskningsresultat

Organisation och ansvarsfördelning

Ytterst ansvarig för kommunens IT-säkerhet är kommunchefen. Vid kommunledningsförvaltningen finns en central IT-avdelning (centrala IT). Vid avdelningen arbetar en IT-chef, en IT-samordnare, samt en driftansvarig.
Totalt finns 2,5 tjänster vid centrala IT. IT-chef arbetar även som upphandlingschef i kommunen. Centrala IT ligger organisatoriskt under serviceenheten för vilken kommunens säkerhetschef ansvarar.

Driften av kommunens servrar sköts i huvudsak av företaget Evry som fysiskt finns i Malmö. Undantaget är socialförvaltningens system Procapita som hanteras av Tieto i Sundsvall samt skolförvaltningens utbildningsnät, vilket skolförvaltningen själva sköter driften för. I de fall driften är utlagd finns ett driftavtal som bland annat beskriver ansvar och vilken säkerhet som finns hos företaget som har hand om driften.

Det har upprättats en förteckning över alla system som används vid förvaltningarna. I förteckningen framgår vilka personer som är systemägare och systemförvaltare.

Varje förvaltning ska ha en "IT-resursperson" som är första kontaktväg mot Centrala IT. Den personen ska också agera "första hjälpen" för att försöka tyda vad som är fel vid eventuella problem med systemen.

För varje verksamhetssystem ska en systemförvaltare och en systemägare vara utsedd. Systemförvaltare ansvarar för utbildning, utveckling, uppdatering, licensadministration i systemet görs. Den sköter också kontakten med systemleverantör och kommunens driftpartner. Dokumentation av rutiner ska också genomföras.

Systemägare är de personer som ansvarar för verksamheten, d.v.s. förvaltningschef eller avdelningschef. Systemägaren har ansvar för bland annat:
- att externa leverantörer av tjänster och produkter blir informerade om kommunens informations- och säkerhetskrav. - att i en systemsäkerhetsanalys fastställa eventuella tilläggskrav utöver basnivån.
- Att organisation och befattningar som rör systemet möter aktuella behov
- Att fastställa IT-systemets dokumentation och användarhandledning
- att fatta beslut om utveckling av IT-systemet vad gäller nya funktioner och samverka med IT-chef då systemförändringar aktualiseras
- att erforderliga licenser och avtal finns
- att i samverkan med IT-chef fastställa kontinuitetsplan för verksamhetssystemen
- att driftgodkänna verksamhetssystemet

Styrdokument

Det finns ett antal övergripande dokument som rör IT och IT-säkerhet i kommunen. Myndigheten för säkerhet och beredskap (MSB) ger ut vägdelningar kring IT-säkerhet för både myndigheter och privata företag och de ligger till grund för kommunen arbete med styrande dokument kring IT- säkerhet.

Följande styrande dokument finns framtagna:

- Informationssäkerhetspolicy
- Vägledande råd och bestämmelser (VROB) för följande områden:

  -Drift

  -Användare

  -Förvaltning

  -mobila enheter

  -USB

  -Sociala medier

  -Skrivare

I informationssäkerhetspolicyn anges övergripande regler, roller, mål etc. De vägledande råden och bestämmelserna ska konkretisera informationssäkerhetspolicyn. Det framgår inte när informationspolicyn och de vägledande råden och bestämmelserna är framtagna.

Vid granskningen har vi noterat att vissa vägledande råd inte gäller i alla delar. Exempel på det är VROBEN för "drift". I denna står exempelvis att det ska finnas systemsäkerhetsplaner för alla system som bedöms som viktiga. I dessa ska exempelvis loggning, behörighetshantering osv dokumenteras. Enligt intervjuer finns inga sådana planer men GAP analyser ska ersätta planerna. Sedan bestämmelserna skrevs har driften till stora delar outsourcats till Evry och deras arbete styrs av avtal.

Tidigare har kommunens dokument upprättats enligt MSB:s basnivå för informationssäkerhet (BITS). Efter det har nya vägledningar utkommit från myndigheten, ledningssystem för informationssäkerhet (LIS) och det är utifrån detta tankesätt har kommunens nuvarande regler utformas. Syftet med metodstöden är att myndigheter ska kunna få stöd i att upprätta ett ledningssystem för informationssäkerhet. IT-säkerheten ska analyseras, det ska göras riskbedömningar, utformas processer och säkerhetsföreskrifter som därefter ska följas upp.

Om ledningssystemet ska införas måste alla delar finnas med. För närvarande råder en viss förvirring kring vad som gäller och de vägledande råd och bestämmelser som tagits fram stämmer inte med de behov och den ansvarsfördelning som råder nu.

Riskanalyser

Under år 2015 har kommunens prioriterade system identifierats och de uppgår till 10 st. För varje prioriterat system genomförs verksamhetsanalyser och riskanalyser, sk. GAP -analyser. Arbetet är inte avslutat än. Enligt intervjuer ska riskanalyser också göras för nya system. Några sådana direktiv finns dock inte i kommunens styrdokument.

Enligt intervjuer genomförs riskanalyser regelbundet, exempelvis när ett nytt system eller en applikation tas i bruk, men det är inget som dokumenterats och de sker inte systematiskt.

Icke önskvärda incidenter

Icke önskvärda incidenter, exempelvis intrång, hanteras där de uppstår. Är det exempelvis något som uppstår i

socialförvaltningens system hanteras det av systemförvaltaren där. Centrala IT får alltid information först av driftleverantören vid incidenter och därefter tas kontakt med systemägaren.

I det vägledande bestämmelserna och råden anges det att incidenter ska rapporteras till systemägaren och därefter ska det tas beslut om vilken åtgärd som ska sättas in. I bestämmelserna finns inga direktiv om vad som sedan ska göras med incidenterna.

För driften finns anvisningar i avtalet som beskriver vad driftleverantören ska gör vid en incident.

Kontroller och uppföljning

I informationssäkerhetspolicyn anges det att uppföljning är en viktig del av informationssäkerhetsarbetet för att bevaka att:

- beslutade åtgärder är utförda
- årliga mål är uppföljda
- regler följs
- informationssäkerhetspolicy, säkerhetsinstruktioner och riskanalyser vid behov revideras.

En uppföljning som görs av centrala IT är ett årligt IT-bokslut. I bokslutet redogörs det för vilka aktiviteter som genomförts under året och vilka aktiviteter som planeras att genomföras under året därpå. Av 2014 års bokslut framgår exempelvis följande:

• Under 2014 har vårt nät varit tillgängligt 99,2% av tiden.
• Upptäckta virusangrepp och andra hot under året var 9 st.
• E-post med virusrisk 2 570 st, endast 2 mail var utgående från vår e-postserver.
• Mail klassade som "Spam" var 229 041 st.
• Totalt skickades 1 284 511 st mail genom vår server under året.
• Antal ärenden till servicedesk var 2 083 st. Fördelade på 1 339 felanmälningar och 753 förändringar.

Informationen har erhållits från driftleverantören.

I kommunstyrelsens internkontrollplan för år 2014 fanns två moment som berör IT-säkerhet. De kontrollmomenten handlade om att personalen skulle genomgått utbildning i IT säkerhet samt tagit del av vägledande råd och bestämmelser (VROB). För 2015 fanns inga moment gällande IT-säkerhet i kommunstyrelsens intern kontrollplan.

Vi har även efterfrågat planen för socialnämnden. Vid socialförvaltningen kontrollerades loggar(d v s vem som varit inne i olika ärenden) av IT-strategen både år 2014 och år 2015.

Centrala IT gör inte kontroller ute vid förvaltningarna, det är systemägare som ska se till att kontroller görs. Information om vilka kontroller som genomförts vid förvaltningarna inhämtas inte.

Behörigheter och lösenord

I kommunens vägledande råd och bestämmelser finns bestämmelser om behörigheter. Om behörighet står följande:

Endast behörig användare ges åtkomst till ett IT-system

• användares behörighet ska styras utifrån dennas arbetsuppgifter och efter beslut av arbetsledningen

• varje användare ska ha en personlig identitet bestående av login-id och lösenord

• den som är tjänstledig eller av annan orsak har längre frånvaro skall ha sin identitet spärrad

• uppföljning och revidering av tilldelade behörigheter ska ske regelbundet.

Systemförvaltaren ansvarar för hanteringen av behörigheter. Vid intervjuer framkommer det att det finns en arbetsgång vid hantering av behörigheter men inga skriftliga rutiner. En blankett ska fyllas i när en ny person anställs. Det görs av närmaste chef. Blanketten lämnas till systemförvaltaren som därefter lägger upp nödvändiga behörigheter.

När en person slutar ska chefen, via samma blankett, meddela systemförvaltaren och behörigheterna ska därefter tas bort. Enligt intervjuer får systemförvaltaren inte alltid den informationen vilket leder till att behörigheter kan ligga kvar trots en person slutat.

I samband med att personer anställs kan det ha lagts upp många olika behörigheter till olika program. I dagsläget finns det enligt intervjuer inget system för att hålla kontroll på vilka system varje anställd har behörighet till. Det ligger på systemägare och systemförvaltare att hålla kontroll på vilka behörigheter som varje anställd fått tilldelat, ett exempel på hur det hanteras är genom Excel blad med information om behörigheter för respektive person.

Lösenord

I de vägledande råden finns beskrivningar av hur lösenord ska användas.

Lösenordet är personligt och skall hanteras därefter.
Det får inte avslöjas och inte heller lånas ut. Lösenorden ska bytas ut på uppmaning samt med jämna mellanrum. Enligt uppgift ska lösenorden bytas ut var 3:e månad men det varierar beroende på vilket system det gäller.
Lösenordet skall bestå av minst 8 tecken och skall konstrueras så att det inte lätt kan kopplas till den anställde.

Om en anställd försöker logga in med felaktigt lösenord låses systemet efter ett visst antal försök.

Det finns också instruktioner för lösenord för internet och e-mail. Lösenorden ska blandas genom att använda stora och små bokstäver, siffror och specialtecken. Lösenordet bör vara minst 12 tecken långt.

3. Bedömning och rekommendationer

Vår bedömning är att den interna kontrollen avseende kommunens IT-säkerhet inte är tillräcklig och bör förbättras.

En stor del av uppgifterna kring IT-säkerhet för verksamhetsspecifika program och applikationer har lagts ut på de olika förvaltningarna som nyttjar systemen. Det är fortfarande kommunstyrelsen som har det övergripande ansvaret för IT-säkerhet och utifrån det anser vi att centrala IT bör ha en mer aktiv roll i att säkerställa den interna kontrollen avseende IT- säkerhet. I dagsläget tar centrala IT fram kommunövergripande bestämmelser och policys men det sker ingen systematisk uppföljning av att bestämmelser tillämpas eller att det finns en intern kontroll. Vår bedömning är att centrala IT bör inhämta information om de kontroller som utförs vid förvaltningarna.

Ansvarsfördelningen för kommunens olika system är dokumenterad i en förteckning, vilket är bra. För varje system finns en systemägare och systemförvaltare. Vad som ingår i ansvaret framgår av kommunens vägledande råd och bestämmelser (VROB). Vår bedömning är att ansvarsfördelningen bör ses över. I nuläget finns det exempelvis bara en systemförvaltare vid socialförvaltningen vilket inte är säkert ur ett intern kontrollperspektiv. Förvaltningen hanterar en stor mängd känsliga uppgifter i sina system vilket gör att det är särskilt viktigt att den interna kontrollen fungerar. Kombinationen med att det bara är en person som arbetar med systemen och att det saknas skriftliga rutiner gör att det potentiellt kan vara en stor säkerhetsrisk. Den situationen behöver hanteras. Ansvaret för detta vilar på socialnämnden men kommunstyrelsen som övergripande ansvarig för IT-säkerheten bör säkerställa att det görs.

Under vår granskning har vi noterat att de vägledande råden som upprättats inte i samtliga fall är aktuella. Vår bedömning är att de bör uppdateras.

Vår bedömning är att det finns förbättringsmöjligheter gällande behörighetshanteringen. Det är upp till varje systemägare (förvaltningschef eller avdelningschef) att se till att det finns rutiner för behörigheter och lösenord. I vår granskning har vi noterat att rutinerna för behörigheter är inte skriftliga. Dessutom fungerar inte arbetsgången för upplägg och borttagande av behörigheter enligt intervjuer, vilket kan leda till att behörigheter ligger kvar trots att en person inte längre är anställd. Det framkommer att systemförvaltare gör egna kontroller med jämna mellanrum, exempelvis genom att kontrollera om en person inte varit aktiv under en längre period. Dessa kontroller görs dock inte systematiskt. Detta måste hanteras.

Vår bedömning är att användandet av kommunens IT-system i dagsläget inte kontrolleras tillräckligt. Under 2015 har exempelvis det inte funnits några moment i den interna kontrollplanen som avser IT. Vid socialförvaltningen har loggar kontrollerats. Det är viktigt att de moment som kontrolleras baseras på en riskbedömning.

Icke önskvärda incidenter, exempelvis intrång har förekommit vid några tillfällen. I kommunens vägledande råd står att

incidenter ska analyseras och den analysen ska lämnas till systemägaren, d.v.s. förvaltningschef eller avdelningschef.

För närvarande pågår ett arbete med riskanalyser för samtliga system som bedömts som prioriterade i kommunen (10 st). Dessa måste färdigställas och vi har fått signaler om att det behövs stöd i det arbetet vid förvaltningarna.

Vår bedömning är att det måste tydliggöras vid vilka tillfällen riskanalyser ska göras, både när det nya systemet tas i bruk och regelbundna riskanalyser.

Efter genomförd granskning lämnar vi följande rekommendationer:

- Färdigställ riskanalyser av prioriterade system och förtydliga vid vilka tillfällen riskanalyser ska göras.
- Se till att de vägledande råden är aktuella.
- Utred om ansvarsfördelningen är ändamålsenlig, exempelvis genom att se till att minst två personer har kännedom om system och rutiner vid varje förvaltning.
- Säkerställ att det finns skriftliga rutiner för exempelvis behörighetshantering och att de rutinerna är ändamålsenliga.
- Se till att det genomförs regelbundna kontroller med avseende på IT-säkerhet och att de kontrollerna baseras på en riskbedömning. Kommunstyrelsen som är övergripande ansvarig för IT säkerheten bör regelbundet inhämta information om vilket arbete som bedrivs vid förvaltningarna.
- Utred om det finns något sätt att automatiskt få en överblick över de anställdas samtliga behörigheter. I dagsläget hålls en manuell förteckning av systemförvaltarna.

Med Deloitte avses en eller flera av Deloitte Touche Tohmatsu Limited, en brittisk juridisk person (Eng: "limited by guarantee"), och dess nätverk av medlemsfirmor, som var och en är juridiskt åtskilda och oberoende enheter. För en mer detaljerad beskrivning av den legala strukturen för Deloitte Touche Tohmatsu Limited och dess medlemsfirmor, besök www.deloitte.com/about.

Deloitte erbjuder tjänster inom revision, skatterådgivning, business consulting och finansiell rådgivning till offentliga och privata klienter inom en mängd branscher. Med ett globalt nätverk av medlemsfirmor i mer än 150 länder, kan Deloitte erbjuda spetskompetens av världsklass och djup lokal expertis för att hjälpa klienter med de insikter de behöver för att ta itu med sina mest komplexa utmaningar. Deloitte har 200 000 medarbetare i nätverket alla fast beslutna att bli standard of excellence.

Detta dokument innehåller endast allmän information. Varken Deloitte Touche Tohmatsu Limited, dess medlemsfirmor eller deras närstående företag (gemensamt kallade "Deloittes Nätverk") lämnar råd eller tjänster genom denna publicering. Innan beslut fattas eller åtgärd vidtas som kan påverka din ekonomi eller din verksamhet, bör du konsultera en professionell rådgivare. Inget företag inom Deloittes Nätverk är ansvarigt för någon skada till följd av att man har förlitat sig på information i detta dokument.

© 2016 Deloitte AB