GAP analys Timrå kommun Informationssäkerhet

Upprättad av: Krister Svärd, EVRY Sweden AB
2016-11-23 ver 0.9

Scope

Timrå kommun har tagit del av en revisionsrapport från KPMG gällande informationssäkerhet.

I rapporten klargörs att ur ett revisionsperspektiv finns en del frågetecken under rubrikområdet informationssäkerhet gällande organisation, beslutsfattande, planering samt uppföljning. Förutom de noterade bristerna rekommenderar man även i rapporten att vid upprättande av handlingsplaner följa de vägledningar och rekommendationer som sammanställts av MSB (Myndigheten för Samhällsskydd och Beredskap) och som i sin tur relaterar till det etablerade ramverket LIS (Ledningssystem för Informationssäkerhet).

Rapporten från KPMG är gjord på en övergripande nivå och bygger på ett begränsat antal intervjuer och endast den dokumentation man tagit del av, vilket innebär att revisionen på inget sätt är komplett. Samtidigt minskar värdet av detaljgranskning om man noterat avvikelser på ledningsnivå och styrning då det inte finns något relevant underlag att utvärdera revisionen mot.

Uppdraget

Att formulera ett förslag på hur förutsättningar definieras samt hur en GAP-analys genomförs på Timrå Kommun med syfte att identifiera avvikelser i förhållande till MSB:s riktlinjer angivna i dokumentet ”Kommunens Informationssäkerhet – en handledning” samt att rekommendera prioriterade åtgärder för att hantera dessa avvikelser i linje med revisionsrapportens noteringar.

Avgränsningar

Förslaget baseras på den information som kommit till kännedom genom intervjuer och publicerade dokument.

1 Bakgrund

Ur standarden finns att läsa följande:

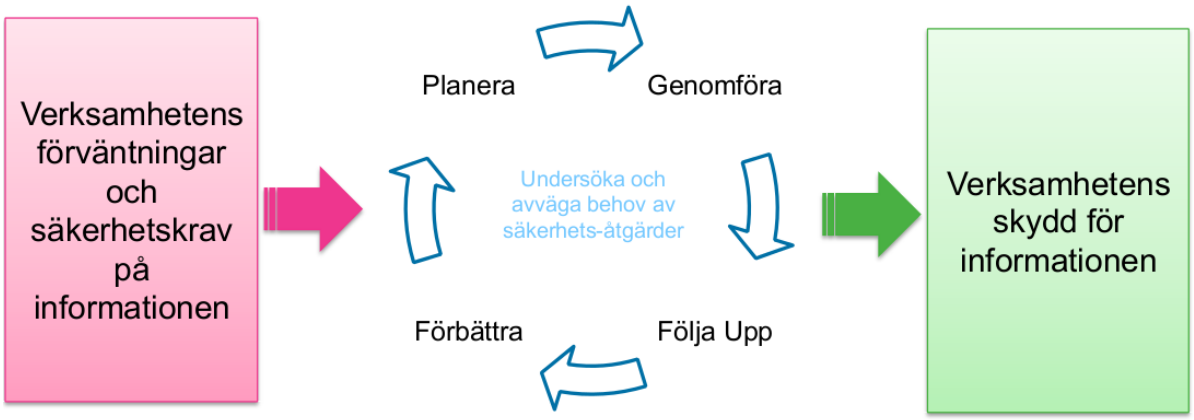
”Liksom andra tillgångar är information en tillgång som är oumbärlig för en organisations verksamhet och följaktligen måste få ett lämpligt skydd. Detta är särskilt viktigt i en alltmer integrerad affärsvärld. Som resultat av denna ökande integration utsätts numera informationen för ökat antal och typer av hot och sårbarhet.”

”Informationssäkerhet innebär skydd av information mot en lång rad hot i syfte att säkerställa kontinuitet, minimera affärsrisk, och maximera investeringsnytta och affärsmöjligheter.”

”Informationssäkerhet uppnås genom att lämpliga skyddsåtgärder införs, inklusive riktlinjer, processer, organisation samt program- och maskinvarufunktioner. Dessa åtgärder behöver utformas, införas, övervakas, granskas och förbättras, där så krävs, för att säkerställa att organisationens specifika säkerhets- och verksamhetsmål uppnås. Detta bör göras samordnat med andra verksamhetsprocesser.”

2 Resultat

Timrå kommun har i sin verksamhet en grundläggande förståelse för vad informationssäkerhet innebär och vid diskussioner med systemägare och systemansvariga finns det en tillräcklig förståelse för grundläggande begrepp. Dock saknas det på flera områden en systematisk handlingsplan avseende hur man identifierar, analyserar och hanterar risker i sin verksamhet vilket måste adresseras.



Genom den outsourcing av infrastruktur som genomförts har Timrå fått möjlighet att säkerställa mycket av de frågeställningar och krav avseende tillgänglighet på IT-system som verksamheten kräver. Detta görs genom de SLA-nivåer som avtalet definierar. (SLA=Service Level Agreement, Servicenivå). Leverantören innehar certifiering avseende ISO27001 och står därmed också under extern revisionskontroll (DNVGL).

3 Förslag till gemensamma handlingsplaner

Risk Management
Denna rapport föreslår att Timrå Kommun införskaffar ett så kallat LIS, dvs Ledningssystem för Informationssäkerhet med fokus på riskhantering och där Central IT är systemägare och systemförvaltare. I ett sådant system registreras alla skyddsvärda system och i detta system hanteras en strukturerad riskhanteringsprocess där man bedömer risker samt också tar dokumenterade och spårbara beslut kring hur man väljer att hantera dessa risker. Ett sådant system kan också säkerställa att verksamheten med automatik blir påmind om att regelbundet genomföra uppdaterade riskanalyser. Det föreslås också att Timrå Kommun väljer en enkel modell för riskbedömning för att säkerställa att bedömningarna utförs och inte onödigt belastar verksamheten med administrativa uppgifter. Bedömning av ett system skall normalt inte ta mer än 30 minuter att genomföra (periodicitet föreslås vara 12 månader)
Det föreslås också att rapporterade risker regelbundet bedöms av kommunens ledningsgrupp som därvid dokumenterar sitt beslut om hantering av riskerna.

Vägledande råd och bestämmelse
I denna rapport förutsätts att de till KS föreslagna VROB avseende IT-relaterade frågor antas och att mandatet för att underhålla och revidera dessa delegeras till Central IT.

Uppdragsbeskrivning Central IT
Under faktainsamlingen till denna rapport har det framkommit oklarheter kring exakt vilket uppdrag och mandat som Central IT har i förhållande till verksamheterna. Som exempel finns inget tydligt ägarskap över den samlade IT-arkitekturen och systemlandskapet.

Dokumentation
Timrå Kommun bör överväga strategi och metodik avseende struktur och metodik avseende framtagning av olika nivåer av dokumentation, tex processdokumentation och tillhörande instruktioner samt övrig systemrelaterad information.

Genom att skapa organisation, systematik och kontinuitet i den interna hanteringen skapar det bättre förutsättningar att genomföra välgrundade investeringar och höja företagets position inom IT på sikt.

Säkerhetsmedvetande
Ledningen för Timrå Kommun bör överväga att genomföra en riktad utbildning inom Informationssäkerhet för samtliga användare. Detta kan tex genomföras genom sk Nano utbildning, där varje utbildningsdel tar 3-5 minuter att genomföra. Genom en sådan utbildning kan driftstörningar minimeras och risken för obehörig informationsspridning minskas.

4 Prioriterade system

Timrå har definierat 10 st prioriterade system (se Prioritering av samhällsviktiga system 2013.pdf). Denna lista bör regelbundet revideras (se förslag om LIS ovan) för att spegla den aktuella verksamheten. Denna rapport tar dock endast upp dessa definierade system.

4.1 IT-infrastruktur

Detta stora område hanteras i princip helt genom det outsourcingavtal som finns etablerat med EVRY och uppfyller alla de krav som verksamheten idag har på tillgänglighet och rapportering. Det är dock viktigt att notera att det är Central IT som måste säkerställa att det inte finns några komponenter som ”faller mellan stolarna”. Som exempel på detta är att kraftförsörjning av kommunhuset faller inom ramen för detta åtagande.
Inom detta område påtalas också att det finns ett behov att central IT validerar att gällande servicenivåer för kommunikation till prioriterade arbetsplatser, tex äldreboenden, uppfyller verksamhetens krav.

4.2 Kommunens telefonväxel

Timrå Kommun har ett samarbete med Sundsvalls kommun avseende teknisk uppbyggnad och bemanning av telefonväxel. Dokumenterat ansvar samt strategi och teknik för att säkerställa tillgänglighet för kommunens telefonväxel saknas i nuläget och bör kompletteras samt testas regelbundet.

4.3 WWW.TIMRA.SE

Den externa webben har små behov av att säkras mot dataförluster då informationsomsättningen är låg. Däremot så har systemet höga krav på tillgänglighet och efter 4 timmars driftsstopp bedöms det som att allvarlig påverkan föreligger.
Denna rapport föreslår att Central IT undersöker om nuvarande Servicenivåer är tillräckliga för detta system eller om högre servicenivåer är nödvändiga. Det föreslås även att det upprättas ett testsystem där kvalitetstester kan genomföras innan driftsättning och i samband med detta föreslås att även detta system kan agera som autonomt reservsystem om sådant behov skulle uppstå och därigenom med snabbhet kunna ersätta ordinarie system tillfälligt vid allvarlig driftstörning.

4.4 Mailsystemet

Mailsystemet har ur tillgänglighetssynpunkt olika värdering beroende på vem i verksamheten som tillfrågas. För vissa delar av verksamheten är det kritiskt för att utväxla information som rör liv och lem (Kommunens

sjuksköterskor som kommunicerar med krypterad mail med Landstinget). Tillgängligheten garanteras genom samma outsourcing avtal som nämns under 4.1

Timrå Kommun bör vara uppmärksam på att det finns flera mailsystem som används, Skola vs administration, och att detta skapar samverkansproblem. En analys bör genomföras om det är möjligt att enas om ett gemensamt system för all personal och evt även elever.

Denna rapport rekommenderar att man genomför en användarutbildning som uppmärksammar användarna på riskerna med att använda okända eller misstänksamma länkar i mail samt öka medvetandet för att information som skickas via mail är läsbart för alla som kan avlyssna datatrafiken.

Det rekommenderas även att det finns en dokumenterad plan, ”Roadmap”, som planerar när Timrå Kommun skall byta version av mailsystem för att bibehålla godkänd servicenivå.

4.5 Geosecma

Geosecma har måttliga krav på tillgänglighet och merparten av förlorad data kan återskapas via andra datakällor eller manuellt arbete. Även om andra funktioner inom kommunen såsom räddningstjänsten och externa parter såsom MittSverige Vatten använder information vid allvarlig kris så är det inget som förhindrar deras arbete. GIS data är i sig själv ett kraftfullt informationsverktyg och skulle felaktigt kunna användas för att sprida känslig information vilket måste beaktas i förvaltningsarbetet. Denna rapport föreslår att de riskscenarier som identifierats för Geosecma aktivt bearbetas och dokumenteras i ett LIS verktyg.

4.6 Procapita

ProCapita är Timrå Kommuns mest komplexa system med både informationsströmmar som avser persondata, men också ekonomiska betalströmmar och operativ planeringsinformation och vårdtagarinformation. Under många år har systemet administrerats, med stor framgång, av en enskild tjänsteman. Detta har skapat ett stort nyckelpersonsberoende som Timrå Kommun inte kan bortse från utan måste aktivt hantera inom närtid. Timrå Kommun bör också se över ansvar och rollfördelning med tillhörande rutiner som skall aktiveras när systemet har driftstörningar. Det finns indikationer på att verksamhetsansvariga inte fullt ut tar sitt ansvar för att hantera sin verksamhet när det uppstår störningar i systemet.
Det finns identifierade informationssäkerhetsrisker i systemet som bör dokumenteras och strukturerat hanteras i en dokumenterad beslutsprocess.

4.7 Teis

Då Teis är en viktig integrationslänk för flera system, är det också viktigt att särskilt fokus sätts på informationsintegriteten. Bedömningen är att det saknas en tydlig definition av vilka integrationer som skall övervakas och vid vilka kriterier som larm skall skapas för analys och åtgärd. Central IT är förvaltare av detta system, men det uppfattas som osäkert om det finns en tydlig förvaltningsinstruktion kring detta system.

4.8 LEX

Lex finns upptagen som prioriterat system då det finns tydliga lagmässiga krav på hur information till kommuner skall hanteras. Till viss del kan störningar hanteras genom strukturerade manuella rutiner, men efter 1-2 dagar blir störningarna besvärande och efter ca en vecka kan det uppstå problem med att uppfylla lagens krav inom detta område. Skulle data förvanskas eller försvinna uppstår problem efter ca 2 dagar att återregistrera information. Då Timrå Kommun har för avsikt att integrera Lex med framtida e-tjänster bör det finnas en dokumenterad godkännande process för varje sådan integration för att säkerställa att det tas hänsyn till eventuella informationssäkerhetsrisker.

4.9 eCompanion/Besched

Timrå Kommun har för avsikt att upphandla nytt lönesystem under 2017. Strategi finns för att säkerställa att lönesystemet är stamdata för all personaldata, som dock även kompletteras med hjälp av data från KIR. Systemet har olika krav på tillgänglighet beroende på vilken tidpunkt som finns i månaden. Som reservplan vid systembortfall under utbetalningsperiod så föreslås att Timrå Kommun etablerar en reservrutin som innebär att utbetalande bank kan betala ut samma transaktioner som föregående månad.

4.10 Aditro (Visma) Redovisning och reskontra/Inköp och faktura

Timrå Kommun har för avsikt att genomföra en upphandling av nytt ekonomisystem under 2017 som skall vara i drift 2018-01-01. I nuvarande system bedöms att stillestånd kan vara upp till en arbetsvecka, men att dataförlust blir kritiskt efter 24 timmar. Det finns ett antal integrationer som transporterar data både in och ut ur systemet och här föreslås att en mer aktiv övervakning av dessa integrationer implementeras.