Kristianstads kommun

KOMMUNREVISIONEN

2018-05-23

Kristianstads kommun
Kommunstyrelsen
Kommunfullmäktige

Granskning av styrning av IT- och informationssäkerhet

På uppdrag av de förtroendevalda revisorerna i Kristianstads kommun har PwC genomfört en en översiktlig granskning av kommunens styrning av IT- och informationssäkerhet. Granskningen omfattar kommunens IT-enhet (IT och serviceavdelningen) såväl som IT-verksamheten inom ett urval av kommunens förvaltningar. Syftet har varit att granska huruvida kommunstyrelsen säkerställt att kommunen arbetat systematiskt och ändamålsenligt med IT- och informationssäkerhet.

Vår övergripande bedömning är att kommunstyrelsen *till viss del* uppfyller revisionsfrågornas innebörd. IT-verksamheten anses vara organiserad enligt god praxis och det finns en genomgående kommunikation mellan IT-enheten, förvaltningarna och kommunledningen. Samtidigt finns det en medvetenhet inom IT-verksamheten att det krävs ett antal åtgärder för att närma sig en optimal IT- och informationssäkerhet.

Vi vill i sammanhanget lyfta fram följande synpunkter:

- Den främsta observationen är att kommunen bör införa IT-säkerhetsutbildningar. Detta skapar en kompetensgrund hos individen som kommunen kan dra nytta av vilket kan öka värdet för medborgare och anställda i kommunen.
- Det finns utvecklingspotential inom ett flertal områden; uppdatering av styrande dokument beträffande IT- och informationssäkerhet, övergripande strategisk IT-säkerhetsstyrning och samordning, processorientering och kvalitetssäkring inom IT-verksamheten och samarbetet med den nya informationssäkerhetssamordnaren.
- IT-verksamheten bör implementera utrustning för att detektera intrång så att risken för förlust av information, ekonomi och anseende minimeras.

Granskningsrapporten överlämnas till kommunstyrelsen med svar över vidtagna åtgärder före 2018-10-31 och till kommunfullmäktige för kännedom.

För revisorerna i Kristianstads kommun

Göran Sevebrant
Ordförande

Göran Wagermark
Vice ordförande

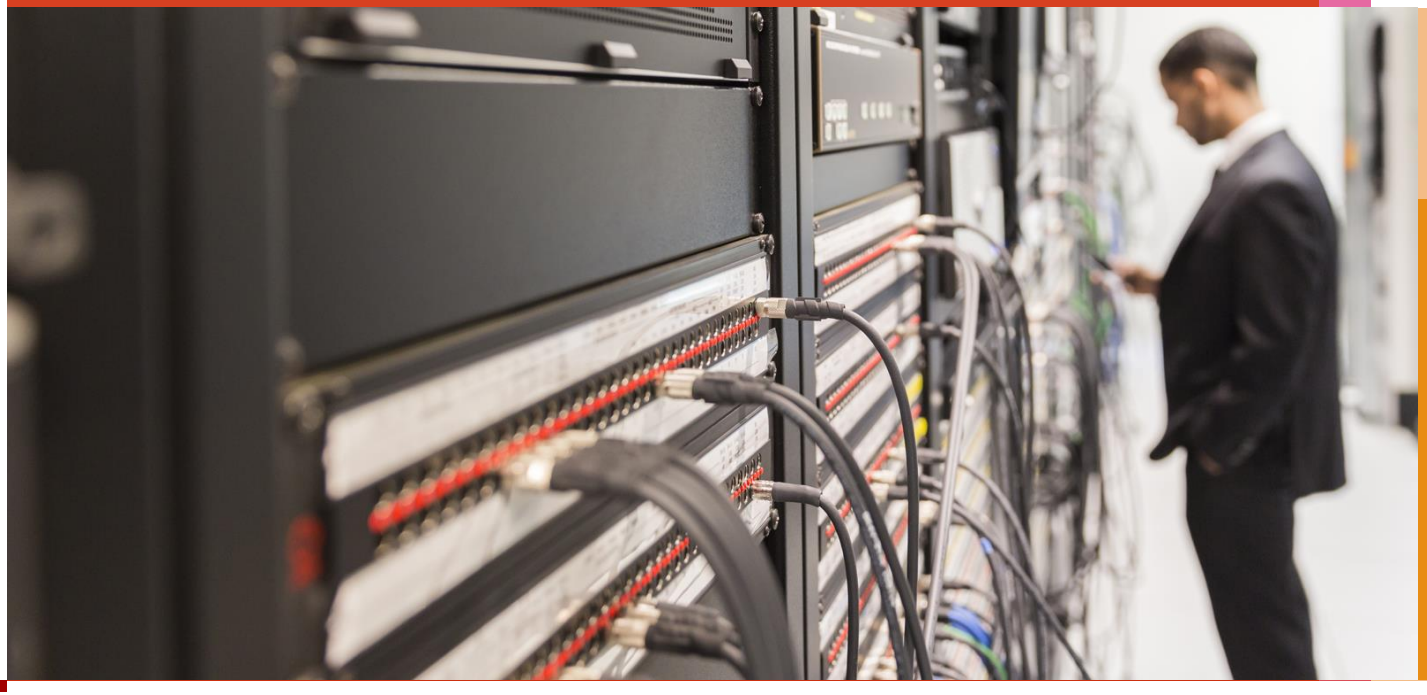
www.pwc.com/se

Kristianstads kommunrevisorer

Granskning: Styrning av IT- och informationssäkerhet

Kristianstads kommun

22 maj 2018



pwc

Contents

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Kristianstad kommun genomfört en översiktlig granskning av kommunens styrning av IT- och informationssäkerhet. Granskningen omfattar kommunens IT-avdelning såväl som IT-verksamheten inom ett urval av kommunens förvaltningar. Syftet har varit att granska huruvida kommunstyrelsen säkerställt att kommunen arbetat systematiskt och ändamålsenligt med IT- och informationssäkerhet.

- Vår övergripande bedömning är att kommunstyrelsen till viss del uppfyller revisionsfrågornas innebörd. IT-verksamheten anses vara organiserad enligt god praxis och det finns en genomgående kommunikation mellan IT-avdelningen, förvaltningarna och kommunledningen. Samtidigt finns det en medvetenhet inom IT-avdelningen att det krävs ett antal åtgärder för att närma sig en optimal IT- och informationssäkerhet.
- Den främsta observationen (och rekommendationen) är att kommunen bör införa informations- och IT-säkerhetsutbildningar . Detta skapar en kompetensgrund hos individen som kommunen kan dra nytta av vilket kan öka värdet för medborgare och anställda i kommunen.
- Det finns utvecklingspotential inom ett flertal områden; uppdatering av styrande dokument beträffande IT- och informationssäkerhet, övergripande strategisk IT-säkerhetsstyrning och samordning, processorientering och kvalitetssäkring inom IT-verksamheten och samarbetet med den nya informationssäkerhetssamordnaren.
- IT-verksamheten bör implementera utrustning för att detektera intrång så att risken för förlust av information, ekonomi och anseende minskas.

Sammanfattande bedömning

Uppfyllt
Delvis uppfyllt
Ej uppfyllt

Kontrollfråga		Observation	Bedömning
1	Finns roller och ansvar tydligt definierade för att säkerställa en effektiv IT- och informationssäkerhet?	Roll- och ansvarsbeskrivningar är bristfälligt reviderade för informationssäkerheten och bristfälligt definierade för IT-säkerheten.	
2	Finns det en väl optimerad och fungerande IT-organisation?	IT-verksamheten anses vara organiserad enligt god praxis med en tydlig ledning och styrning.	
3	Finns styrande dokument för informations- och IT-säkerhet och är de kontinuerligt reviderade?	Erforderliga styrande dokument relaterade till IT- och informationssäkerhet finns till viss del men är bristfälligt reviderade.	
4	Bedriver IT-organisationen ett aktivt IT-säkerhetsarbete?	Det bedrivs både ett reaktivt och proaktivt IT-säkerhetsarbete. Det proaktiva arbetet bör utvecklas mer tex med utrustning för att kunna detektera intrång.	
5	Arbetar IT-organisationen kontinuerligt och strukturerat med att hålla servrar, switchar, brandväggar etc. uppdaterade?	Ett kontinuerligt och strukturerat arbete kring uppdatering av kommunens IT-komponenter sker till viss del.	
6	Hur ser arbetet med kontrollsystem, så som t ex behörighetstilldelning, ut inom kommunen?	Relativt genomgående behörighetstilldelning dock bristfällig lösenordshantering.	
7	Finns det en tydlig målbild och definierad ambitionsnivå för arbetet med informationssäkerhet inom kommunen?	Bristfälligt definierad målbild och ambitionsnivå kring arbetet med informationssäkerhet.	
8	Utbildas och informeras medarbetarna inom kommunen löpande i frågor inom IT- och informationssäkerhet?	Bristfällig löpande utbildning av medarbetarna kring IT- och informationssäkerhet.	
9	Är IT-system och informationstillgångar omhändertagna i kommunens kris- och katastrofplan?	IT-system och informationstillgångar är till viss del inkluderade i kris- och katastrofplanen.	

Bakgrund och syfte

Inledning

PwC har på uppdrag av de förtroendevalda revisorerna i Kristianstads kommun genomfört en översiktlig granskning av kommunens IT-verksamhet med fokus på IT- och informationssäkerhet. Granskningen omfattar kommunens IT-avdelningen såväl som IT-verksamheten inom ett urval av kommunens förvaltningar.

Resultatet av granskningen presenteras i denna rapport.

Bakgrund

Kommunens revisorer har uppmärksammat att risker och hot från det digitala landskapet, s.k. cyberrisker, får ökande uppmärksamhet från företag och myndigheter. Främst orsakats av de senaste årens digitala utveckling med efterföljande exponering mot internet samt ökade användning av smartphones och andra bärbara enheter hos medarbetare. Ökad aktivitet bland kriminella och andra antagonistiska aktörer bidrar också starkt till den växande hotbilden.

Uppdraget innebar att inom ramen för revisionsarbetet inom kommunen genomföra en övergripande granskning av kommunens IT-verksamhet med fokus på IT- och informationssäkerhet för att förstå och analysera huruvida kommunen hanterar IT- och informationssäkerheten på lämpligt sätt. Granskningen, som kan liknas vid en förstudie, har översiktligt fokuserat på; styrning och ledning av IT, strategifrågor, teknologi och funktionalitet, projekt och processer, ekonomi och uppföljning, samt personalaspekter såsom kompetens och bredd.

Syfte

Syftet med granskningen är att klargöra vilka eventuella områden som kommunen behöver utveckla för att uppnå en balanserad IT- och informationssäkerhet.

Övergripande revisionsfrågor

Rapporten avser att belysa följande övergripande revisionsfrågor:

1. Har kommunstyrelsen säkerställt att organisationen arbetar systematiskt med IT-säkerhetsfrågor?
2. Har kommunstyrelsen säkerställt att man har en ändamålsenlig informationssäkerhet?

För att besvara de övergripande revisionsfrågorna, har nio kontrollmål definierats, se nästa sida.

Kontrollmål

Kontrollmål

1. Finns roller och ansvar tydligt definierade för att säkerställa en effektiv IT- och informationssäkerhet?
2. Finns det en väl optimerad och fungerande IT-organisation?
3. Finns styrande IT- och informationssäkerhetsdokument som organisationen behöver och är de kontinuerligt reviderade?
4. Bedriver IT-organisationen ett aktivt IT-säkerhetsarbete?
5. Arbetar IT-organisationen kontinuerligt och strukturerat med att hålla servrar, switchar, brandväggar etc. uppdaterade?
6. Hur ser arbetet med kontrollsystem, så som t ex behörighetstilldelning, ut inom kommunen?
7. Finns det en tydlig målbild och definierad ambitionsnivå för arbetet med informationssäkerhet inom kommunen?
8. Utbildas och informeras medarbetarna inom kommunen löpande i frågor inom IT- och informationssäkerhet?
9. Är IT-system och informationstillgångar omhändertagna i kommunens kris- och katastrofplan?

Metod och fokus

ITM-metoden bygger på fem områden som tillsammans representerar och sammanfattar IT-verksamheten inom en organisation. Metoden tar även hänsyn till så kallad ”good practice” inom IT generellt och jämför erhållet resultat med hur IT hanteras hos andra organisationer.

Resultatet bygger på intervjuer med identifierade nyckelpersoner i kommunen, (se intervjulista, bilaga 1) samt inläsning och genomgång av tillgänglig dokumentation och styrande dokument.

Grad av fokus

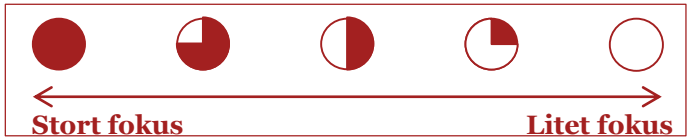
Informationssäkerhet
- Finns det en tydlig målbild och ansvarsfördelning för arbetet med informationssäkerhet? Hur arbetar man med att klassificera och kategorisera data samt känslig data?

Teknisk säkerhet
- Hur arbetar organisationen med att utveckla och hålla sig á jour med den tekniska säkerheten? Hur säkerställer man säkerheten hos externa system? Sker det löpande uppdatering av tekniska komponenter? Är driftorganisationen ordentligt rustad för att klara ett systemhaveri?

Drift
- Hur ser den dagliga driften ut? Hur ser processer, rutiner, dokumentation samt loggföring ut för driftorganisationen?

Organisation och Personal
- Hur ser rollfördelningen ut inom organisationen? Finns det en tydlig ansvarsfördelning? Är bemanningen i driftorganisationen samt service-desk tillräcklig och har dom rätt kompetens? Är organisationen strukturerad och uppbyggd för att inte hamna i beroende till nyckelpersoner?

Utveckling och framtid
- Hur arbetar organisationen med förändringsarbete, utveckling och målsättningar? Finns det planer och strategier för att leda organisationen framåt? Finns tydliga mål och visioner från ledningen uppsatta och dokumenterade?



Revisionell bedömning

Övergripande revisionsfrågor

1. ***Har kommunstyrelsen säkerställt att organisationen arbetar systematiskt med IT-säkerhetsfrågor?***
2. ***Har kommunstyrelsen säkerställt att man har en ändamålsenlig informationssäkerhet?***

Bedömning

Vår övergripande bedömning är att kommunstyrelsen till viss del uppfyller innebörden i revisionsfråga 1, dock anses revisionsfråga 2 ej vara uppfylld.

IT-verksamheten anses vara organiserad enligt god praxis och det finns en genomgående kommunikationen mellan IT-avdelningen, förvaltningarna och kommunledningen. Arbetet med IT-säkerhet i kommunen bedrivs till stor del reaktivt, vilket leder till att det saknas verktyg till att detektera och förhindra IT-incidenter. Samtidigt finns det en medvetenhet inom IT-verksamheten att det krävs ett antal åtgärder för att närma sig en optimal IT-säkerhet.

Informationssäkerhetsarbetet anses ej vara ändamålsenligt. Kommunen har uttalade arbetssätt kring klassning av system men detta sker idag med bristande genomförande. Kommunen saknar en roll som aktivt bedriver ett fullgott informationssäkerhetsarbete, dock noterades att kommunen har tillsatt en tjänst som informationssäkerhets- och krisberedsskapssamordnare.

- Den främsta observationen (och rekommendationen) gällande IT-säkerhetsfrågor är avsaknaden av detekteringsförmåga för att förhindra incidenter. IT-verksamheten bör implementera utrustning för att detektera intrång så att risken för förlust av information, ekonomi och anseende minskas.
- Den främsta observationen (och rekommendationen) gällande informationssäkerhet är avsaknaden av en aktiv informationssäkerhetssamordnare. Kommunen bör säkerställa att rollen som informationssäkerhetssamordnare besitter mandat att bedriva ett aktivt arbete.
- Den gemensamma observationen (och rekommendationen) är den bristande kunskapsnivån av IT- och informationssäkerhet bland kommunanställda. Kommunen bör aktivt säkerställa att utbildning sker och information kring området kommuniceras ut ändamålsenligt i syfte att höja den grundläggande kompetensnivån bland kommunanställda.
- Det finns utvecklingspotential inom ett flertal områden; uppdatering av styrande dokument beträffande IT- och informationssäkerhet, övergripande strategisk IT-säkerhetsstyrning och samordning och processorientering och kvalitetssäkring inom IT-verksamheten.

Detaljerad analys

Observationer och rekommendationer

Revisionsfråga 1 -
Finns roller och ansvar tydligt definierade för att säkerställa en effektiv IT- och informationssäkerhet?

Observationer

Granskningen visar att det generellt sett finns angivna roller inom kommunen med fokus på koncernstöd inom IT- och informationsverksamheten, men att roll- och arbetsbeskrivningar för informationssäkerheten inte är uppdaterade och att det antingen finns bristfälligt definierade roll- och arbetsbeskrivningar kopplade till IT-säkerhet eller saknas helt.

- Baserad på genomförd granskning noterades att rollbeskrivningar kopplade till IT-stöd finns dokumenterade men att datumstämpel och versionshantering i dokumentet saknas. Vidare noterades att rollerna ”Enhetschef IT Infrastruktur & Säkerhet” och ”Enhetschef IT Drift” är sammanförd till en roll benämnd ”Enhetschef, IT Drift & Infrastruktur”, något som inte är reviderat i ansvars- och rolldokumentet.
- Det saknas tydliga ansvarsbeskrivningar kring ansvaret av IT-säkerhet inom IT-avdelningen, vidare noterades att IT-säkerhetsfrågor inte uteslutande ligger hos en individ utan hanteras av flera personer i IT-avdelningen gemensamt. Det finns en risk att avsaknad av tydliga ansvarsbeskrivningar medför en osäkerhet och otydlighet kring vilka individer som ska driva IT-säkerhetsfrågor för delar inom IT-verksamheten.
- Det noterades att säkerhetschefen i nuläget innehar ansvaret för informationssäkerheten i kommunen och att resurser har anställts för att hantera operativa informationssäkerhetsfrågor. Dels har ett dataskyddsombud med ansvar för dataskyddsförordningen (GDPR) anställts och en nyanställd informationssäkerhets- och krisredskapssamordnare börjar i maj.
- Införandet av IT-handläggare/kundansvarig gentemot förvaltningarna i kombination av en transparent kommunikation från IT-verksamheten mot förvaltningarna har upplevts väldigt positivt utifrån genomförd granskning.
- I systemförvaltningsmodellen noterades att en roll ”Testare” finns övergripande beskriven som en acceptanstestare vid förändringar och uppgraderingar. Baserat på genomförd granskning noterades att ingen sådan roll finns i nuläget utan övergripande testning sker av driftteknikerna.
- Vidare noterades i systemförvaltningsdokumentet, att en roll betecknad ”Samordnande Systemförvaltare” finns betecknad. Utöver rollen som systemförvaltare är personen ansvarig att upprätta en gemensam förvaltningsplan för de ingående IT-systemen samt kalla till regelbundna möten med alla systemförvaltare. Baserat på genomförd granskning ligger ansvaret i nuläget hos enhetschefen för drift och infrastruktur, se även fråga 2.
- Enligt den strategiska planen för IT-avdelningen utgör IT-chefen tillsammans med IT-avdelningens enhetschefer ledningsgruppen. Under granskningen noterades att även IT-strategen och IT-projektledaren ingår i ledningsgruppen.

Revisionsfråga 1 -
Finns roller och ansvar tydligt definierade för att säkerställa en effektiv IT- och informationssäkerhet?

Rekommendationer

- Kommunen bör överväga att tillsätta en roll alternativt anpassa en nuvarande roll på övergripande nivå för att skapa tydliga ansvarsfördelningar och samordna samtliga frågor rörande IT-säkerhet. Rollen bör ha ansvaret att fånga upp verksamhetens IT-säkerhetsbehov och prioritera dessa i förhållande till kommunens och IT-avdelningens strategi, utveckling och vision. Se även fråga 2.
- Kommunen bör säkerställa att den nytillsatta informationssäkerhets- och krisberedskapssamordnaren tydligt inkluderas i kommunens målbild för informationssäkerhet. Vidare bör rollen tilldelas mandat för att effektivt verka som kravställande mot verksamheten.
- Kommunen bör uppdatera och revidera dokumentation kring ansvar, roll- och arbetsbeskrivningar för att tydliggöra roller och befogenheter för att säkerställa en effektiv IT- och informationssäkerhet.

Revisionsfråga 2 -
Finns det en väl optimerad och fungerande IT-organisation?

Observationer

Det framkommer i granskningen att kommunen har en IT-enhet som kan anses vara organiserad enligt god praxis. Samordningen inom IT-verksamheten och kommunikationen mellan IT-avdelningen, förvaltningarna och kommunledningen bedöms vara god. Det finns en tydlig styrning och ledning som utgår ifrån en övergripande strategisk agenda och ett operativt stöd etablerade delvis ur IT-processramverket och förvaltningsmodellen ITIL* och PM3**.

- Det framkommer att IT-verksamheten på senare år knutit åt sig värdefullt humankapital och gjort organisatoriska omstruktureringar vilket bidragit till en ändamålsenlig IT-verksamhet.
- Kommunen har en gemensam IT-avdelning med ett 50-tal anställda där majoriteten av drift och utveckling sker i egen regi. IT-chefen har på ledningsnivå ansvar för IT-frågor inom kommunen med tre underordnande enhetschefer inom Drift- och Infrastruktur, Teknik och Service. Tillsammans med IT-strategen och IT-projektledaren utgör dessa IT-ledningsgruppen.
- Det noterades att IT-verksamheten samarbetar med andra IT-verksamheter i närområdet där synergieffekter uppnås genom exempelvis samdrift av nätverk och gemensamma upphandlingar.
- Det noterades att kommunen till stor del utgått processorienterat vid utvecklingen av IT-verksamheten men att det ibland brister i rutinmässiga genomföranden.
- IT-verksamhetens generella arbete upplevs proaktivt, främst då organisationen genomgående känns tillräckligt resurstillsatt och kompetent. Dock betraktas IT-säkerhetsarbetet som främst reaktivt. Ett flertal respondenter belyser att ett mer reaktivt arbetssätt inom IT-säkerhet är önskat men att det saknas en tydlig samordnare med tydlig ansvar- och arbetsbeskrivning.

Rekommendationer

- Kommunen bör förankra arbetssätt, rutiner och processer utifrån IT-verksamhetens uppgift att utföra samhällsservice och kundnytta för att dra nytta av de synergier ITIL och PM3 möjliggör. Kommunen bör säkerställa att de rutiner och arbetssätt som utvecklats är anpassade utifrån verksamhetens behov och att de som innehar dessa roller har rätt kompetens och utbildningsnivå.
- Kommunen bör överväga att tillsätta en roll alternativt anpassa en nuvarande roll på övergripande nivå för att samordna samtliga frågor rörande IT-säkerhet. Rollen bör ha ansvaret att fånga upp verksamhetens IT-säkerhetsbehov och prioritera dessa i förhållande till kommunens och IT-verksamhetens strategi, utveckling och vision.
- För att applicera det proaktiva generella arbetssättet i IT-verksamheten på IT-säkerheten rekommenderas att ett förtydligande kring vem som har ansvaret att driva IT-säkerhetsarbetet görs. Rollen bör tilldelas mandat för att effektivt verka inom sitt område samt sitta i kommunens strategiska IT-råd. Se även fråga 4.
- Det noterades att enhetschefen för drift och infrastruktur är sammankallande för systemförvaltargruppen som hanterar de övergripande systemen i kommunen. Ifall enhetschefen ska kunna fokusera mer mot IT-säkerhet bör sammankallande bytas ut mot tilltänkta informationssäkerhetssamordnaren. Se även fråga 1.

*) **ITIL** – (Information Technology Infrastructure Library). ITIL är en samling principer för strukturerad hantering av IT-tjänster.
) **PM3 - Förvaltnings- och portföljsstyrningsmodell för effektiv hantering av IT-system och processer.

Revisionsfråga 3 -
Finns styrande IT- och informationssäkerhetsdokument som organisationen behöver och är de kontinuerligt reviderade?

Observationer

Informationssäkerhet

På övergripande nivå konstateras att det finns en del styrande dokument relaterade till informationssäkerhet, exempelvis ”*riktlinjer för informationssäkerhet”,* ”informationssäkerhetsinstruktion – *kontinuitet och drift*” samt ”informationssäkerhetsinstruktion – förvaltning”. Dock noterades att det finns skiftande kontinuitet i revideringen och att somliga har versionshantering:

- *Riktlinjerna för informationssäkerhet* (version 3) är reviderad 2014-09-03,
- *Kontinuitet- och driftdokumentet* är reviderat 2016-07-07, *Förvaltningsdokumentet* är reviderat 2011-02-22.

IT-säkerhet

Med utgångspunkt från de styrdokument som inhämtats är bedömningen att erforderliga styrande dokument för IT finns men att dessa är bristfälliga och generella avseende IT-säkerheten. Det noteras i rollbenämningen i systemförvaltningsmodellen att systemägares ansvar är att efterfölja rådande säkerhetspolicy. Ifall IT-säkerhetspolicyn saknar kontinuerlig revidering kan ogynnsamma händelser uppstå.

- Det noterades att det finns en kontinuitetsplan för servrar och system, nätverk samt telefoni härledd från en riskanalys men att instruktioner kring utförandet är generell och en rutin kring kontinuerlig revidering och versionshantering saknas.
- Det saknas en reviderad policy för IT-säkerhet.
- Det finns en IT-strategi med en gemensam strategisk agenda för IT på plats, dock utelämnas IT-säkerheten.
- Kommunen har tagit fram SLA-dokument (Service Level Agreement) med leverantörer vilket tydliggör leverans, tillgänglighet och kvalitet.
- Det noterades att riktlinjer på lösenordslängd om minst åtta tecken utan krav på specialtecken i IT-policyn är bristfälliga.

Rekommendationer:

- Kommunen bör uppdatera och revidera styrande dokument kring IT-säkerhet.
- Kommunen bör revidera styrande dokument kring informationssäkerhet och inkludera rollen informationssäkerhetssamordnare och DPO*.
- Kommunen bör höja kraven på lösenord inom kommunens IT-system och nätverk för att öka säkerheten. Förslagsvis till 12 tecken långt med krav på ett/flera specialtecken och lösenordsbyte var 180:e dag istället för 90:e dag.

*) **DPO** – Dataskyddsombud (Data Protection Officer) vars ansvar är att kontrollera att GDPR följs inom organisationen.

Revisionsfråga 4 -
Bedriver IT-organisationen ett aktivt säkerhetsarbete?

Observationer

Det framkommer i granskningen att det sker en kombination av pro- och reaktiva säkerhetsarbeten i IT-verksamheten där förbättringspotential finns inom en del områden. Kristianstads kommun har byggt en, såvitt det kan bedömas baserat på granskningen, modern och anpassningsbar infrastruktur för IT. Med hjälp av tredjepart utförde IT-verksamheten under året en sårbarhetsanalys på interna och externa IT-miljöer utifrån SANS 20 Critical Security Control *(SANS20)**. Vidare noterades att det inplementerats en MDM lösning för nya mobiltelefoner (Mobileiron), arbetet med 802.1x har kommit halvvägs samt att samdriften av Skåneost-nätet mellan 7-8 kommuner innehar redundans i Kristianstad och Hässleholm.

- Under året gjordes en sårbarhetsanalys (SANS20), ett penetrationstest samt en sårbarhetsscanning på kommunens IT-miljö. Resultatet ger en övergripande nulägesanalys över IT-strukturen som kan användas som vägledning och prioriteringsordning för säkerhetsarbetet i framtiden.
- Det tecknades ett avtal med tredje part att genomföra månatliga sårbarhetsscanningar på kommunens systemen för att upptäcka serverpatchar och dess sårbarheter.
- Det framkommer att IT-verksamheten utformat en säkerhetsgrupp bestående av en handfull representanter från IT-enheterna där huvudfokus ligger på tekniska frågeställningar inom IT-verksamheten. Enhetschefen för infrastruktur och drift är sammankallande kvartalsvis och har noterat en sjunkande mötesfrekvens på grund utav prioriteringssvårighet hos deltagarna.
- Det finns inga dokumenterade rutiner kring hanteringen av utrangerad IT-utrustning för att säkerställa att information inte hamnar i orätta händer.
- Det noterades att omvärldsbevakning kring IT-säkerhet görs ad-hoc.
- Det framkommer att arbetet med 802.1x är omfattande, men väl implementerat kommer riskerna kopplade till nätverkssäkerhet att minskas.

Rekommendationer

- IT-verksamheten bör höja verksamhetsfokus på säkerhetsgruppen där reaktiva arbetssätt främjas för att skydda information och system. Prioriteringsordning kan förslagsvis sättas utifrån resultatet från den utförda sårbarhetsanalysen.
- IT-verksamheten bör fortsätta genomföra en sårbarhetsanalys på årsbasis för att mäta baslinjen av IT-säkerhet på kommunen. Vidare kan ett systematiskt angreppssätt inbringa nya prioriteringsområden för kommunen då säkerhetsarbetet är komplext och föränderligt.
- Kommunen bör dokumentera upp sin rutin kring utrangerad IT-hårdvara för att säkerställa att ingen känslig information finns lagrad vid kassering.
- IT-verksamheten bör införa en konsekvent omvärldsbevakning. Viktiga iakttagelser summeras i nyhetsbrev internt till IT-verksamheten och ett övergripande till resterande anställda i syfte att öka medvetenheten kring IT-säkerhet.

*) **SANS20** – Riskbedömningsmetod för IT-säkerhet som hjälper organisationer att genomföra och utvärdera sina IT-säkerhetskontroller.
) **MDM – Programvara som används av en IT-avdelning för att övervaka, hantera och säkra medarbetarnas mobila enheter.
***) **802.1x** – Skapar en säkerhetsbarriär för intranät för att förhindra datorer som inte kan autentisera sig att ansluta sig till intranätet.

Revisionsfråga 5 -
Arbetar IT-organisationen kontinuerligt och strukturerat med att hålla servrar, switchar, brandväggar etc. uppdaterade?

Observationer

Granskningen visar att Kristianstads kommun strukturerat och kontinuerligt arbetar med uppdatering av drift- och nätverksutrustning såsom servrar, switchar och brandväggar. IT-arkitekternas arbete avser den övergripande arkitekturen för system och lösningar samt att omsätta verksamhets- och användarkrav till en realiserbar struktur. Till sin hjälp har de en handfull nätverks- och servertekniker. Den löpande utvecklingen sker internt och expertis kontrakteras vid behov. SLA-dokument har tagits fram för att tydliggöra leverans. Kravställning sker vid upphandling för att säkerställa att systemet klarar den senaste Microsoft-patchen och annan ny teknik.

- Kommunen har på senare tid genomfört ett omsorgsfullt arbete för att bygga upp en modern och anpassningsbar infrastruktur, exempelvis genom kravställning vid upphandlingar.
- Kommunen har under året avtalat om en månatlig sårbarhetsscanning mot IT-systemen innan varje Microsoft-patch tillfälle.
- Det noterades att nätverket har segmenterats upp på senare år och det pågår ett arbete med att utöka segmenteringen.
- IT-verksamheten håller sig väl uppdaterad med hårdvaruinköp, exempelvis används Cisco Prime för att hantera och administrera kommunens nätverk och Cisco Firepower, nästa generations brandvägg.
- På årsbasis revideras öppnade portar i brandväggen för att säkerställa riktighet.

Rekommendationer

- Kommunen bör införa tidsbegränsad öppning av temporära brandväggsportar för att minska risken för obehörigt intrång.
- Kommunen bör revidera brandväggsinställningar kvartals- eller halvårsvis för att säkerställa riktighet.
- IT-verksamheten bör fortsätta arbetet med att inkludera samtliga system i SCCM* så att automatiserad patchning kan genomföras.
- IT-verksamheten bör dokumentera samt strukturera upp ett arbetssätt kring patchning av IT-infrastruktur som exempelvis brandvägg, switch, router och accesspunkt.
- IT-verksamheten bör, ifall resurs och utrymme finns, även genomföra sårbarhetsscanningen omedelbart efter Microsoft-patchning för att få direkt feedback om sårbarheter.

*) **SCCM** – En systemhanteringsprogramvara för hantering av stora datorgrupper.

Revisionsfråga 6 -
Hur ser arbetet med kontrollsystem, så som t.ex. behörighetstilldelning, ut inom kommunen?

Observationer

Granskningen visar att det generellt finns ett arbete kring kontrollsystem på plats inom kommunen, men det saknas en robust process kring hanteringen av lösenord. IT-verksamheten har identifierat en rad behörighetstilldelningsproblem som kan uppstå då samma individ innehar olika roller inom kommunen.

- Det förekommer en bristande efterlevnad av rutin kring lösenordshanteringen och byte av lösenord i kommunen. Enligt informationssäkerhetsinstruktionen sker identifikation av användaren genom att *"e-post med det tillfälliga lösenordet skickas till närmaste chef som förmedlar det till användaren, alternativt att användaren kommer till IT-avdelningen personligen och identifierar sig"*. Baserat på vad som framkommit under granskningen ges medarbetare möjlighet att ringa in till ServiceDesk för lösenordsbyte genom att uppge personnummer.
- Det finns en god hantering av behörigheter styrd genom Active Directory (AD) som integrerar med Microsoft Forefront Identity Manager (FIM), Microsoft Identity Manager (MIM) och Exchange Server. FIM och MIM är identitets- och åtkomsthanteringssystem där person tilldelas behörighet och Exchange Server är kommunens mailtjänst.
- Det finns en dokumenterad behörighetsprocess som automatiskt hanterar ifall en person som är både anställd och förtroendevald inom kommunen väljer att avsluta sin anställning och är fortsatt förtroendevald. Processen säkerställer att personen har rätt behörighet i systemen. Däremot har personen kvar sitt mailkonto och kan därmed ha tillgång till känslig information som var tillgänglig då personen var anställd.
- Det finns en dokumenterad behörighetsprocess som hanterar ifall en person är anställd och elev samtidigt. Personen tilldelas två mailadresser, en per ändamål, samt får en specifik roll som begränsar tillgången i intranätet.
- Det finns en god hantering av generella servicekonton genom KeyPass. Dock noteras att personliga servicekonton har samma lösenordskrav som vanliga användarkonton. Det finns heller ingen krav att lösenorden ska särskiljas.

Rekommendationer

- IT-verksamheten bör skapa två e-mailadresser när en person är anställd och förtroendevald i syfte att särskilja känslig information från en förtroendevald som avslutar sin anställning.
- IT-verksamheten bör införa en regel som fastställer att IT-personal som handskas med servicekonton inte får ha samma lösenord som de har på sitt användarkonto.
- Kommunen bör öka lösenordslängden på användarkonton till 12 tecken då detta ökar säkerheten markant. Som komplement kan lösenordet bytas var 180:e dag istället för var 90:e.
- IT-avdelningen bör säkerställa att instruktion och rutin kring lösenordshantering överensstämmer.

Revisionsfråga 7 -
Finns det en tydlig målbild och definierad ambitionsnivå för arbetet med informationssäkerhet inom kommunen?

Observationer

- Det noterades att det finns riktlinjer kring arbetet med informationssäkerhet inom kommunen att dessa är föråldrade.
- Granskningen visar att det inte finns en fullständig målbild och definierad ambitionsnivå kring informationssäkerhet fastställd i kommunen. Vi noterar däremot en uttryckt önskan från IT-avdelningen att riktning bör ske mot ISO 27000 i det fortsatta arbetet med informationssäkerhet, något som däremot inte är fastställt av kommunstyrelsen.
- Det noterades att en informationssäkerhets- och krisberedskapssamordnare har anställts inom kommunen. Dock noterades att resursen är junior och det beräknas ta tid innan denna personen kommer in i sin roll.
- Det framkommer att klassning av system genomförs av systemförvaltarna men att det finns brister i genomförandet.

Rekommendationer

- Kommunen bör uppdatera och revidera riktlinjer kring informationssäkerhet.
- Kommunen bör säkerställa att ambitionsnivån kring informationssäkerhet klargörs från kommunstyrelse.
- Kommunen bör säkerställa att målbilden uppföljs, förslagsvis ett arbete som hamnar hos informationssäkerhetsanordnaren
- Kommunen bör säkerställa att klassning av system genomförs kontinuerligt, detta är systemförvaltarnas ansvar. Inför kontrollfunktion för att säkerställa att klassning har genomförts för samtliga system. Detta arbete bör vara informationssäkerhets-samordnarens ansvar.

Revisionsfråga 8 -
Utbildas och informeras medarbetarna inom kommunen löpande i frågor inom IT- och informationssäkerhet?

Observationer

Det framkommer i granskningen att det sker introduktionsutbildning av nyanställda men att försumbar tid läggs mot IT-området och följaktligen på frågor inom IT- och informationssäkerhet. Det finns inte heller någon strukturerad plan eller strategi för vilken typ av utbildning som ska erbjudas.

- Bristande utbildning kan leda till att IT-system och applikationer inte används på rätt sätt. Ett förebyggande arbetssätt kan minska skada både ekonomiskt och anseendemässigt.
- Det framkommer i granskningen att det finns en avsaknad av utbildning avseende IT- och informationssäkerhet.
- Det noterades att personalen inom IT-avdelningen erbjuds utbildning. Utbildningen är främst inriktad mot enskild persons vidareutveckling och efterfrågan inom verksamhetsområdet, här inkluderas ofta IT-säkerhet för det specifika utbildningsområdet.
- Däremot finns en avsaknad av generell informations- och IT säkerhetsutbildning kring hot och risker riktade mot organisationen inom både IT-avdelningen och ute hos förvaltningarna.
- Baserat på vad som framkommit i granskningen bedöms medarbetarna inom IT-avdelningen var för sig ha en relevant och god kompetens inom IT- och informationssäkerhet. Det noteras att den fördelning av kompetenser som IT-avdelningen har bidrar till en generellt god kompetensnivå för avdelningen som sådan.
- Det noterades att systemförvaltarna får stöttning på olika plan inom IT-säkerhet från IT-avdelningen. Baserat på vad som framkommit menar systemförvaltarna att stödet främst kommer från att förvaltningarna har en kundansvarig på IT-avdelningen, det finns ett förvaltningsöverskridande IT-råd, och att det finns en god kommunikation mellan IT-avdelningen och förvaltningarna.
- Det framkommer att medarbetare inom IT-verksamheten ges möjlighet att besöka exempelvis mässor och event hos leverantörer vilket ökar medarbetarens IT-kompetens och följaktligen IT- och informationssäkerhet.

Rekommendationer

- Kommunen bör implementera en plan och långsiktig strategi kring kompetensutveckling inom IT- och informationssäkerhet som helhet. Detta bör kopplas till kommunens vision och övergripande strategi. Kompetensen bör säkerställas utifrån kommunens behov. Att kompetensutveckla personalen inom IT- och informationssäkerhet är en viktig del i att säkerställa att kommunen kan dra nytta av den snabba utveckling som sker inom digitalisering och IT och hantera den på rätt sätt med hänsyn till de framväxande hoten i det digitala landskapet.
- Kommunen bör öka sin informationsspridning av aktuella IT- och informationssäkerhetshot för att öka grundförståelsen.

Revisionsfråga 9 -
Är IT-system och informationstillgångar omhändertagna i kommunens kris- och katastrofplan?

Observationer

I granskningen noterades att IT-system och informationstillgångar finns omhändertagna i kommunens kris- och katastrofplan. Dock noterades att det finns utrymme för förbättring.

- Det framkommer att utvärdering av genomförd kris- och katastrofövning görs men att processen ej är dokumenterad.

Rekommendationer

- Kommunen bör simulera ett IT-haveri för att säkerställa att processer, rutiner och prioriteringsordning är på plats för att få upp IT-systemet och i största möjliga mån undvika väsentlig påverkan vid allvarliga händelser.

Avslutning

2018-05-15

Niklas Ljung

Uppdragsledare

Projektledare

Bilaga

Bilaga 1, Intervjulista

Namn	Roll	Verksamhet
Martin Ranstorp	IT-chef	IT-avdelningen
Jörgen Hermansson	Enhetschef, IT Teknik	IT-avdelningen
Pierre Andersson	IT-arkitekt	IT-avdelningen
Andreas Poppius	Säkerhetschef	Räddningstjänsten
Jimmy Nilsson	Enhetschef, IT Service	IT-avdelningen
Jonas Månsson	IT-drifttekniker	IT-avdelningen
Linda Söderberg	Enhetschef, IT Drift & Infrastruktur	IT-avdelningen
Angelica Andersson	Systemförvaltare	Barn- och utbildningsförvaltningen
Pia Friberg	Systemförvaltare	Arbete- och välfärdsförvaltningen

© 2018 PricewaterhouseCoopers i Sverige AB. Att mångfaldiga innehållet helt eller delvis är förbjudet enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk. Förbudet gäller varje form av mångfaldigande genom tryckning, kopiering etc.