

ABCD

Varbergs kommun

**Kommunens IT-verksamhet
Granskningsrapport**

Audit
KPMG AB
13 april 2015

Innehåll

1.	Sammanfattning	2
2.	Bakgrund och syfte	4
3.	Ansvarig nämnd/styrelse	5
4.	Metod	5
5.	Projektorganisation	5
6.	Organisation inkl. resurser	5
7.	Hur är ansvarsfördelningen reglerad mellan styrelse och nämnder?	6
8.	Kommunikationen mellan centrala IT-avdelningen och verksamheterna	8
9.	Inköp av utrustning och olika system	8
10.	Hur harmoniserar olika system med varandra?	9
11.	Tillgodoses verksamheternas önskemål på olika system	9
12.	Vem har helhetssyn på kapacitetsutnyttjandet avseende de olika systemen?	10
13.	Hur fungerar konsultstödet till de olika systemen?	11
14.	Hur är ansvaret för IT-säkerheten reglerat?	11
15.	Vilka kontroller kopplat till IT-säkerhet genomförs?	13
16.	Är IT-säkerhetsplaner och annan dokumentation uppdaterade?	13
17.	Övrigt	14

1. Sammanfattning

Vi har av Varbergs kommuns revisorer fått i uppdrag att göra en granskning av kommunens IT-verksamhet. Syftet med granskningen har varit att bedöma om kommunens organisation, ansvarsfördelning och finansiering är effektiv och ändamålsenlig.

Granskningen har i första hand avsett kommunstyrelsen som är strategiskt ansvarig för IT-frågorna och servicenämnden som är operativt ansvarig. Även barn- och utbildningsnämnden har ingått i granskningen.

Kommunens IT-verksamhet är fördelad på olika funktioner i kommunen. Förutom IT-avdelningen som organisatoriskt ligger under servicenämnden finns en servicedesk som är förvaltningsövergripande. De större förvaltningarna har även egna personella resurser för att stötta förvaltningsinternt i IT-frågor. Kommunen har en hög ambitionsnivå vad gäller utveckling av IT-lösningar riktade såväl kommuninternt som utåt mot medborgarna. Samtidigt är antalet anställda inom IT-avdelningen relativt få i jämförelse med andra liknande kommuner vilket gör att vi kan fundera över sårbarheten vid t.ex. sjukfrånvaro eller frånvaro på grund av vård av sjuka barn.

Ansvarsfördelningen är väl definierad i "IS/IT Varbergs kommun" daterad 2011-05-09. Denna är dock under uppdatering och en ny ansvarsfördelning har godkänts i kommunens IT-styrgrupp och ligger för närvarande för beslut i KSAU. Innebörden av det nya förslaget är att allt mer av strategiska frågor förs över från kommunstyrelsen till servicenämnden. Det är i detta sammanhang viktigt att inte tappa bort kommunstyrelsens övergripande ansvar för kommunens informationssäkerhet.

Kommunikationen mellan centrala IT-avdelningen och verksamheterna har förbättrats betydligt under senare år. Fortfarande finns brister och dessa beror mest på låg bemanning på IT-avdelningen varför supportärenden kan bli liggande längre tid än den som behöver supporten förväntar sig. Anledningen kan vara att mer prioriterade ärenden dyker upp och/eller på grund av sjukdom inom IT-avdelningen.

Inköp av utrustning sker genom att verksamheterna inom sin budget avropar utrustning via kundservice. Kommunen har ramavtal med ATEA som levererar av kommunen specificerad utrustning. Kommunövergripande system ansvarar IT-avdelningen för medan verksamheterna köper in sina egna verksamhetsspecifika system. IT-avdelningen stöttar tillsammans med upphandlingsavdelningen vid dessa tillfällen. Barn- och utbildningsförvaltningen köper utöver detta Apple-datorer till eleverna och ansvarar själva för driften av dessa.

Varbergs kommun har ett antal tekniska integrationsplattformar vilket gör att olika system kan prata med varandra (harmoniserar). Detta fungerar i huvudsak väl.

Verksamheternas önskemål på olika system är väl tillgodosedda. Verksamhetsspecifika system ansvarar förvaltningarna själva för att de är uppdaterade och anpassade för verksamheten. De kommunövergripande systemen ansvarar IT-avdelningen för. I övrigt är inriktningen att använda

så mycket som möjligt av Microsofts produkter som möjligt vilket skapar en standard och rimliga förväntningar hos användarna.

Avseende frågan om vem som har helhetssyn på kapacitetsutnyttjandet av de olika systemen är svaret att det inte finns någon som särskilt ansvarar för detta. Varje nämnd och förvaltning har själva ansvaret för vilka system de vill använda. Den rent tekniska kapaciteten övervakas av IT-avdelningen och man har också gjort en genomgång huruvida kommunen har system som gör samma saker. Denna genomgång resulterade i att tre enkätsystem plockades bort. I takt med att kommunen använder sig alltmer av molntjänster¹ blir frågan mindre aktuell.

Konsultstöd till de stora systemen såsom ekonomi- och PA-system, Procapita etc. köps av leverantören. I övrigt är det kundservice och IT-avdelningen som supportar. I första hand är det Kundservice, som fungerar som s.k. first line support, som användare ska vända sig till vid problem. Här sitter tre personer som tidigare arbetade på IT-avdelningen och man kan fundera över om detta är en bra lösning. Risken finns att dessa personer tappar i kompetens då de inte har daglig kontakt med IT-avdelningen på samma sätt som tidigare, samt att de även arbetar med fastighetsfrågor.

Begreppet IT-säkerhet håller på att fasas ut. Man talar gärna istället om informationssäkerhet numera där IT-säkerhet ingår som en del. I takt med att Varbergs kommun blir alltmer öppen mot omvärlden ökar vikten av informationssäkerhetsarbetet. Det finns ett antal dokument som reglerar ansvaret för informationssäkerheten i kommunen. En del är av äldre datum men det pågår ett arbete med att uppdatera. Fullmäktige beslutade t.ex. 2014-11-25 att anta policy för informationssäkerhet i Varbergs kommun och i beslutet ingår att ge kommunstyrelsen i uppdrag att utarbeta en strategi för genomförandet av policyn.

Kontroller kopplade till IT-säkerhet och informationssäkerhet förekommer sparsamt i nämndernas interna kontrollplaner. En gång per år genomförs kontroll av verifieringssystemet för hemtjänstpersonal och denna revision görs av en utomstående organisation – Veritas. Vi rekommenderar att t.ex. IT-styrgruppen ansvarar för att påminna nämnderna om att det bör finnas en kontrollpunkt om informationssäkerhet varje år i de interna kontrollplanerna.

Vad gäller aktualiteten i IT-säkerhetsplaner och annan dokumentation finns brister. Bristerna är dock uppmärksammade och det pågår ett intensivt och stort arbete med uppdatering av relevanta dokument.

Vad gäller den fysiska säkerheten finns brister. T.ex. förvaras servrar och backup-utrustning i samma lokal. Vi rekommenderar en genomgång av den fysiska säkerheten där med fördel MSB:s rekommendationer kan vara till hjälp.

Vi rekommenderar:

¹ En molntjänst är en teknik där stora skalbara resurser, exempelvis processorkraft, lagring och funktioner, tillhandahålls som tjänster på Internet. Användaren eller köparen behöver i sin tur inte ha någon teknisk kunskap eller kontroll över infrastrukturen. En molntjänst omfattar även programvara där Internet används för att tillgodose slutanvändarnas IT-behov, exempelvis genom att använda en webbläsare och via den köra ett program som finns på en okänd server. En vanligt förekommande molntjänst är webmail.

- Se över bemanningen på IT-avdelningen med tanke på det ambitiösa uppdrag som avdelningen har.
- Att kommunstyrelsen även fortsättningsvis tar sitt övergripande ansvar för informationssäkerheten med tanke på att allt mer av ansvar förs över på Servicenämnden.
- Fundera över om det är lämpligt att first line support ska finnas utanför IT-avdelningen som en egen funktion.
- Se över hur man kan säkerställa att nämnderna alltid har med en kontrollpunkt i sina interna kontrollplaner som har bäring på informationssäkerhet.
- Genomlysning och riskbedömning av den fysiska säkerheten

2. Bakgrund och syfte

Vi har av Varbergs kommuns revisorer fått i uppdrag att göra en granskning av kommunens IT-verksamhet. Syftet med granskningen har varit att bedöma om kommunens organisation, ansvarsfördelning och finansiering är effektiv och ändamålsenlig.

I granskningen ingår att bedöma följande övergripande frågor:

- Hur är kommunens IT-verksamhet organiserad?
- Hur är ansvarsfördelning reglerad mellan styrelse och nämnder?
- Hur fungerar kommunikation mellan centrala IT-avdelningen och olika verksamheter?
- Hur regleras inköp av utrustning och olika system?
- Hur harmoniserar olika system med varandra?
- Tillgodoses verksamheternas önskemål på olika system?
- Vem har helhetssyn på kapacitetsutnyttjandet avseende de olika systemen?
- Hur fungerar konsultstödet till de olika systemen?
- Hur är ansvaret för IT-säkerheten reglerat?
- Vilka kontroller kopplat till IT-säkerhet genomförs?
- Är IT-säkerhetsplaner och annan dokumentation uppdaterade?
- Vilka resurser (ekonomiska och personella) finns för att säkerställa IT-verksamheten?

3. Ansvarig nämnd/styrelse

Granskningen avser i första hand kommunstyrelsen som är strategiskt ansvarig för IT-frågorna och servicenämnden som är operativt ansvarig. Dock ingår även och barn- och utbildningsnämnden i granskningen.

4. Metod

Granskningen har genomförts genom dokumentstudier och analys av relevanta dokument samt avstämningar med berörda personer.

5. Projektorganisation

Granskningen har genomförts av Göran Andersson, Certifierad kommunal revisor.

6. Organisation inkl. resurser

6.1 Iakttagelser

Varbergs kommuns IT-avdelning ingår i serviceförvaltningen som även ansvarar för "Kost och städ", "Fastighet" samt "Kundservice".

Budgetomslutningen är ca 36 miljoner kronor och avdelningen är helt och hållet intäktsfinansierad via förvaltningsorganisationens budgetar. D.v.s. de olika förvaltningarna i kommunen köper IT-avdelningens tjänster till priser som fastställs i prislista. Priset som respektive förvaltning betalar för de olika tjänsterna är beroende på serverkapacitet, grad av service, eventuella tilläggstjänster etc.

Avdelningen har 18 personer anställda som är indelade i tre enheter. Utveckling och förvaltning driver olika former av utvecklingsprojekt. Underavdelningen har förutom avdelningschefen sex projektledare anställda. På IT-service arbetar förutom enhetschefen nio personer. De flesta av dessa är tekniker. IS/IT-strategikontor består av IT-chefen och kommunens IS-strateg.

IT-avdelningens målgrupp består av ca 16.000 användare förutom alla kommuninvånare som är ca 60.000. Antal datorer som finns i nätverket är ca 8.000 st.

Barn- och utbildningsförvaltningen som också ingår i denna granskning har en egen organisation som arbetar gentemot skolan. Den består av sammanlagt sex personer varav tre arbetar med administration, upphandling, system och ekonomi. Tre personer arbetar som IT-pedagoger med att bland annat stötta lärarna i sitt IT-användande.

6.2 Analys och bedömning

Varbergs kommun har i förhållande till en genomsnittlig kommun en hög ambitionsnivå. Ambitionen är en öppen kommun med allt vad det för med sig av IT-lösningar som ska underlätta

för medborgarna att komma i kontakt med kommunen t.ex. via webben. Ett stort arbete pågår också med att standardisera och att staka ut vägen mot allt mer av molnlösningar. Utvecklingen kan ses som ett paradigmskifte.

Sett i detta perspektiv är organisationen något sårbar. De arton personer som arbetar på avdelningen har sina specialområden vilket innebär att om någon är frånvarande på grund av sjukdom eller vård av sjukt barn påverkas servicen till verksamheterna. Det är något som t.ex. barn- och utbildningsförvaltningen påpekat.

En jämförelse som IT-avdelningen själva gjort med andra IT-avdelningar inom länet visar att antalet anställda i Varberg är lågt. Kungsbacka kommun som kan betecknas likvärdig har drygt dubbelt så många anställda inom IT-avdelningen (42 st).

Vi kan självklart inte rekommendera att utöka antalet anställda utan någon grundläggande analys men rekommenderar att en genomgång görs av arbetsuppgifter och koppling till ambitionsnivån gällande IT-utbyggnaden i kommunen och utifrån detta göra en bedömning av hur mycket personal som är rimligt att ha.

7. Hur är ansvarsfördelningen reglerad mellan styrelse och nämnder?

7.1 Iakttagelser

Ansvarsfördelningen beskrivs i IS/IT för Varbergs kommun daterad 2011-05-09. Sedan granskningen gjordes har ny ansvarsfördelning godkänts i IT-styrgrupp och ligger för beslut i KSAU.

Nuvarande ansvarsfördelning är enligt nedan.

Kommunfullmäktige fastställer vision/mål och inriktning för Varbergs kommun.

Kommunstyrelsen ansvarar för tillämpningen av visioner och mål genom att fastställa strategi för IS/IT-verksamheten. Kommunstyrelsen har ansvaret för kommunövergripande uppföljning och utvärdering av strategin. I kommunstyrelsens ledningsfunktion ingår att leda och samordna kommunens IS/IT-strategiska frågor.

Nämnderna har ansvar att arbeta vidare med strategin för den egna verksamheten.

Servicenämnden har ett särskilt ansvar för IS/IT-frågorna i form av drift, användarstöd samt förvaltning och ändringshantering för kommunens grundläggande teknik- och systemplattform samt på uppdrag för övriga system.

Kommunstyrelsen ansvarar också för:

- IT/IS-utveckling för systemlösningar som antingen involverar flera förvaltningar, flera processägare eller flera systemägare. Hit hör t.ex. det samlade utbudet av e-tjänster.
- Att ha överblick över kommunens samlade systemlösningar och integrationer.
- Att hålla i de grundläggande krav på system i kommunen som ska gälla i alla upphandlingar.
- Utveckling som berör flera huvudmän.
- Gemensamma metoder.
- Övergripande uppföljning av IS/IT-verksamheten.
- Övergripande ansvar för IT-säkerhet.

I förslaget till ny ansvarsfördelning är det mesta av ovanstående flyttat till servicenämnden.

I Varbergs kommun talas det allt mindre om IT. I allt större utsträckning används ett vidare begrepp som benämns ”Digitala tjänsters livscykel”. Ett utvecklingsprojekt startades i december år 2014 och pågår fortfarande. Ansvarsfördelningen mellan kommunstyrelsen och servicenämnden kommer att förändras så att troligen mer ansvar kommer att läggas på servicenämnden. I vilken omfattning är ännu inte klart.

Tanken med projektet är delvis att tona ner begreppet IT och istället fokusera på verksamhetsutveckling, d.v.s. stötta förvaltningarna med IT-lösningar i syfte att underlätta deras verksamhetsutveckling och måluppfyllelse. Projektet ska leda till en strukturerad process med tydliga roller för den ”digitala resa” som kommunen inlett med allt mer digitala tjänster. Även roller på såväl strategisk, taktisk och operativ nivå ska mejslas ut och tydliggöras enligt projektdirektiven.

7.2 Analys och bedömning

Ansvarsfördelning och roller är tydliga och väl dokumenterade. I praktiken upplevs det inte lika tydligt. Det har varit otydliga beslutsvägar, otydliga roller, mandat och forum. I den översyn av roller av ansvar som kommunen nu håller på med är det viktigt att inte kommunstyrelsens roll som ytterst ansvarig för informationssäkerheten förminskas.

Vi anser det vara föredömligt att ”växla spår” från att se IT som en fristående företeelse för att istället se IT som ett stöd i verksamhetsutvecklingen som pågår i förvaltningarna. Här finns ett ömsesidigt ansvar fördelat mellan servicenämnden (IT-avdelningen) och övriga nämnder. En väl utvecklad kommunikation mellan IT-avdelningen och förvaltningarna gör sannolikt att nya lösningar kommer till stånd. Viljan och inriktningen finns.

8. Kommunikationen mellan centrala IT-avdelningen och verksamheterna

8.1 Iakttagelser

Kommunikation med verksamheterna sker på olika nivåer. På strategisk nivå finns en IT-styrgrupp med representanter från verksamheterna och IT-avdelningen. På taktisk nivå finns ett antal kundansvariga på IT-avdelningen som kommunicerar med verksamheterna genom att t.ex. föra en dialog om hur IT-tjänsterna kan hjälpa till att stödja verksamheterna. Den operativa nivån handlar om mer konkreta saker som teknisk drift, applikationsdrift och servicedesk.

På strategisk och taktisk nivå fungerar kommunikationen väl. På den operativa nivån fungerar det inte lika bra. Det förklaras av de som vi har intervjuat med att IT-avdelningen är sårbar såtillvida att flera av de anställda är specialiserade inom vissa områden. På grund av att IT-avdelningen har relativt få anställda och kommunen har en hög ambitionsnivå kan det vid t.ex. sjukdom, VAB och liknande gå ut över servicen till verksamheterna. Detta är ett problem som både verksamheterna och IT-avdelningen påpekar. Alla operativa ärenden genomgår en prioritetsprövning såtillvida att t.ex. kritiska systems funktion prioriteras före problem av mindre allvarlig karaktär. Det är inte alltid som verksamheterna får information om varför just deras ärende tar längre tid än vad de förväntat sig.

8.2 Analys och bedömning

Vår bedömning är att Varbergs kommun har en hög ambitionsnivå inom området digitala tjänster. IT-avdelningen har en ambition att gå från traditionell driftorganisation till en framåtsyftande och stödjande funktion till övrig verksamhet i kommunen. Uttrycket "IT-projekt" har ersatts av "Verksamhetsutvecklingsprojekt". Detta synsätt bygger på en väl utvecklad kommunikation på strategisk och taktisk nivå och här har man kommit långt. Lika mycket fokus har inte lagts på kommunikationen på den operativa nivån och detta i kombination med en slimmad organisation gör att det ibland blir brister i kommunikationen på den nivån. Det upplevs dock inte som ett stort problem av de personer vi har intervjuat i barn- och utbildningsförvaltningen. I huvudsak upplevs kommunikationen ha förbättrats radikalt de senaste åren.

9. Inköp av utrustning och olika system

9.1 Iakttagelser

Inköp av utrustning görs av IT-avdelningen. Avdelningen avgör själva, inom ramen för sin budget, vilken utrustning den behöver köpa in för att hålla och utveckla nivån på den infrastruktur som krävs för att hela den digitala miljön ska fungera. Förvaltningarna beställer sin utrustning via kundservice som via ramavtal med ATEA beställer och levererar, via IT-avdelningen, till verksamheterna.

Kommunövergripande system ansvarar IT-avdelningen för medan verksamheterna köper in sina verksamhetsspecifika system. I framtagande av kravspecifikation inför upphandling deltar IT-avdelningen med sin expertis.

Barn- och utbildningsförvaltningen har datorer från Apple som elevdatorer. Dessa leasas och är konfigurerade enligt förvaltningens specifikationer vid leverans. IT-avdelningen har ingenting med dessa att göra utan tillhandahåller bara trådlös uppkoppling till internet. Att barn- och utbildningsförvaltningen valt Apple beror på att man upplever att det blir ”mindre strul” med dessa jämfört med andra.

9.2 Analys och bedömning

Vår bedömning är att inköp av utrustning och olika system är ändamålsenlig.

10. Hur harmoniserar olika system med varandra?

10.1 Iakttagelser

Varbergs kommun har ett antal integrationsplattformar som möjliggör att olika system kan ”prata” med varandra. För att ytterligare underlätta informationsöverföring mellan olika system försöker man hålla dem uppdaterade versionsmässigt.

Det hela fungerar bra men små irritationsmoment förekommer, dock inte ofta. Det handlar om att vissa system inte ”synkar” på grund av att något system kräver senaste version av Java och IT-avdelningen har kanske inte certifierat användningen av den.

10.2 Analys och bedömning

Med så många olika system som en kommun har är det ofrånkomligt att det någon gång uppstår problem, eller i det fall som barn- och utbildningsförvaltningen berättade om, smärre irritation.

Att IT-avdelningen måste certifiera olika program innan de används i skarp miljö är en självklarhet.

11. Tillgodoses verksamheternas önskemål på olika system

11.1 Iakttagelser

Förutom rena verksamhetssystem använder sig Varbergs kommun av Microsoft i så stor utsträckning det går. Man försöker också göra allting så standardiserat som möjligt.

Kommungemensamma system ansvarar IT-avdelningen för. Att de verksamhets specifika systemen tillgodoses ansvarar verksamheterna själva för.

IT-avdelningens uppfattning är att verksamheternas önskemål tillgodoses. Barn- och utbildningsförvaltningen har ingen annan uppfattning.

11.2 Analys och bedömning

Det finns ingenting som tyder på att verksamheternas önskemål på olika system inte skulle vara tillgodosedda. Standardisering är bra. Det minskar sårbarhet och det skapar rimliga förväntningar hos användarna.

12. Vem har helhetssyn på kapacitetsutnyttjandet avseende de olika systemen?

12.1 Iakttagelser

Det finns ingen som har som särskilt ansvar att ha helhetssyn på kapacitetsutnyttjandet. Det har varje nämnd och förvaltning ansvar för själva.

Det har under de senare åren gjorts genomgång av system där man faktiskt eliminerat olika system som gör samma saker. Ett exempel är tre enkätsystem som togs bort för några år sedan. Det planeras just nu en större genomgång av systemen i syfte att upptäcka om det finns system som gör samma sak.

Kapaciteten på servrar och övrig infrastrukturell utrustning övervakas av IT-avdelningen.

I övrigt går Varbergs kommun mot molnet i allt högre utsträckning vilket, beroende på vilka molntjänster man kommer att använda, minskar behovet av egen kapacitet.

12.2 Analys och bedömning

Ansvar för systemen är lokalt förutom för grundläggande kommungemensamma system. Det gjordes en genomgång för några år sedan och system togs bort. IT-avdelningen listar de system som man känner till och är med vid upphandlingar av system. Man har alltså bra koll på vilka system som finns så att det inte finns flera system som gör samma sak.

Den medvetna strävan mot molntjänster gör att den egna rent tekniska kapaciteten blir allt mindre viktig.

13. Hur fungerar konsultstödet till de olika systemen?

13.1 Iakttagelser

Konsultstöd till de stora systemen såsom ekonomi- och PA-system, Procapita etc. köps av leverantören till respektive system.

För kontorsprogramvaror får verksamheterna vid behov stöd ifrån antingen egna förvaltningsinterna stödpersoner, kundservice eller IT-avdelningen.

Kundservice står för funktionerna ”servicedesk” eller s.k. ”first line support”. För detta ändamål har tre personer från IT-avdelningen flyttats till Kundservice. Dessa personer arbetar även med fastighetsfrågor.

Inga synpunkter på att konsultstödet inte fungerar har framförts i våra intervjuer. Det förekommer dock irritation på väntetider på support från IT-avdelningen då och då (se avsnitt 8 ovan).

13.2 Analys och bedömning

Konsultstödet i stort förefaller vara adekvat och följer den ordning som förekommer i de flesta kommuner.

Det som kan diskuteras är om det är lämpligt att förlägga servicedesk och first line support utanför IT-avdelningen. De personer som arbetar med dessa frågor inom kundservice riskerar tappa i kompetens då de är frikopplade från IT-avdelningen och dessutom jobbar med andra frågor också. Vi rekommenderar en genomlysning av detta och fundera på om det verkligen är den bästa lösningen.

14. Hur är ansvaret för IT-säkerheten reglerat?

14.1 Iakttagelser

Begreppet IT-säkerhet håller på att fasas ut – inte bara i Varbergs kommun. Utvecklingen i omvärlden och Varbergs kommuns strävan att vara öppna mot medborgarna, näringsliv och andra utförare innebär såväl en bättre service men också större risker för attacker av olika slag. Därför talar man istället allt oftare om informationssäkerhetsarbete där traditionell IT-säkerhet bara utgör en del.

Det finns ett antal dokument i Varbergs kommun som reglerar ansvar och roller. Några är gamla (från år 2001) men det kommer fler och fler av nyare datum. Det är ett pågående arbete. Fullmäktige beslutade 2014-11-25 (Kf § 168) på förslag från kommunstyrelsen att anta policy för informationssäkerhet i Varbergs kommun, daterad den 2 oktober 2014. I beslutet ingår även att ge Kommunstyrelsen i uppdrag att utarbeta en strategi för genomförandet av policyn.

Det policydokument som fullmäktige tog beslut om anger ansvarsförhållanden enligt nedan:

- Kommunstyrelsen har det kommunövergripande ansvaret för informationssäkerheten vid Varbergs kommun. Kommunstyrelsen har ansvar för att initiera samordning av informationssäkerhet som berör flera verksamheten.
- Varje nämnd har ansvar för den egna verksamhetens informationssäkerhet.
- Varje chef inom Varbergs kommun ansvarar för att förutsättningar för informationssäkerheten inom det egna området finns och fungerar.
- Systemägare ansvarar för informationssäkerheten inom respektive verksamhetssystem.
- Medarbetare i Varbergs kommun har ett eget ansvar för informationssäkerheten avseende den information de själva hanterar.

Fullmäktiges beslut har lett till att IT-avdelningen nu leder och samordnar en revidering av kommunens hela ramverk för informationssäkerheten. Man följer SKL:s arbete nationellt.

Revidering av följande processer pågår:

- Informationssäkerhet Användare.
- Informationssäkerhet Drift.
- Informationssäkerhet Förvaltning.
- Riktlinjer för digital kommunikation. (För närvarande ligger för beslut: E-post, LYNC, m.m.)
- En inventering av samtliga system i kommunen pågår. Inventeringen ska ligga till grund för revision av informationsklassning.
- Processerna för Identitetshantering för att hantera SITHS-kort inom Socialtjänsten revideras varje år.

14.2 Analys och bedömning

Det finns en hög medvetenhet om vikten av informationssäkerhet (där IT-säkerhet ingår). Ansvaret har även tidigare varit tydligt men på förekommen anledning och den snabba utvecklingen inom informationsområdet som Varberg slagit in på har man sett att rutinerna och synsättet behöver ses över.

15. Vilka kontroller kopplat till IT-säkerhet genomförs?

15.1 Iakttagelser

Ansvar för IT-säkerhet, eller informationssäkerhet vilket är ett vidare begrepp, följer kommunens ordinarie roller och ansvarsstruktur. Nämnders och förvaltningars arbete med kontroller ska alltså återfinnas i de interna kontrollplanerna. Det förekommer sparsmakat och sporadiskt. En gång per år genomförs kontroll av legitimeringssystemet för hemtjänstpersonal. Denna genomförs av en utomstående organisation – Veritas.

Ansvar för den tekniska IT-säkerheten åligger IT-avdelningen. Den styrs av bl.a. standarder av olika slag, löpande övervakning av systemen, test och installation av säkerhetsuppgraderingar etc.

15.2 Analys och bedömning

Det finns en medvetenhet i organisationen om vikten av informationssäkerhet där bland annat IT-säkerheten ingår. Det pågår ett stort arbete med att uppdatera relevanta dokument. En policy för informationssäkerhet har beslutats av fullmäktige och tillämpningsanvisningar är under utarbetande. Dessutom finns numera en IT-styrgrupp där funktionsbeskrivning av denna är under utarbetande.

Vi rekommenderar att t.ex. styrgruppen ansvarar för att påminna om att det bör finnas relevanta och löpande kontroller av IT- och informationssäkerheten i de olika nämndernas interna kontrollplaner.

16. Är IT-säkerhetsplaner och annan dokumentation uppdaterade?

16.1 Iakttagelser

Generellt är inte IT-säkerhetsplaner uppdaterade.

Det som är uppdaterat är säkerhetsplaner rörande e-post och annan digital kommunikation.

Det finns en hög medvetenhet om bristerna och det pågår ett stort arbete med att uppdatera strategidokument, policydokument, tillämpningsanvisningar etc.

16.2 Analys och bedömning

Många styrande dokument är gamla och inte uppdaterade. Dock pågår ett genomgripande arbete som dessutom kommit långt.

17. Övrigt

17.1 Iakttagelser

Vi har *övergripande* kontrollerat den fysiska säkerheten genom att besöka det utrymme där serverhallen är lokaliserad. Lokalen finns hos Varbergs Energi AB.

Vi kan konstatera att servrar och backup-utrustning finns i samma lokal. Vi kan också konstatera att utrymmet ligger under markplan. I övrigt är utrymmet välstädat och god ordning råder.

17.2 Analys och bedömning

Vår bedömning är att kommunen lever med en risk. Det är inte bra att ha servrar och backup-utrustning i samma lokal om det t.ex. skulle utbryta brand eller uppstå översvämning.

MSB² har utarbetat rekommendationer kring hur den rent fysiska säkerheten kan ordnas. Detta beskrivs i dokumentet <https://www.msb.se/RibData/Filer/pdf/27280.pdf>.

Vi rekommenderar IT-avdelningen att göra en genomgång av den fysiska säkerheten i enlighet med MSB:s rekommendationer, därmed inte sagt att de behöver följas till punkt och pricka då de är extremt omfattande. En riskbedömning får ligga till grund för vilka åtgärder som ska vidtas.

KPMG, dag som ovan

Göran Andersson
Certifierad kommunal revisor

² Myndigheten för samhällsskydd och beredskap