Kommunens beredskap för IT-störningar och incidenter

Rapport

Tjörns kommun

KPMG AB

2022-10-27

Antal sidor 17

© 2022 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document classification: KPMG Confidential

Tjörns kommun
Kommunens beredskap för IT-störningar och incidenter

2022-10-27

Innehållsförteckning

© 2022 KPMG AB. All rights reserved.

Document classification KPMG Confidential

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Tjörns kommun fått i uppdrag att genomföra en granskning av beredskap för IT-störningar och incidenter i ett urval av kommunens nämnder. Uppdraget ingår i revisionsplanen för 2022.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna inte fullt ut har ändamålsenliga rutiner för att upprätthålla verksamheter vid större IT-störningar.

Vi kan konstatera att det i nuläget inte finns ett tillräckligt systematiskt och riskbaserat informationssäkerhetsarbete (där den tekniska IT-säkerheten ingår) etablerat i kommunen. Kommunstyrelsen har därigenom brustit i sitt ansvar. Bland annat saknas styrande dokument och en etablerad uppföljning av det arbete som bedrivs. Ett bristande informationssäkerhetsarbete påverkar i sin tur kommunens samlade förutsättningar att skydda informationstillgångar och upprätthålla verksamhetens kontinuitet i händelse av incident eller allvarlig störning.

Kommunledningskontoret har genomfört ett antal genomlysningar under 2022 för att identifiera ett nuläge för kommunens informations- och IT-säkerhet. Dessa visar att utvecklingsbehov finns avseende organisation, resurser, systematik och tekniska åtgärder. Kommunstyrelsen har utifrån genomförd genomlysning beslutat om vissa åtgärder men vi kan inte utesluta att det finns risk att inte tillräckliga åtgärder vidtagits som ett resultat av de brister och sårbarheter som rapporterna visat.

Inom socialnämnden och samhällsbyggnadsnämnden finns dokumenterade kontinuitetsplaner där bedömningar av risker och bortfall av IT är inkluderat. Barn- och utbildningsnämnden har gjort vissa klassificeringar och riskbedömningar för sina verksamhetskritiska system men vi uppfattar att det i nuläget saknas dokumenterade kontinuitetsplaner vid bortfall av IT eller allvarlig störning. Det finns till viss del manuella rutiner men en bedömning bör göras om dessa skulle vara tillräckliga vid avbrott eller störning.

Utifrån vår sammanfattande bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Besluta om styrande dokument inom beredskap för IT-störningar/incidenter och informationssäkerhet för att etablera en styrning med krav om beredskap och kontinuitet för kommunens verksamheter.
- Besluta om styrande dokument inom informationssäkerhet inkl. den tekniska säkerheten så att ansvar, krav och uppföljningsrutiner finns dokumenterade.
- Tillse att ett systematiskt informationssäkerhetsarbete är etablerat med tydliggjorda krav och rutiner för uppföljning så att förbättringsåtgärder kan vidtas på kommunövergripande nivå.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

— Säkerställa att det finns en organisation för informations- och IT-säkerhetsarbetet med tillräckliga förutsättningar att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete där åtgärder vidtas utifrån identifierade risker och hot.
— Genomföra utbildning för samtliga medarbetare och förtroendevalda i informations- och IT-säkerhet så att grundläggande kunskap och medvetenhet finns etablerat.
— Etablera incidenthanteringsrutiner för informations- och IT-säkerhetsincidenter tillsammans med utbildningsinsatser för att säkerställa att incidenter upptäcks och anmäls.
— Säkerställa att dokumenterade planer revideras löpande utifrån nya hot och risker.

Utifrån vår sammanfattande bedömning och slutsats rekommenderar vi socialnämnden, barn- och utbildningsnämnden samt samhällsbyggnadsnämnden att:

— Säkerställa att de beredskaps- och kommunikationsplaner som finns är uppdaterade och tillräckliga att utgå från i händelse av IT-incident eller störning, exempelvis genom regelbundna tester.
— Tillse att ett systematiskt informationssäkerhetsarbete är etablerat med tydliggjorda krav och rutiner för uppföljning. En grund för detta är att riskanalys och informationsklassning genomförs som leder till att krav om säkerhetsåtgärder ställs utifrån ett bedömt skyddsvärde.
— Etablera incidenthanteringsrutiner för informations- och IT-säkerhetsincidenter tillsammans med utbildningsinsatser för att säkerställa att incidenter upptäcks och anmäls.
— Säkerställa att dokumenterade kontinuitetsplaner revideras löpande utifrån nya hot och risker.

Vi rekommenderar även samhällsbyggnadsnämnden att:

- Vidta de tekniska åtgärder som är nödvändiga för en efterlevnad av NIS-direktivet.

Vi rekommenderar även barn- och utbildningsnämnden att:

— Säkerställa att det finns dokumenterade kontinuitetsplaner.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

2 Bakgrund

Vi har av Tjörns kommuns revisorer fått i uppdrag att granska kommunens beredskap för IT-störningar och incidenter. Uppdraget ingår i revisionsplanen för år 2022.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och en stor del av informationen hanteras i IT-system vilket ställer höga krav på att dessa är tillgängliga och säkra. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Hotbilden med risker för intrång förändras och ökar i omfattning vilket innebär att kommunens arbete med IT-säkerhet behöver vara i ständig utveckling. En regelbunden omvärldsanalys och tekniska funktioner för övervakning behövs för att i tid upptäcka och i den mån det går förhindra att dessa leder till att information förvanskas eller röjs. Det behövs även en beredskap och rutiner hur IT-miljön och dess komponenter ska hanteras vid störningar och avbrott i form av reserv-, återställnings-, och återgångsrutiner finns för att säkra kärnverksamhetens kontinuitet.

Under 2021 inträffade ett antal IT-incidenter vilket tydliggjorde hur sårbart samhället är för större IT-störningar. Bland annat utsattes Kalix kommun och Emmaboda kommun. Attackerna genomförs av olika aktörer och med olika motiv, allt ifrån att destabilisera demokratin, kräva ekonomisk ersättning (lösensumma) eller få tag i känslig information som kan utnyttjas och spridas. IT-säkerheten blir allt viktigare men även robustheten i organisationen för att verksamheter ska kunna fortgå utan tillgång till IT och system.

Med anledning av ovan har revisorerna i sin risk- och väsentlighetsanalys bedömt att kommunens beredskap för IT-störningar och incidenter behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen är att bedöma om kommunen har ändamålsenliga rutiner för att upprätthålla verksamheter vid större IT-störningar.

Granskningen avser att besvara följande revisionsfrågor:

- Har kommunstyrelsen efter senaste tidens händelser vidtagit åtgärder för att uppdatera sig om kommunens förutsättningar att stå emot eventuella intrångsförsök och allvarlig IT-störning?
- Har riskanalyser upprättats för att identifiera sårbarheter?
    - Har åtgärder vidtagits som ett resultat av dessa?
- Finns beredskapsplan/-er för hur kommunen ska agera om en incident av allvarligare karaktär inträffar?
    - Avseende IT-drift för hantering av servrar, nätverk, system och klienter?
    - Inom respektive verksamhet för att säkerställa kontinuiteten och upprätthålla verksamheter inom exempelvis vård, omsorg, skola och samhällsservice?

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

  - För intern och extern kommunikation?
- Finns etablerade incidenthanteringsrutiner med tydliggjorda eskaleringsvägar?

Granskningen omfattar

- Kommunstyrelsen
- Samhällsbyggnadsnämnden
- Barn- och utbildningsnämnden
- Socialnämnden

Nämnderna berörs i granskningen utifrån deras arbete med beredskaps- och kontinuitetsplaner. I övrigt har granskningen avsett arbetet på kommunövergripande nivå.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Styrdokument i form av policys och riktlinjer
- Interna rutinbeskrivningar inom området

2.3 Metod

Granskningen har genomförts genom intervjuer med tjänstepersoner och förtroendevalda samt en dokumentgranskning av relevanta dokument. Dessa presenteras löpande i rapporten.

De funktioner som intervjuats är:

- Kommunstyrelsens ordförande
- Kommundirektör
- Avdelningschef kommunledningskontoret
- Beredskapssamordnare
- Enhetschef IT
- Förvaltningschef socialförvaltningen
- Förvaltningschef utbildningsförvaltningen
- Förvaltningschef samhällsbyggnad
- Kommunikationschef

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

- Digitaliseringsstrateg
- Dataskyddsombud med ansvar för informationssäkerhet
- Säkerhetssamordnare

Samtliga intervjuade har beretts möjlighet att faktagranska rapporten.

Granskningen har genomförts av William Andreasson, kommunal revisor, under ledning av Jenny Thörn, certifierad kommunal revisor. Liz Gard har deltagit som kvalitetsansvarig för rapporten utifrån sin roll som kundansvarig för Tjörns kommun.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

3 Resultat av granskningen

3.1 Styrning av säkerhets- och beredskapsarbetet

3.1.1 Styrande dokument

Tjörns kommuns säkerhetspolicy[1]

Kommunens säkerhetspolicy är ett övergripande styrdokument som beskriver det kommunövergripande säkerhetsarbetet.

I policyn anges att kommunen ska bedriva arbete med säkerhet och riskhantering i syfte att uppnå att verksamheter utifrån policyn definierar och utformar säkerhetsarbetet i balans med krav på öppenhet och tillgång genom kontinuerlig utveckling, uppföljning och analys.

I policyn beskrivs vidare att kommunens medarbetare ansvarar för gällande säkerhetsregler och rutiner inom sina respektive arbetsområden. Policyn anger mål med säkerhetsarbetet, exempelvis att riskanalyser ska vara en naturlig del vid verksamhetsförändring, att anställda ska utbildas i säkerhetsfrågor och att säkerställa en god beredskap för hantering av eventuella krissituationer.

Vi noterar att säkerhetspolicyn inte inkluderar informations- eller IT-säkerhet.

Informationssäkerhetspolicy (Ej beslutad)

Det har tidigare funnits styrdokument i form av rutiner, riktlinjer och instruktioner för informationssäkerhetsarbetet. Av vad vi tagit del av framgår inte att styrdokumenten varit politiskt beslutade. Dokumenten uppges även av intervjupersoner i nuläget vara inaktuella, då informationssäkerhetsarbetet omarbetas. Kommunen befinner sig i nuläget i en omorganisation avseende informationssäkerhetsarbetet. Som ett resultat av detta har en ny informationssäkerhetspolicy[2] arbetats fram, vilken fastställdes vid kommunfullmäktiges möte 2022-10-20.[3]

Den nya informationssäkerhetspolicyn ska ange den övergripande viljeriktningen för kommunens informationssäkerhetsarbete. I policyn anges att kommunens information ska skyddas utifrån principerna riktighet, tillgänglighet och konfidentialitet.

Vidare framgår att kommunens informationssäkerhetsarbete ska ske utifrån standardserien ISO/IEC 27000. Kommunledningen ska tillse att informationssäkerhetsarbetet ges lämpliga resurser och att interna regelverk avseende informationssäkerhet upprättas, efterlevs, utvärderas och anpassas.

[1] 2013-05-02, § 82.
[2] Arbetsdokument, förvaltningens förslag till informationssäkerhetspolicy 2022-07-15.
[3] Protokollet var inte justerat och offentliggjort vid tiden för rapportens färdigställande.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

Informationssäkerhetspolicyn är tänkt att kompletteras med organisationsövergripande riktlinjer för informationssäkerhet.

Övriga stödjande dokument

Kommunen använder Länsstyrelsens rutindokument *Kriskommunikationssamverkan i Västra Götaland*, *När de ordinarie kanalerna inte räcker till* samt MSB:s handbok *Att möta informationspåverkan*.

3.1.2 Roller och ansvar för krisledning och krisberedskap

Krisledningsorganisation och ansvarsfördelning

Tjörns kommun har en krisledningsorganisation som kan aktiveras för att stärka verksamheter vid kris. Vid extraordinära händelser finns det en krisledningsnämnd som initieras.

Enligt reglementet för kommunstyrelsen[4] framgår att den är ansvarig för det övergripande säkerhetsarbetet i kommunen och att säkerhetsskyddslagstiftning följs.

Enligt säkerhetspolicyn ansvarar nämnderna för säkerhetsarbetet inom sitt område och svarar för att fastställa verksamhetsspecifika kompletteringar till säkerhetspolicyn. Policyn beskriver också det utökade säkerhetsansvar en chefsbefattning inbegriper.

Kommunens säkerhetspolicy beskriver att säkerhetsansvaret ska följa det normala verksamhetsansvaret på olika nivåer i kommunen. Av policyn framgår även en uppställning av de anställdas säkerhetsansvar, bland annat att samtliga anställda ansvarar för ett aktivt säkerhetsarbete och att påpeka säkerhetsbrister. Vi noterar dock att utbildningar inom informations- och IT-säkerhet inte har erbjudits medarbetare eller förtroendevalda i närtid. En kompetensplattform har upphandlats men vid tiden för granskningen har inga utbildningar genomförts.

3.2 IT-säkerhetsarbetet

Enligt uppgift har kommunen under flera års tid arbetat för att stärka IT-säkerheten. Bland annat har dataskyddsombudsrollen etablerats på kommunledningskontoret, för att stärka den centrala kompetensen. Av intervjuer framgår att händelserna i Kalix intensifierat både kommunledningens och kommunstyrelsens arbete avseende informationssäkerhet och beredskap för IT-störningar eller incidenter. Detta styrks av protokoll (KSAU, 2022-05-19 §103) där det framgår att resultatet av en genomlysning av kommunens informationssäkerhet presenterats för kommunstyrelsen. Presentationen av rapporten innehöll grundläggande begrepp om informationssäkerhet och exempel på incidenter i linje med de som inträffat i Kalix och Emmaboda kommuner. Presentationen avslutas med en summering, där det konstateras att åtgärder utifrån de risker och förbättringsområden som identifierats under

[4] KF 2020-02-20 § 37, senast reviderad KF 2022-03-24 § 60.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

genomlysningen behöver hanteras. I rapporten lyfts att kommunledningens engagemang i frågan är avgörande. Engagemang från ledningen krävs bland annat genom att tillse tillräckliga resurser för säkerhetsarbetet och prioritera åtgärder. Det fastställs ett antal nödvändiga åtgärder i presentationen, bland annat att fastställa en informationssäkerhetsorganisation, organisera centralt stöd för förvaltningschefer, bolagsdirektörer och andra nyckelpersoner och att etablera en förvaltningsorganisation för kritiska system eller produkter.

Kommunstyrelsens arbetsutskott föreslog kommunstyrelsen att med anledning av säkerhetsskäl ta steg mot att förlägga kommunens IT-drift på en extern leverantör. Kommunstyrelsen beslutade att Soltak AB:s IT-tjänster i de fall som de lever upp till kommunens behov och krav ska nyttjas. Kommunen ska enligt beslutet även medverka till utveckling av IT-tjänster hos bolaget (2022-06-02 § 127).

Kommunledningen vill även framhålla att de anser att kommunen historiskt haft en god IT-säkerhet avseende externt skydd som exempelvis brandväggar. Kommunledningen framhåller att de ser positivt på det fördjupade samarbetet med Soltak AB och tror att det kan bidra till att höja kommunens IT-säkerhet.

Av granskningen framgår att det saknas styrande dokument avseende informations- och IT-säkerhet inklusive roll- och ansvarsfördelning. På så vis saknas en övergripande styrning av informations- och IT-säkerhetsarbetet. Uppdragsbeskrivning och kravnivåer är inte heller dokumenterade. Detta styrks även av intervju med kommunens IT-enhet, som menar att det i nuläget i stort saknas en organisation för IT-säkerhetsarbetet.

Enligt intervjuer ingår bedömningar av IT-störning och intrång i den koncernövergripande risk- och sårbarhetsanalys som upprättas en gång per mandatperiod utifrån lagkrav[5] för beredskapsarbetet. Riskanalysen genomförs bland annat i workshopform med verksamhetsföreträdare.

Av intervjuer framgår vidare att i riskanalysen, där identifiering av kritiska verksamhetssystem ingår, ska följande bedömning göras av kommunens verksamhetsföreträdare:

- Internetbortfall i minst 24 timmar – Här ska verksamheterna beskriva hur bortfallet påverkar dem och om deras kritiska system påverkas.
- Dataintrång, förlust av information – Här ska verksamheterna beskriva hur de påverkas om kritisk information i deras system görs otillgänglig eller röjs.

Kommunledningskontoret har tillsammans med IT-enheten genomfört tre analyser under 2022 för att identifiera ett nuläge för kommunens informationssäkerhet. I genomlysningarna ingick bland annat mognadsmätning avseende organisation och systematik, mätningen tillhandahålls av Myndigheten för samhällsskydd och beredskap, MSB. En GAP-analys har gjorts avseende administrativ, fysisk och teknisk

[5] Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap samt Myndigheten för samhällsskydd och beredskaps föreskrifter om kommuners risk- och sårbarhetsanalyser (MSBFS 2015:5).

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

säkerhet utifrån krav i enlighet med standarden ISO 27001. Därutöver har en extern granskning genomförts av konsult.[6]

Av GAP-analysens resultat framgår att kommunen inte når önskade nivåer på något av de uppmätta områdena.[7] Av resultatet av den externa konsultens analys framgår att kommunen behöver förbättra sitt arbete med IT-säkerhet. Resultatet visade bland annat att teknisk modernisering är nödvändig tillsammans med en utveckling av organisation och systematik. Resultatet från dessa analyser har sammanställts och presenterats för kommunledningsgruppen och kommunstyrelsen.

3.2.1 Bedömning

Vi bedömer att kommunstyrelsen i viss utsträckning vidtagit åtgärder utifrån den senaste tidens händelser och det förändrade säkerhetsläget avseende cyberhot och intrång. Den har mot bakgrund av resultatet i genomlysningen beslutat att kommunen utifrån säkerhetsskäl i högre grad ska nyttja extern leverantör för IT-drift. Vi kan dock inte utesluta att det utifrån genomlysningens resultat finns ytterligare behov av åtgärder som kommunstyrelsen bör fatta beslut om för att stärka både informations- och IT-säkerheten.

Vi bedömer vidare att kommunstyrelsen utifrån sitt övergripande ansvar att styra säkerhetsarbetet bör säkerställa att styrande dokument inom informationssäkerhet och en tydligare styrning av IT-säkerhetsarbetet upprättas. En ny informationssäkerhetspolicy tas fram i nuläget vilket kan bidra till ökad tydlighet inom dessa frågor. Vi bedömer dock att det är av stor vikt att kommunstyrelsen tillser att den nya informationssäkerhetspolicyn och tillhörande, mer specifika riktlinjer och rutiner får förankring i verksamheten för att effektivt kunna styra säkerhetsarbetet. I samband med implementeringen bör utbildningstillfällen genomföras för att etablera en grundläggande kunskap och medvetenhet om säkerhetsfrågor för att skapa en säkerhetskultur.

Vår bedömning är att riskanalys i syfte att identifiera sårbarheter avseende IT-drift, servrar, nätverk och system delvis har gjorts i genomlysningar under 2022. Dessa har identifierat ett antal sårbarheter och risker för kommunens informationshantering och IT-säkerhet. Vid tidpunkten för granskningen kan vi dock inte utesluta att det finns nödvändiga säkerhetsåtgärder som inte vidtagits. Den koncernövergripande risk- och sårbarhetsanalys som görs en gång per mandatperiod omfattar också dessa områden

Kommunstyrelsen bör säkerställa att ett systematiskt informationssäkerhetsarbete etableras, för att stärka förutsättningarna till en god informations- och IT-säkerhet. Vi bedömer även ett behov av att kommunstyrelsen utvärderar om IT-avdelningens

[6] Den externa granskningen innefattade maskinell analys av IT-infrastruktur samt organisatorisk mognad och systematik.
[7] GAP-analysen innehåller flera områden där respondenter inom kommunen får svara genom självskattningar. Exempel på områden är hantering av informationssäkerhetsincidenter, hantering av informationstillgångar, driftssäkerhet och efterlevnad.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

resurser är tillräckliga i förhållande till de behov som finns för att ha en motståndskraft mot risker och hot. Därtill bör IT-avdelningens ansvar och uppdrag tydliggöras så att det finns dokumenterat vilka kravnivåer som de har att efterleva i IT-säkerhetsarbetet.

3.3 Kriskommunikation

Kommunen arbetar efter det koncernövergripande styrdokumentet Kommunikation – riktlinjer.[8] Dokumentet fastställer kommunens mål- och övergripande viljeriktning med kommunikationsarbetet. Av dokumentet beskrivs även mål och principer för kommunens kommunikationsarbete. Principer för kriskommunikation framgår av riktlinjerna. Bland annat framgår en checklista vid kriskommunikation, som anger att kriskommunikationen ska samla relevant information, innehålla tydliga budskap, undvika ryktesspridning, med mera.

I intervjuer framgår att kommunikationsavdelningen i sitt arbete utgår från Riktlinje för kriskommunikation[9] om en särskild händelse inträffar i kommunen.

Riktlinjerna för kriskommunikation är ett kompletterande dokument till kommunens övriga styrdokument inom kommunikation, exempelvis de övergripande riktlinjerna för kommunikation. I riktlinjen beskrivs och definieras centrala begrepp för krishantering, som exempelvis samhällsstörning och extraordinär händelse. Riktlinjen beskriver även de grundläggande principerna för krisberedskap – ansvars-, likhets- och närhetsprincipen.

Ansvaret för kriskommunikation anges riktlinjen, bland annat framgår att respektive nämnd eller styrelse som påverkas av en samhällsstörning är ansvarig för kriskommunikation i relation till dess påverkan på den egna verksamheten. I riktlinjen beskrivs också hur nämnder/styrelser ska arbeta med kriskommunikation inför, under och efter en samhällsstörning. Det beskrivs exempelvis hur kriskommunikationsarbetet ska genomföras, hur det ska säkerställas att en adekvat kriskommunikationsplan utvecklas under störningens gång, samt hur utvärdering och avveckling av arbetet ska ske.

Av intervjuer framgår att kommunikationsenheten har etablerade arbetssätt för att nå ut till medborgarna vid IT-bortfall. Kommunen har exempelvis utsatta trygghets- och informationspunkter, mikrofoner och färdigtryckta skyltar. Av intervju framgår vidare att kommunikationsavdelningen deltagit i krisövningar som hållits inom kommunen, men att dessa inte berört IT-störningar eller incidenter.

Vad gäller den interna kommunikationen vid händelse av kris framkommer en viss problematik att nå ut till samtliga medarbetare genom en kanal.

[8] Riktlinjerna beslutades av dåvarande kommunchef den 2011-03-22. Enligt uppgift har förnyelse av riktlinjerna diskuterats med kommundirektör 2022, men att nuvarande bedömning är att riktlinjerna i befintlig form fortsatt är relevanta.
[9] Dessa riktlinjer är ännu inte beslutade, men motsvarar enligt uppgift kommunikationsavdelningens arbetssätt vid kris.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

3.3.1 Bedömning

Vi bedömer att det finns etablerade riktlinjer, arbetssätt och analoga kanaler för att externt nå ut med information till medborgare. Vi bedömer dock att kommunstyrelsen bör säkerställa att den interna kommunikationen fungerar även under IT-bortfall och att det finns möjlighet att samlat nå kommunens medarbetare.

3.4 Förvaltningarnas kontinuitet i händelse av IT-störning

3.4.1 Socialnämndens verksamheter

Socialförvaltningen har etablerade interna styrdokument för krishantering och krisledning. I förvaltningens lednings- och informationsplan för krishantering framgår exempelvis ansvar, roller och uppgifter för förvaltningens funktioner vid hantering av särskilda eller extraordinära händelser. Vidare tydliggörs förvaltningens organisation och ledning vid kris i dokumentet. Dokumentet beskriver också förvaltningens krisledningsgrupp, kommunikation, samt utvärdering och uppföljning av hur krisen hanterats.

Förvaltningen har tagit fram stödmaterial avseende informationsklassning i sina digitala system och genomför enligt intervjuuppgifter klassningar aktivt. Vi har tagit del av ett exempel för informationsklassning av socialnämndens verksamhetssystem. Klassningen genomfördes 2016. Vi har därtill tagit del av dokumenterad riskanalys och kontinuitetsplan i vår granskning. Det finns kontinuitetsplan för förvaltningens centrala verksamhetssystem. I kontinuitetsplanen framgår hur förvaltningen ska arbeta i de fallen systemet inte är tillgängligt. I planen beskrivs hur kontinuiteten i identifierade kritiska resurser ska upprätthållas, hur resursen återställs vid störning samt hur återgång till normalläge ska ske då resursen fungerar normalt. I dokumentet framgår dokumentägare och systemansvarig, en objektsbeskrivning av systemet och hur kontinuitetsplanen ska aktiveras. Kontinuitetslösningar är beskrivna i en checklista för att underlätta ett systematiskt tillvägagångssätt. I checklistan ingår bland annat ett mål för återställningstid samt reservrutiner och ansvarig per punkt i listan.

Förvaltningen har därtill en rutin för nätverksbortfall eller driftfel där dessa kan få en påverkan på verksamhetssystem. Rutinen innehåller punktvisa beskrivningar för de aktuella verksamhetssystemen, där bland annat utskrift av manuella listor ingår. Rutinen revideras årsvis eller vid behov.

Av intervjuer uppges att förvaltningen har ett robust IT-säkerhetsarbete och att risk för IT-bortfall beaktas i riskanalyser, vilket är i linje med det material vi tagit del av. Kritiska verksamhetssystem finns identifierade och kontinuitetsplaner har upprättats för verksamheten vid IT-bortfall eller avsaknad av telefoni. Förvaltningens trygghetslarm, som används av brukare, är exempelvis beroende av fungerande telefoni. I de fall telefonin inte fungerat finns en rutin för hur medarbetarna ska säkerställa brukarnas hälsa. Rutinen har använts i närtid med anledning av telefonistörningar och uppges vara välfungerande.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

Socialförvaltningen arbetar i nuläget med upphandling av ett nytt verksamhetssystem som ska ersätta det nuvarande Magna Cura. I upphandlingen har förvaltningen haft ett nära samarbete med kommunens IT-avdelning, som bistått med stöd. Av intervju framgår att ett säkerhetsperspektiv ingår i kommunens kravställning gentemot leverantör.

3.4.2 Samhällsbyggnadsnämndens verksamheter

Av intervjuer framgår att man arbetar systematiskt riskbedömning och beredskap för IT-störningar eller bortfall, i huvudsak avseende den samhällsviktiga verksamheten inom förvaltningen. I granskningen har vi tagit del av dokumentation som styrker detta.

VA-verksamhetens driftssystem är ISO 27001-certifierat. Emellertid så är ytterligare säkerhetsåtgärder för driftssystemet nödvändiga. De nödvändiga åtgärderna är kända inom kommunledningen och kommer inte specificeras i rapporten. För de digitala system som används inom den samhällsviktiga verksamheten som omfattas av NIS-direktivet[10] finns dokumenterade kontinuitetsplaner.

Vi har för övriga system och digitala tjänster som nyttjas inom samhällsbyggnadsförvaltningen fått detaljerade beskrivningar av säkerhetsåtgärder för att upprätthålla verksamheten både i den dagliga driften och vid särskilda händelser. Förvaltningen uppger i intervjuer att de har etablerade arbetssätt med risk- och sårbarhetsanalyser där IT-relaterade risker ingår att bedöma. Vi har dock inte tagit del av dokumentation eller annat material.

Utbildningar har även genomförts med kommunens centrala säkerhetssamordnare för vissa medarbetare inom förvaltningen. Dessa utbildningar har berört generell säkerhet och inkluderat IT-säkerhetsfrågor, som exempelvis försiktighet vid länkar i mejl.

3.4.3 Barn och utbildningsnämndens verksamheter

Barn och utbildningsförvaltningen arbetar aktivt med informationsklassificering i sina digitala system. Förvaltningen ställer också krav på informationssäkerhet vid upphandling av digitala system. Förvaltningen har gjort riskanalyser för de system som verksamheten bedömt vara kritiska. Utifrån vad som framkommit i riskanalyserna har åtgärder vidtagits, däribland behörighetskontroller och utbildningsinsatser.

Av intervju med barn- och utbildningsförvaltningen framgår att de upplever att säkerhetsmedvetenheten inom förvaltningen är hög. Förvaltningen har vissa manuella rutiner/arbetssätt vid händelse av en IT-störning, exempelvis i form av utskrivna klasslistor som förvaras inlåsta.

[10] Network and Information Security Directive (2016/1148), översatt till Nätverks- och informationssäkerhetsdirektivet (NIS) innehåller säkerhetskrav på nätverk och informationssystem i verksamheter som bedöms som samhällsviktiga. Exempel på sådana verksamheter är hälso- och sjukvård, leverans och distribution av dricksvatten, energi och digital infrastruktur.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

Informationssäkerhetsarbetet uppges av intervjupersoner inte vara systematiskt. Intervjupersoner uppger att det saknas interna styrdokument, riktlinjer och rutiner för exempelvis kontinuitetsplanering.

3.4.4 Bedömning

Vi noterar vissa skillnader mellan förvaltningarnas beredskap för en IT-störning eller incident. För att säkerställa en jämnare nivå på beredskapen för IT-störningar eller incidenter i förvaltningarna anser vi att kommunstyrelsen bör tydliggöra styrning och krav på riskanalyser och dokumenterade kontinuitetsplaner där bland annat IT-bortfall ingår och att dokumenterade planer revideras löpande utifrån nya hot och risker.

Socialnämnden

Vi bedömer att socialnämnden i huvudsak har ett systematiskt arbete med riskanalyser, handlings- och kontinuitetsplaner som inkluderar bortfall av IT. Vi vill dock påtala vikten av att löpande uppdatera och omvärdera riskanalyser och informationsklassningar utifrån förändringar i system, omvärldsfaktorer eller nya lagkrav så att säkerhetsåtgärder kan vidtas utifrån det bedömda skyddsvärdet.

Samhällsbyggnadsnämnden

Vi bedömer att samhällsbyggnadsnämnden till viss del har ett systematiskt arbete med riskanalyser, handlings- och kontinuitetsplaner som inkluderar bortfall av IT. Detta avser främst den verksamhet som är samhällsviktig. Vi bedömer emellertid att tekniska åtgärder bör vidtas för att möta de krav som finns för informationssystem som används för samhällsviktig verksamhet. Samhällsbyggnadsnämnden bör därtill inrätta ett systematiskt informationssäkerhetsarbete för övriga informationstillgångar som nämnden ansvarar för så att dessa är skyddade utifrån ett bedömt skyddsvärde.

Barn- och utbildningsnämnden

Vi bedömer att barn- och utbildningsnämnden i vissa delar har en systematik i arbetet med informationsklassningar och bedömningar för sina verksamhetskritiska system. Det är positivt att förvaltningen har en god säkerhetskultur och manuella rutiner för exempelvis utskrift av klasslistor men vi bedömer att nämndens arbete kan utvecklas genom ytterligare riskanalyser och dokumenterade kontinuitetsplaner i händelse av IT-bortfall eller allvarlig störning.

3.5 Incidenthantering

I avsaknad av styrande dokument inom informationssäkerhetsområdet har vi inte tagit del av beskrivning av hur incidenter av olika slag ska hanteras inom kommunen.

Av intervjuer framkommer att kommunen saknar fastställda rutiner för incidenthantering och vi noterar att olika beskrivningar över incidenthantering förvaltningsvis framkommer. Intervjupersoner inom förvaltningarna uppger bland annat att de flesta användare sannolikt skulle ta direktkontakt med kommunens IT-enhet om en incident

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

inträffar. Vissa lyfter även att kommunen har ett avvikelserapporteringssystem på intranätet som nyttjas för incidentrapportering av vissa förvaltningar.

3.5.1 Bedömning

Vår bedömning är att det saknas etablerade, tydliga incidenthanteringsrutiner med tillhörande eskaleringsvägar. Detta bör tydliggöras för ökade förutsättningar att agera i händelse av attack eller incident. Vi bedömer även att styrdokument bör tillses för arbetet med incidentrapporteringen. Detta för att tydliggöra vad som är en incident och hur den ska rapporteras.

Utbildning avseende incidenter bör även genomföras för att öka kunskap och medvetenheten kring vad som är incidenter och hur dessa ska hanteras. Incidenter bör även dokumenteras och analyseras så att eventuella brister och sårbarheter kan mötas med proportionerliga åtgärder.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

4 Slutsats och rekommendationer

4.1 Slutsats

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och nämnderna inte fullt ut har ändamålsenliga rutiner för att upprätthålla verksamheter vid större IT-störningar.

Vi kan konstatera att det i nuläget inte finns ett tillräckligt systematiskt och riskbaserat informationssäkerhetsarbete (där den tekniska IT-säkerheten ingår) etablerat i kommunen. Kommunstyrelsen har därigenom brustit i sitt ansvar. Bland annat saknas styrande dokument och en etablerad uppföljning av det arbete som bedrivs. Ett bristande informationssäkerhetsarbete påverkar i sin tur kommunens samlade förutsättningar att skydda informationstillgångar och upprätthålla verksamhetens kontinuitet i händelse av incident eller allvarlig störning.

Kommunledningskontoret har genomfört ett antal genomlysningar under 2022 för att identifiera ett nuläge för kommunens informations- och IT-säkerhet. Dessa visar att utvecklingsbehov finns avseende organisation, resurser, systematik och tekniska åtgärder. Kommunstyrelsen har utifrån genomförd genomlysning beslutat om vissa åtgärder men vi kan inte utesluta att det finns risk att inte tillräckliga åtgärder vidtagits som ett resultat av de brister och sårbarheter som rapporterna visat.

Inom socialnämnden och samhällsbyggnadsnämnden finns dokumenterade kontinuitetsplaner där bedömningar av risker och bortfall av IT är inkluderat. Barn- och utbildningsnämnden har gjort vissa klassificeringar och riskbedömningar för sina verksamhetskritiska system men vi uppfattar att det i nuläget saknas dokumenterade kontinuitetsplaner vid bortfall av IT eller allvarlig störning. Det finns till viss del manuella rutiner men en bedömning bör göras om dessa skulle vara tillräckliga vid avbrott eller störning.

Utifrån vår sammanfattande bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Besluta om styrande dokument inom beredskap för IT-störningar/incidenter och informationssäkerhet för att etablera en styrning med krav om beredskap och kontinuitet för kommunens verksamheter.
- Besluta om styrande dokument inom informationssäkerhet inkl. den tekniska säkerheten så att ansvar, krav och uppföljningsrutiner finns dokumenterade.
- Tillse att ett systematiskt informationssäkerhetsarbete är etablerat med tydliggjorda krav och rutiner för uppföljning så att förbättringsåtgärder kan vidtas på kommunövergripande nivå.
- Säkerställa att det finns en organisation för informations- och IT-säkerhetsarbetet med tillräckliga förutsättningar att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete där åtgärder vidtas utifrån identifierade risker och hot.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

- Genomföra utbildning för samtliga medarbetare och förtroendevalda i informations- och IT-säkerhet så att grundläggande kunskap och medvetenhet finns etablerat.
- Etablera incidenthanteringsrutiner för informations- och IT-säkerhetsincidenter tillsammans med utbildningsinsatser för att säkerställa att incidenter upptäcks och anmäls.
- Säkerställa att dokumenterade planer revideras löpande utifrån nya hot och risker.

Utifrån vår sammanfattande bedömning och slutsats rekommenderar vi socialnämnden, barn- och utbildningsnämnden samt samhällsbyggnadsnämnden att:

- Säkerställa att de beredskaps- och kommunikationsplaner som finns är uppdaterade och tillräckliga att utgå från i händelse av IT-incident eller störning, exempelvis genom regelbundna tester.
- Tillse att ett systematiskt informationssäkerhetsarbete är etablerat med tydliggjorda krav och rutiner för uppföljning. En grund för detta är att riskanalys och informationsklassning genomförs som leder till att krav om säkerhetsåtgärder ställs utifrån ett bedömt skyddsvärde. Detta är ett pågående arbete och behöver kontinuerligt omprövas för att möta nya risker.
- Etablera incidenthanteringsrutiner för informations- och IT-säkerhetsincidenter tillsammans med utbildningsinsatser för att säkerställa att incidenter upptäcks och anmäls.
- Säkerställa att dokumenterade kontinuitetsplaner revideras löpande utifrån nya hot och risker.

Vi rekommenderar även samhällsbyggnadsnämnden att:

- Vidta de tekniska åtgärder som är nödvändiga för en efterlevnad av NIS-direktivet.

Vi rekommenderar även barn- och utbildningsnämnden att:

- Säkerställa att det finns dokumenterade kontinuitetsplaner.

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential

2022-10-03
KPMG AB

Jenny Thörn	William Andréasson	Liz Gard
Kommunal revisor	Kommunal revisor	Certifierad kommunal revisor

© 2022 KPMG AB. All rights reserved.

Document classification: KPMG Confidential