Mölndals stad

Datum
2011-04-13

Vår beteckning

Ert datum

Er beteckning

Revisorerna

Kommunfullmäktige
Kommunstyrelsen
Serviceutskottet

Granskning av IT-säkerhet

Revisorerna har uppdragit åt KPMG att granska kommunens arbete med IT-säkerhet.

Syftet med granskningen är att på en övergripande nivå belysa struktur och ändamålsenlighet avseende IT-säkerhetsarbetet i Mölndals stad.

Rapporten visar på svagheter i arbetet med informationssäkerhet. Det är kommunstyrelsen som ytterst ansvarar för informationssäkerheten kommunövergripande.

Kommunrevisionen rekommenderar att kommunstyrelsen:
- ser över informationssäkerhetsarbetet, med anledning av de områden i rapporten som berörs och att det behöver finnas en medvetenhet om hot och med riskanalyser som verktyg.
- tilldelar en roll för just informationssäkerhetsansvaret för att kunna koordinera verksamhetens kravställning gentemot bland annat centrala IT-enheten.
- ser över att införa ett ledningssystem för informationssäkerhet, som berörs i ISO 27001:annex A

Marcus Broman

Besöksadress
Stadshuset
Göteborgsvägen 11-17

Postadress
Mölndals stad
431 82 Mölndal

Telefon/fax
031-315 12 64
031-315 10 09 (fax)

E-post/webb
karolina.engman@molndal.se
www.molndal.se

KPMG

cutting through complexity™

Mölndals Stad
Revisorerna
Granskning av IT-säkerhet

2 mars 2011

Innehållsförteckning

Kontaktpersoner vid KPMG:

Annika Hessler
Senior Manager, KPMG
Göteborg
Tel: 031 – 61 47 21
annika.hessler@kpmg.se

Johnny Berggren
Senior Associate, KPMG
Göteborg
Tel: 031 – 61 48 58
johnny.berggren@kpmg.se

Inledning

Bakgrund

Revisorerna gör varje år en risk- och väsentlighetsanalys för att se var i verksamheterna de största riskerna finns. Riskerna inom stadens IT-hantering bedöms som stora, både ekonomiska risker, effektivitet och säkerhet.

Syfte och revisionsfrågor

Syftet med granskningen är att på en övergripande nivå belysa struktur och ändamålsenlighet på IT-säkerhetsarbetet i Mölndals stad.

I granskningen har följande revisionsfrågor belysts:

- Har staden en tillräcklig och fastställd IT-säkerhetspolicy?
- Hur står sig stadens IT-säkerhetspolicy i jämförelse med tillämpliga delar av ISO 27002:2005 (Informationsteknik – Säkerhetstekniker – Riktlinjer för styrning av informationssäkerhet)?
- Hur ser ansvar och roller för IT-säkerhetsfrågor ut inom stadens centrala IT-avdelning?
- Vilka rutiner ligger till grund för uppföljning och uppdatering av den fastställda IT-säkerhetspolicyn och övrig säkerhetsrelaterad information?

Omfattning och avgränsning

Granskningen har omfattat stadens serviceförvaltning och dess lokala IT-avdelning. Granskningen har därmed inte omfattat de andra förvaltningarna Mölndals stad.

Metod

Granskningen har inriktats på studier och analys av väsentliga styrande dokument och instruktioner (främst antagen IT-säkerhetspolicy) samt genomförande av strukturerade intervjuer med IT-chef, driftschef samt IT-strateg inom den centrala IT-avdelningen samt kommunens säkerhetschef.

Förutsättningar för vårt uppdrag

KPMG AB (härefter kallat KPMG) har genomfört uppdraget i enlighet med granskningsplan daterad 2011-02-01. Informationsinsamlingsperioden avslutades den 18:e februari 2011 och rapporten innehåller information sammanställt upp till och med den dagen. Omständigheter eller tillkommande information efter den 18:e februari 2011 innebär därmed inte ett krav på KPMG att rätta vår framlagda rapport.

KPMGs primära källa för informationsinsamling har varit dokumentstudier och intervjuer med berörd personal. KPMG kan av naturliga skäl inte ta ansvar för information som inte KPMG har skapat eller ansvarar för. Detta ansvar bär originalförfattaren eller källan till informationen. Förutom en professionell rimlighetsbedömning har inte KPMG inom ramen för detta uppdrag verifierat validiteten eller sanningshalten av informationen erhållen under intervjuerna (det vill säga vi har inte genomfört en faktakontroll av informationen så som systemkontroller eller stickprov av informationen). Vi har, så långt som det är möjligt, bedömt om informationen oss tillhandahållen under intervjuerna är korrekt och i enighet med granskningsplanen.

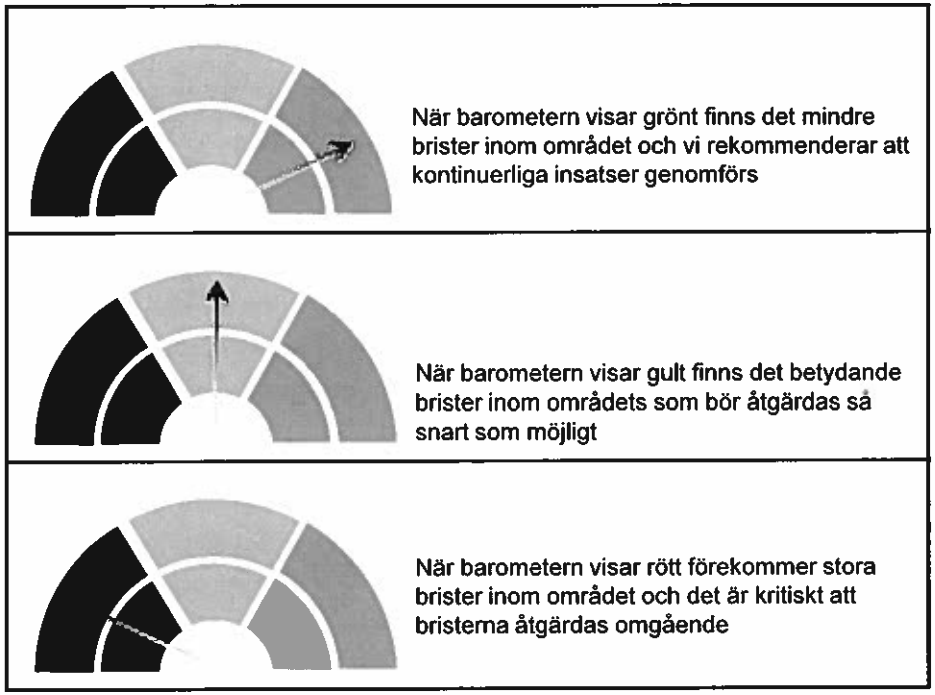
Denna rapport refererar till en "granskning" vilken enbart indikerar att vi har genomfört någon form av analytisk bedömning av den givna informationen för att komma fram till slutsatserna i denna rapport. KPMG har av dessa skäl inte accepterat något ansvar för den underliggande data och därmed att slutsatserna är korrekta.

Kriterier för bedömning

Kriterier för bedömning

Den internationella standarden ISO 27002:2005 har använts som grund för bedömning. De delar i standarden som främst legat till grund för bedömningen är avsnitt 5 – Säkerhetspolicy, avsnitt 6 – Organisation av informationssäkerheten, avsnitt 10 – Styrning av kommunikation och drift samt avsnitt 14 – Kontinuitetsplanering för verksamheter.

Utöver dessa avsnitt har delar av andra avsnitt används där så är tillämpligt. Samtliga avsnitt har grupperats ihop i denna rapport för översiktens skull och värderingen har skett genom en tregradig skala enligt nedan.



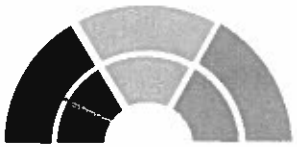
När barometern visar grönt finns det mindre brister inom området och vi rekommenderar att kontinuerliga insatser genomförs

När barometern visar gult finns det betydande brister inom områdets som bör åtgärdas så snart som möjligt

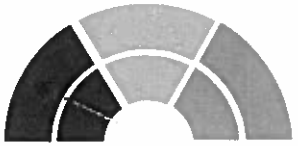
När barometern visar rött förekommer stora brister inom området och det är kritiskt att bristerna åtgärdas omgående

Sammanfattande slutsatser och rekommendationer

IT-säkerhetspolicy, riskanalys och ansvarsfördelning

IT-säkerhetspolicy	**Sammanfattande slutsats** ■ Den IT-säkerhetspolicy som antogs av kommunfullmäktige under 2006 har ej uppdaterats ■ Den framtagna IT-säkerhetspolicyn är inte kopplad till ett ramverk för säkerhetsåtgärder, struktur samt riskbedömning ■ IT-säkerhetspolicyn är framtagen av centrala IT-avdelningen tillsammans med extern part men ingen oberoende granskning av policyn är genomförd ■ Utöver IT-säkerhetspolicyn finns det inga centrala uttalade krav gällande informationssäkerhet **Rekommendationer** Vi rekommenderar att kommunen utarbetar en informationssäkerhetspolicy i linje med ISO 27002:2005, där IT-säkerhet utgör en del av policyn. Informationssäkerhetspolicyn bör vara initierad av kommunledningen för att tydliggöra kraven på säkerhet inom kommunen, uttrycka ledningens engagemang samt visa organisationens angreppssätt gällande styrning av informationssäkerhet.	**Gradering** 
Riskanalys	**Sammanfattande slutsats** ■ En sårbarhetsanalys i enlighet med SFS 2006:544 är genomförd 2009, med två identifierade IT-säkerhetsrisker gällande placering av backup samt otillräckliga system för att snabbt återskapa totalhavererade system ■ Någon heltäckande riskanalys har inte genomförts inom kommunen ■ Ett ramverk för riskbedömning finns inte framtaget **Rekommendationer** Vi rekommenderar att en riskbedömning utförs för att identifiera de hot som föreligger mot kommunen samt skattar storleken hos relaterade risker i linje med ISO 27002:2005. Vi rekommenderar vidare att säkerhetsåtgärder för identifierade risker genomförs för att minska risker till en av kommunen acceptabel nivå.	
Ansvarsfördelning	**Sammanfattande slutsats** ■ En övergripande ansvarfördelning finns inkluderat i IT-säkerhetspolicyn och IT-kontaktpersoner är utsedda inom de olika förvaltningarna ■ Det finns brister i kommunikationen mellan förvaltningarna och den centrala IT-avdelningen ■ Inköp av IT-utrusning, samt i vissa fall även IT-system, sker, i viss utsträckning utan den centrala IT-avdelningens kännedom **Rekommendationer** Vi rekommenderar att kommunen ser över ansvarsfördelningen i IT-säkerhetspolicyn och utarbetar tydliga instruktioner och rutiner per förvaltning.	

Sekretess, rutiner och efterlevnad

Sekretess	**Sammanfattande slutsats** ■ De leverantörer och konsulter som får tillgång till sekretessbelagd information är reglerade enligt sekretessavtal ■ De rutiner som finns för att säkerställa att nyanställda får ta del av information om de bestämmelser i sekretesslagen, som respektive tjänst berörs av, är bristande **Rekommendationer** Vi rekommenderar kommunen att se över de rutiner som finns gällande behandling och tillgång till sekretessbelagd information. Kommunen bör vidare genomföra en analys över risken för informationsläckage/otillbörlig tillgång till sekretessbelagd information .	Gradering 
Rutiner och efterlevnad	**Sammanfattande slutsats** ■ Det finns ingen utarbetad kontinuitetsplan för kommunen ■ Få fastställda skriftliga rutiner är framtagna inom den centrala IT-avdelningen ■ Kryptering av data sker i Procapita, för övriga databaser och hårddiskar sker ingen kryptering av data ■ Kommunen har inte etablerat rutiner för att kontrollera de risker som ny teknik har medfört **Rekommendationer** Vi rekommenderar att kommunen utarbetar en kontinuitetsplan med fokus på den verksamhet som bedrivs samt med utgångspunkt från en riskanalys. Ett samlat ramverk för kontinuitetsplanering bör finnas för att säkerhetsställa att alla planer är konsekventa, att informationssäkerhetskraven behandlas konsekvent samt för att fastställa prioriteringar gällande test och underhåll av system. Vi rekommenderar även att kommunen ser över riskerna i dagens IT-miljö för att överväga kryptering av data av känslig eller kritisk natur. Om en krypteringslösning implementeras bör en krypteringspolicy utarbetas för att klargöra ansvar, minimera risker och för att undvika olämplig eller felaktig användning. Vår rekommendation gällande användandet av ny teknik inom kommunen är att utföra en riskanalys gällande bärbar media, smartphones samt molnteknik för att förhindra att sekretessbelags information medförs utan kommunens godkännande.	

Riktlinjer enligt den svenska standarden ISO 27002:2005

En informations-säkerhetspolicy bör omfatta följande enligt ISO 27002:2005:

- **Definition av IT-säkerhet**
- **Uttalande från ledningen om dess avsikt som ger stöd åt IT-säkerhet**
- **Ramverk för beslut gällande IT-säkerhet**
- **Kort förklaring av IT-säkerhetspolicy, principer och standarder**
- **Definition av allmänna och särskild ansvar**
- **Hänvisning till övrig dokumentation**

Riskbedömning bör utföras periodiskt.

Varje identifierad risk behöver ett riskbehandlings-beslut.

Enligt ISO 27002:2005 bör det inom verksamheten (kommunen) finnas en informationssäkerhetspolicy vilken styr den totala informationssäkerheten i verksamheten och skall vara fastställd och godkänd av verksamhetens ledning (kommunledningen). Informationssäkerhetspolicyn bör innehålla ett avsnitt gällande IT-säkerhet som övergripande specificerar vilken IT-utrustning som skall användas och hur för att uppnå de fastställda målen i informationssäkerhetspolicyn. Den centrala IT-avdelningen bör stå för verkställandet av de av kommunstyrelsen uppsatta kraven, i enlighet med den fastställda informationssäkerhetspolicyn.

Följande punkter bör inkluderas i en informationssäkerhetspolicy;

- Definition av IT-säkerhet, dess övergripande mål och omfattning samt vikten av säkerhet
- Uttalande från ledningen om dess avsikt som ger stöd åt IT-säkerhetens mål och principer i linje med organisationens strategi och mål
- Ett ramverk för beslut om åtgärdsmål och säkerhetsåtgärder inklusive strukturen för riskbedömning och riskhantering
- Kort förklaring av IT-säkerhetspolicy, principer, standarder och efterlevnadskrav av särskild betydelse för organisationen, innefattande:
  - a) Överensstämmelser med lagar, förordningar och avtalskrav
  - b) Krav på medvetenhet, utbildning samt praktiskt övning gällande säkerhet
  - c) Kontinuitetsplanering
  - d) Konsekvenser vid avvikelser från IT-säkerhetspolicy
- En definition av allmänna och särskilda ansvar rörande styrning av IT-säkerhet, inklusive rapportering av IT-säkerhetsincidenter
- Hänvisning till dokumentation som kan stödja policyn, t.ex. mera detaljerade säkerhetspolicys och rutiner för specifika informationssystem eller säkerhetsregler användare bör efterleva.

Policyn bör kommuniceras genom hela organisationen till användare i en form som är relevant, tillgänglig och begriplig för den avsedda läsaren.

Riskbedömning bör utföras periodiskt för att behandla de ständiga förändringar som sker samt för att återspegla säkerhetskraven och det aktuella riskläget. En riskbedömning kan omfatta hela organisationen, delar av den, enskilda system eller tjänster där en riskbedömning är till hjälp och är realistiskt.

Varje risk som identifieras behöver ett riskbehandlingsbeslut som kan innefatta lämpliga säkerhetsåtgärder, medvetet acceptera risker, undvika risker och aktiviteter som orsakar att risker uppkommer samt överföring av risker till andra parter såsom försäkringsgivare eller leverantörer.

IT-säkerhetspolicy

Väsentliga iakttagelser och rekommendationer

Den nuvarande IT-säkerhetspolicyn antogs den 18 januari 2006 och har inte uppdaterats sedan antagandet.

Policyn är framtagen av den centrala IT-avdelningen tillsammans med extern part men har inte granskats av en oberoende part.

Det finns inga centrala krav gällande informations-säkerhet utöver IT-säkerhetspolicyn.

Väsentliga iakttagelser

Den nuvarande policyn antogs av kommunfullmäktige den 18 januari 2006 och framställdes av centrala IT-avdelningen tillsammans med en extern konsult. Dock har ingen oberoende part granskat policyn sedan införandet och den har ej uppdaterats sedan antagandet. Vid granskning av den nuvarande policyn har det framkommit att den saknar väsentliga delar i jämförelse med vad som rekommenderas i enlighet med ISO 27002:2005. Det finns i policyn inget avsnitt med ett uttalande från ledningen om dess avsikt, som ger stöd åt IT-säkerhetens mål och principer som dessutom skall vara i linje med kommunens mål och strategi.

Vidare innehåller policyn inte heller någon koppling till ett ramverk som behandlar säkerhetsåtgärder, struktur för riskbedömning samt riskhantering. Enligt de intervjuer vi genomfört har det framkommit att det inte finns något ramverk för riskhantering.

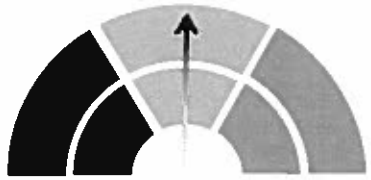
Utöver IT-säkerhetspolicyn finns det inga centrala uttalade krav gällande informationssäkerhet.

Rekommendationer

Vi rekommenderar att kommunen utarbetar en informationssäkerhetspolicy, i linje med ISO 27002:2005, där IT-säkerhet utgör en del av policyn. Informationssäkerhetspolicyn bör vara initierad av kommunledningen för att tydliggöra kraven på säkerhet inom kommunen, uttrycka ledningens engagemang samt visa organisationens angreppssätt gällande styrning av informationssäkerhet. Policyn bör även granskas och utvecklas löpande och om betydande förändringar genomförs.

Det är kommunens ledning som fastställer de krav kommunens informationssäkerhet skall följa och således är det kommunledningen som bör formulera och godkänna informationssäkerhetspolicyn, granska verkan av införandet av en sådan policy och dess löpande uppföljning samt tillgodose behovet av resurser för informationssäkerhet.

Gradering



När barometern visar gult finns det betydande brister inom området som bör åtgärdas så snart som möjligt

Riskanalys

Väsentliga iakttagelser och rekommendationer

Det finns inget ramverk för riskbedömning framtaget och någon riskanalys har i dagsläget inte genomförts.

En sårbarhetsanalys har genomförts 2009 där två IT-säkerhetsrisker identifierades.

Väsentliga iakttagelser

Under 2009 genomfördes en sårbarhetsanalys i enlighet med SFS 2006:544, Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Enligt kommunens säkerhetschef framkom det två risker inom IT-säkerhetsområdet som ej levde upp till kraven utifrån SFS 2006:544. De identifierade riskerna var placeringen av backup media (som tidigare skedde i samma lokaler som övrig lagringsmedia) samt att det ej fanns ett tillförlitligt system för att snabbt återskapa data efter ett totalhaveri.

Det finns inget ramverk för riskbedömning framtaget inom kommunen. Enligt såväl IT-chefen som säkerhetschefen finns det i dagsläget inget beslut om att införa ett sådant ramverk i kommun. Det görs informella riskbedömningar inom den centrala IT-avdelningen ,men inga löpande analyser genomförs.

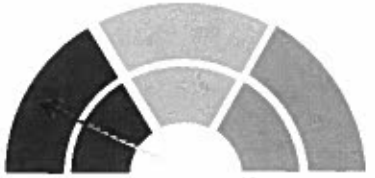
Ingen övergripande riskanalys har gjorts i kommunen utan endast en sårbarhetsanalys. Vidare görs inga löpande dokumenterade riskanalyser. Diskussioner angående IT-relaterade risker förs löpande på möten inom IT-avdelningen samt hur dessa skall hanteras, dock sker detta informellt.

Rekommendationer

Vi rekommenderar att riskanalys och riskbedömning gällande informationssäkerhet periodiskt genomförs för att identifiera de hot som föreligger mot kommunen samt skattar storleken hos relaterade risker, i linje med ISO 27002:2005.

Vi rekommenderar vidare att säkerhetsåtgärder för identifierade risker genomförs för att minska risker till en, av kommunledningen, accepterad nivå med hänsyn tagen till krav och restriktioner enligt gällande lagstiftning, organisationens mål samt kommunens krav och restriktioner.

Gradering



När barometern visar rött förekommer stora brister inom området och det är kritiskt att bristerna åtgärdas omgående

Riktlinjer enligt den svenska standarden ISO 27002:2005

Ansvar för IT-säkerhet bör överensstämma med IT-säkerhetspolicyn.

Ansvar bör vara tydligt definierat och omfatta samverkan.

Metoder för att hantera IT-säkerhet bör granskas av oberoende part.

Tilldelning av ansvar för IT-säkerhet bör vara förenligt med vad som föreskrivits i den fastställda IT-säkerhetspolicyn. Ansvar för skydd av enskilda tillgångar och för att utföra särskilda säkerhetsprocesser, exempelvis kontinuitetsplanering, bör anges tydligt.

Vidare bör:

- Tillgångar och säkerhetsrutiner inom varje separat system identifieras och förtydligas
- Ansvarig enhet utses för varje tillgång och säkerhetsrutin samt en detaljerad beskrivning dokumenteras
- Behörighetsnivåer tydligt dokumenteras

Samordning av IT-säkerhet bör omfatta samverkan och samarbete mellan chefer, användare, systemerare och säkerhetspersonal samt även HR-personal.

Kommunens metoder för att hantera IT-säkerhet och ansvarfördelning bör, i enlighet med ISO 27002:2005, granskas av en oberoende part med planerade mellanrum eller när det inträffar väsentliga förändringar som berör tillämpligheten av säkerheten.

Ansvarfördelning

Väsentliga iakttagelser och rekommendationer

En övergripande ansvarsfördelning finns definierad i IT-säkerhetspolicyn.

IT-kontaktpersoner finns etablerade inom de olika förvaltningarna.

Inköp av IT-utrustning samt i vissa fall system, sker i viss utsträckning utan den centrala IT-avdelningens inflytande.

Väsentliga iakttagelser

Det finns inom varje förvaltning utsedda IT-kontaktpersoner, vars uppgift är att vara en länk mellan den centrala IT-avdelningen och de olika förvaltningarna. Vid granskningen har det framkommit att formerna för samarbetet inte är klargjorda. Det finns inget IT-råd inom kommunen, men det finns en nyinrättad gruppering kallad Gammagruppen, vars uppgift är att behandla strategiska IT-frågor. Gruppen utgörs av tre förvaltningschefer och stadens utvecklingschef. IT-chefen är adjungerande. Gammagruppen är det översta beredningsorganet för IT-frågor och ansvarar för att ett kommunledningsperspektiv tas tillvara i beslut som rör IT.

Kommunen har anställt en IT-strateg som börjar sin tjänst den 1 april 2011. IT-strategens uppgifter kommer bland annat att omfatta behandling av strategiska IT-frågor och ansvar för att ett kommunledningsperspektiv tas tillvara rörande IT-frågor.

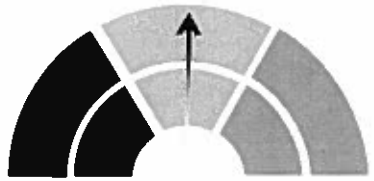
Det finns i IT-säkerhetspolicyn en övergripande beskrivning över ansvarsområden inom IT-säkerhet för alla nivåer från kommunfullmäktige och kommunstyrelse till den enskilde slutanvändaren. Vidare finns det ett klart och uttalat ansvar för den operativa IT-säkerheten inom den centrala IT-avdelningen, dock inget som är formellt dokumenterat.

Enligt Mölndals stads IT-säkerhetsregler för användare i Mölndals stad ,vilken antogs 2006, initierar systemägaren behovet av IT-stöd och beslutar om nyanskaffning. Dock har den centrala IT-avdelningen ansvar för IT-infrastrukturen samt ett övergripande ansvar för systemens tekniska funktion samt ansvarar och genomför beställning och inköp av IT-utrustning i enlighet med fastlagd standard. Det har skett att förvaltningar köper in såväl IT-system som datorer lokalt, som inte tekniskt godkänts av den centrala IT-avdelningen och det har hänt att IT-avdelningen kontaktas först i slutet av en systemupphandling. Ansvarsfördelningen medför risk att IT-system och IT-utrustning införs som inte harmoniserar med rådande IT-miljö.

Rekommendationer

Vi rekommenderar att kommunen ser över ansvarsfördelningen och utarbetar tydliga riktlinjer och rutiner för varje ansvarsområde inom IT-säkerheten. Vi rekommenderar vidare att ansvarsfrågan gällande inköp av IT-system och IT-utrustning i de olika förvaltningarna tydligt definieras för att undvika att inköp sker som ej harmoniserar med kommunens IT-miljö.

Gradering



När barometern visar gult finns det betydande brister inom området som bör åtgärdas så snart som möjligt

Sekretess

Väsentliga iakttagelser och rekommendationer

Rutiner gällande sekretess och vem som har tillgång till sekretessbelagd information är i nuläget otydliga.

Leverantörer och konsulter som får tillgång till personuppgifter är reglerade med sekretessavtal.

Väsentliga iakttagelser

Vid nyanställning är det närmaste chefs ansvar att säkerställa att arbetstagaren är införstådd i de säkerhetsregler gällande IT som finns samt den eventuella sekretess som tjänsten kräver. Det finns en ruta på anställningsavtalet, vilken kryssas i för att påvisa att den anställde tagit del av de bestämmelser i sekretesslagen som berörs. Det är i dagsläget oklart hur kontroll av detta sker. Enligt IT-chefen kännedom finns det i nuläget inga bra rutiner för de som har tillgång till sekretessbelagd information och deras ansvar för informationen.

Varje chef ansvarar för de leverantörer och konsulter som anlitas. IT-avdelningen ger dessa tillgång till de, av verksamhetschefen, angivna systemen. Leverantörer och konsulter ges tillgång till system genom engångslösenord via SMS (Mobility Guard) samt, enligt uppgift, fastställda rutiner hur tillgång till detta ges. De leverantörer och konsulter som kommer åt personuppgifter är enligt uppgift reglerade med sekretessavtal.

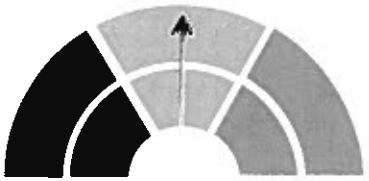
Det finns ingen löpande kontroll över att leverantörer och konsulter inte använder tillgången till kommunens system på ett otillbörligt sätt. Vidare var risken för informationsläckage inte inkluderat i den sårbarhetsanalys som gjordes under 2009. Loggning av händelser sker i nätverk och system, dock sker ingen strukturerad återkommande analys av loggarna.

Rekommendationer

Vi rekommenderar att kommunen ser över de rutiner som finns gällande behandling och tillgång till sekretessbelagd information för att säkerställa att ingen otillbörlig person får till gång till känslig information.

Vidare bör kommunen säkerställa att de system som leverantörer och konsulter ges tillgång till har ett väl fungerande logiskt skydd, utöver det i dagsläget implementerade åtkomstskyddet Mobility Guard samt att det finns rutiner för att säkerhetsställa att sekretessbelagd data inte ändras, flyttas eller kopieras till annan media. Kommunen bör göra en riskanalys över eventuell informationsläckage/otillbörlig tillgång till sekretessbelagd information för att säkerställa ett fullgott skydd av informationen.

Gradering



När barometern visar gult finns det betydande brister inom området som bör åtgärdas så snart som möjligt

Riktlinjer enligt den svenska standarden ISO 27002:2005

Rutiner för IT-säkerhetsincidenter bör fastställas.

Vid en eventuell incident bör det finnas noggranna och formella rutiner för att säkerhetsställa fullständig och korrekt återhämtning av data.

Kontinuitetsplan bör finnas som ledningsprocess och uppdateras kontinuerligt.

För att säkerhetsställa en organisations informationshantering bör det finnas fasställda rutiner för IT-säkerhetsincidenter. Dessa bör, enligt ISO 27002:2005 innefatta:

- Fel i informationssystem och bortfall av tjänst
- Skadlig kod
- Tillgänglighetsattacker
- Del som resultat av ofullständiga eller felaktiga verksamhetsdata
- Överträdelser mot konfidentialitet och riktighet
- Felaktig informationshantering

Utöver de ovan nämnda rutinerna bör det även finnas rutiner som täcker:

- Analys och identifiering av orsaken till incidenten
- Begränsning/avgränsning av incidenten
- Planering och korrigerande åtgärder för att förhindra upprepande incidenter
- Kommunikation med påverkad part och de som är involverade i återhämtningen
- Rapportering till eventuell myndighet

Vid eventuella incidenter bör det finnas rutiner fastställda för spårbarhetsloggar som kan komma att användas som rättsligt underlag men även som intern problemanalys. Då det förekommit ett incident bör det finnas noggranna och formella rutiner för att säkerhetsställa att en återhämtning sker korrekt och att inget dataförlust sker samt att avbrotten minimeras.

Enligt ISO 27002:2005 bör det finnas en kontinuitetsplan som bör underhållas kontinuerligt. Planen bör innehålla, men inte begränsat till, en identifiering av samtliga berörda tillgångar i kritiska verksamhetsprocesser, förståelse för den inverkan ett avbrott orsakar på kommunen, säkerhetsställande av personalsäkerhet samt skydd av informationsbehandlingsresurser och av kommunens egendom.

Väsentliga iakttagelser och rekommendationer

Det finns i nuläget ingen kommunövergripande kontinuitetsplan.

Behörighetskontrollsystem med tilldelade roller finns etablerade i nätverk och system.

IT-säkerhetspolicyn är inte anpassad för de risker som ny teknik medfört.

Det sker ingen kryptering av sekretessbelagd information, förutom i systemet Procapita.

Väsentliga iakttagelser

Det finns enligt säkerhetschefen såväl som IT-chefen och driftchefen för IT ingen övergripande kontinuitetsplan i kommunen och det är, enligt uppgift, osäkert huruvida några kontinuitetsplaner finns för någon av förvaltningarna. Enligt IT-säkerhetspolicyn skall en ständigt aktuell kontinuitetsplan finnas inom varje verksamhetsområde där organisering samt åtgärdsplan vid störningar i IT-stödet finns definierat. Det finns i nuläget få skriftliga och fastställda rutiner inom den centrala IT-avdelningen.

Enligt IT-säkerhetspolicyn skall ett utsett IT-säkerhetsombud inom varje förvaltning säkerställa att regelverk tillämpas inom samtliga förvaltningar och löpande rapportera detta till säkerhetschefen. Detta är något som, enligt uppgift, inte sker i nuläget.

Det finns tydliga fastställda behörighetskontrollsystem med tilldelade roller i kommunens nätverk och system. Närmsta chef bestämmer vilka roller som skall tilldelas en användare och kan inte ändras utan chefens godkännande.

Det sker i nuläget inte någon generell kryptering av hårddiskar och sekretessbelagd data. Detta gäller dock inte systemet Procapita som är krypterat. IT-avdelningen gör inga aktiva analyser av intrångsförsök utan det kommer dem endast till kännedom om ett konto låses eller om någon kontaktar dem. Det finns på helpdesk fasta skriftliga rutiner om hur användare återfår ett nytt lösenord samt inloggning.

IT-säkerhetspolicyn är inte anpassad för de risker som ny teknik såsom USB-minnen, bärbar lagringsmedia, smartphones, molnteknik med mera medfört. Den centrala IT-avdelningen har regelbundna möten där ny teknik diskuteras och vad som skall fasas ut. Ny utrustning som upphandlas av IT-avdelningen testas och godkänns innan implementering.

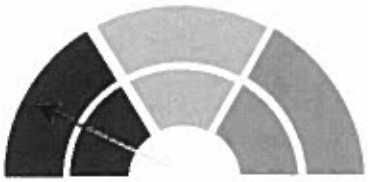
Rekommendationer

Vi rekommenderar att IT-avdelningen utarbetar en kontinuitetsplan med fokus på den verksamhet som bedrivs samt med dagens gällande risker. Ett samlat ramverk för kontinuitetsplanering bör finnas för att säkerställa att alla planer är konsekventa, att informationssäkerhetskraven behandlas konsekvent samt för att fastställa prioriteringar gällande test och underhåll av IT-system.

Vi rekommenderar vidare att kommunen ser över riskerna i dagens IT-miljö för att överväga kryptering av data av känslig eller kritiskt slag. Om kommunen väljer att implementera en krypteringslösning bör en krypteringspolicy implementeras för att klargöra ansvar, minimera risker och för att undvika olämplig eller felaktig användning.

Vår rekommendation gällande användandet av ny teknik inom kommunen är att utföra en riskanalys gällande bärbar media, smartphones samt molnteknik för att förhindra att sekretessbelags information medförs utan kommunens godkännande. Krypteringen bör dimensioneras utifrån en riskbedömning och områden som bör beaktas är bland annat in-/urkoppling av I/O-enheter och ned-/uppladdning av vissa filtyper till moln som kan innehålla sekretessbelagd information.

Gradering



När barometern visar rött förekommer stora brister inom området och det är kritiskt att bristerna åtgärdas omgående

Please consider the environment before printing.