Bodens kommun

Kommunrevisionen **2023-02-20**

För kännedom
Fullmäktiges presidium
Partiernas gruppledare

Till
Kommunstyrelsen
Socialnämnden
Samhällsbyggnadsnämnden
Miljö- och byggnadsnämnden
Kultur-, fritids och ungdomsnämnden
Överförmyndarnämnden
Arbetsmarknads- och utbildningsnämnden
Bodens Energi
Bodens Näringsfastigheter
Stiftelsen Bodenbo
Bodens Business Park

Granskning av hantering av IT-störning

På vårt uppdrag har sakkunniga från KPMG granskat rutinerna för att upprätthålla verksamheter vid större IT-störning. Uppdraget ingår i revisionsplanen för år 2022. Syftet med granskningen är att bedöma om kommunen har ändamålsenliga rutiner för att kunna upprätthålla verksamheter vid större IT-störningar.

Vår sammantagna bedömning är att kommunen *på nämndnivå* endast *delvis har ändamålsenliga rutiner* för att kunna upprätthålla verksamheter vid större IT-störningar. Det grundar sig i att skriftliga rutiner i de flesta fall helt saknas och i något fall delvis saknas.

Vår sammantagna bedömning gällande granskade *bolag/stiftelse* är att de *till övervägande del* har *ändamålsenliga rutiner* för att kunna upprätthålla verksamheter vid större IT-störningar. Det grundar sig i att skriftliga rutiner i ett fall helt saknas och i något fall delvis saknas.

Vår bedömning gällande de utvalda verksamhetsområdena i avsnitt 4 är att det inom samtliga områden finns en medvetenhet gällande IT-avbrott och dess eventuella konsekvenser och det finns också till övervägande del fungerande arbetssätt samt dokumentation i form av till exempel riktlinje eller checklista för vilka åtgärder som ska vidtas om ett IT-avbrott skulle inträffa.

Vi anser dock att det finns förbättringsområden och lämnar därför mot bakgrund av vår granskning följande rekommendationer:

- kommunstyrelsen, miljö- och byggnadsnämnden och samhällsbyggnadsnämnden, kultur-, fritids och ungdomsnämnden att säkerställa att det finns planering av hur verksamheternas väsentligaste uppgifter ska lösas vid eventuellt IT-avbrott.
- kommunstyrelsen, socialnämnden, miljö- och byggnadsnämnden, samhällsbyggnadsnämnden, kultur-, fritids och ungdomsnämnden, överförmyndarnämnden samt arbetsmarknads- och utbildningsnämnden att arbeta fram/färdigställa skriftliga riktlinjer/rutiner där det framgår hur arbetet inom de väsentligaste verksamhetsområdena ska bedrivas vid eventuellt IT-avbrott.

- Bodens Energi, Bodens Näringsfastigheter samt Stiftelsen Bodenbo att arbeta fram/färdigställa skriftliga riktlinjer/rutiner där det framgår hur arbetet inom de väsentligaste verksamhetsområdena ska bedrivas vid eventuellt IT-avbrott.

Revisorerna överlämnar härmed granskningsrapporten för kännedom och yttrande. Yttrande från kommunstyrelse, berörda nämnder samt bolag/stiftelse önskas senast den 30 april 2023.

För revisorerna i Bodens kommun

Per-Ulf Sandström Michael Sundberg

Bilaga Granskningsrapport ”Granskning av hantering av IT-störning”, KPMG, februari 2023.

Granskning av hantering av IT-störning

Revisionsrapport

Bodens kommun

KPMG AB

2023-02-20

Antal sidor 30

Antal bilagor 11

© 2023 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 Public

Innehållsförteckning

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

1 Sammanfattning

Vi har av Bodens kommuns revisorer fått i uppdrag att granska rutinerna för att upprätthålla verksamheter vid större IT-störning. Uppdraget ingår i revisionsplanen för år 2022. Syftet med granskningen är att bedöma om kommunen har ändamålsenliga rutiner för att kunna upprätthålla verksamheter vid större IT-störningar.

Vår sammantagna bedömning är att kommunen *på nämndnivå* endast *delvis har ändamålsenliga rutiner* för att kunna upprätthålla verksamheter vid större IT-störningar. Det grundar sig i att skriftliga rutiner i de flesta fall helt saknas och i något fall delvis saknas.

Vår sammantagna bedömning gällande granskade *bolag/stiftelse* är att de *till övervägande del* har *ändamålsenliga rutiner* för att kunna upprätthålla verksamheter vid större IT-störningar. Det grundar sig i att skriftliga rutiner i ett fall helt saknas och i något fall delvis saknas.

Vår bedömning gällande de utvalda verksamhetsområdena i avsnitt 4 är att det inom samtliga områden finns en medvetenhet gällande IT-avbrott och dess eventuella konsekvenser och det finns också till övervägande del fungerande arbetssätt samt dokumentation i form av till exempel riktlinje eller checklista för vilka åtgärder som ska vidtas om ett IT-avbrott skulle inträffa.

Vi anser dock att det finns förbättringsområden och lämnar därför mot bakgrund av vår granskning följande rekommendationer:

- kommunstyrelsen, miljö- och byggnadsnämnden och samhällsbyggnadsnämnden, kultur-, fritids och ungdomsnämnden att säkerställa att det finns planering av hur verksamheternas väsentligaste uppgifter ska lösas vid eventuellt IT-avbrott.
- kommunstyrelsen, socialnämnden, miljö- och byggnadsnämnden, samhällsbyggnadsnämnden, kultur-, fritids och ungdomsnämnden, överförmyndarnämnden samt arbetsmarknads- och utbildningsnämnden att arbeta fram/färdigställa skriftliga riktlinjer/rutiner där det framgår hur arbetet inom de väsentligaste verksamhetsområdena ska bedrivas vid eventuellt IT-avbrott.
- Bodens Energi, Bodens Näringsfastigheter samt Stiftelsen Bodenbo att arbeta fram/färdigställa skriftliga riktlinjer/rutiner där det framgår hur arbetet inom de väsentligaste verksamhetsområdena ska bedrivas vid eventuellt IT-avbrott.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

2 Bakgrund

Under 2021 kom ett antal IT-incidenter i fokus, detta i och med att det blev tydligt för medborgarna hur sårbart samhället är för större IT-störningar. Attacker mot både dagligvaruhandeln och Kalix kommun synliggjorde konsekvenserna av när IT-systemen slutar fungera.

Attacker mot samhällsviktig verksamhet är inget nytt, det pågår dygnet om alla dagar om året och mot en stor bredd av mål. I majoriteten av fallen så blir konsekvenserna inte synliga för medborgarna, men för olika aktörers IT-säkerhetsavdelningar innebär det stora påfrestningar.

Attackerna genomförs av olika aktörer och med olika motiv, allt i från nyfikenhet på om det går att genomföra en attack, till att bidra till att destabilisera demokratin och bidra till den gråzonsproblematik som vi befinner oss i.

IT-säkerheten blir därmed allt viktigare, men det blir också robustheten i organisationen. Hur klarar man sig utan för oss i vardagen till synes oumbärliga IT-system? Hur klarar vi att hantera allt från liv och hälsa till service för kommuninnevånarna?

Med anledning av ovanstående har kommunens revisorer dragit slutsatsen i sin riskanalys, att området behöver granskas. Uppdraget ingår i revisionsplanen för år 2022.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen är att bedöma om kommunen har ändamålsenliga rutiner för att kunna upprätthålla verksamheter vid större IT-störningar. Detta bedöms utifrån följande revisionsfrågor:

Granskningen utgår från följande områden:

- Har kommunen/berörd nämnd analyserat vilka verksamhetsområden som är kritiska vid ett IT- avbrott och om det finns en planering om hur uppgifterna ska lösas utan IT-stöd?
- Vi kommer även att bedöma om det finns lösningar för ett antal verksamhetsområden som revisionen bedömer är väsentliga såsom hemtjänst, utbetalning av försörjningsstöd och löner, mm
- Har det vid något tillfälle genomförts test av att de alternativa lösningarna fungerar?

Granskningen omfattar verksamheten i samtliga nämnder samt verksamheterna i de kommunala bolagen Bodens Energi, Bodens Business Park, Bodens Näringsfastigheter samt Stiftelsen Bodenbo.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

2.2 Revisionskriterier

Vi kommer att bedöma om rutinerna uppfyller:

- Kommunallagen 6 kap. 6 §
- Tillämpbara interna regelverk, policys och beslut

2.3 Metod

Granskningen har genomförts genom dokumentstudier av både centrala och förvaltningsspecifika styrdokument, checklistor samt mallar och processkartor.

Intervjuer har genomförts med verksamhetsföreträdare från kommunstyrelsen, socialnämnden, miljö- och byggnämnden, arbetsmarknads- och utbildningsnämnden, samhällsbyggnadsnämnden, kultur-, fritids- och ungdomsnämnden, överförmyndarnämnden samt för bolagen Bodens Energi, Bodens Business Park, Bodens Näringsfastigheter och slutligen med representant för Stiftelsen Bodenbo.

Företrädare för samtliga verksamhetsområden har beretts möjlighet att faktakontrollera rapporten.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

3 Resultat av granskningen

3.1 Styrande dokument

Bodens kommun har etablerat ett antal styrande dokument med beröring på granskningsområdet. Flertalet av dessa beskriver styrning av krisledning och säkerhetsarbete på en övergripande nivå och innehåller inte specifikt information gällande kriser med anledning av incidenter eller IT-störning och beredskap för dessa. Vi inkluderar dock dessa styrdokument med kortfattad beskrivning utan att genomföra vidare analys i denna rapport. Det finns även ett flertal mallar framtagna för att underlätta arbetet för medarbetarna.

Strategi för trygghet och säkerhet[1]

Det övergripande syftet med styrdokumentet är att upprätthålla och kvalitetssäkra trygghet- och säkerhetsprocesser i Bodens kommun, samt att säkerställa att gällande lagar och myndigheters krav följs. Styrdokumentet ska ge förutsättningar för en sammanhållen styrning och ledning och möjliggöra en uppföljning av inriktningsmål och delmål gällande Bodens trygghet och säkerhetsarbete. Bodens kommuns styrdokument för trygghet- och säkerhet utgör, enligt dokumentet, kommunfullmäktiges styrning av kommunens arbete inom trygghet och säkerhet för perioden 2020–2023. (se bilaga A)

Av styrdokumentet framgår hur kommunen ska arbeta inom prioriterade målområden. Arbetet med trygghet och säkerhet berör enligt dokumentet samtliga förvaltningar och kommunala bolag i olika utsträckning. Respektive förvaltning ska enligt dokumentet årligen och skriftligen rapportera de åtgärder som genomförts för att uppnå delmålen till ansvarig nämnd. Räddnings- och säkerhetsförvaltningen sammanställer en rapport till kommunstyrelsen senast 28 februari nästkommande år.

Enligt dokumentet har särskilt fokus för perioden 2020-2023 legat på cybersäkerhet, krisberedskap, informationssäkerhet, fysisk säkerhet, trygghet samt civilt försvar och säkerhetsskydd.

Policy för trygghet och säkerhet i Bodens kommun[2]

Syftet med policyn är att beskriva hur kommunens säkerhets- och trygghetsarbetet är organiserat för att stärka den gemensamma samordningen och förmågan inom området.

Policyn gäller för all verksamhet som kommunen ansvarar för och i tillämpliga delar även de kommunala bolag eller motsvarande som omfattas av företagspolicyn. Policyn tas fram av räddnings- och säkerhetsförvaltningen för beslut i kommunfullmäktige.

Räddnings- och säkerhetsförvaltningen ansvarar för att följa upp det samlade trygghet och säkerhetsarbete till kommunstyrelsen. Policyn ingår i den strategiska planen och som en del i kommunens kvalitetsarbete.

[1] Daterad 2019-10-17
[2] Daterad 2017-09-22.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

Risk och sårbarhetsanalys för Bodens kommun

Dokumentet redogör för kommunens samhällsviktiga verksamheter, kritiska beroenden, riskbild, sårbarheter och krisberedskapsförmåga. Framtagandet av risk- och sårbarhetsanalysen görs i enlighet med föreskrifterna MSBFS[3] 2015:5.

Kommunen har i samverkan med andra aktörer som verkar inom kommunens geografiska område tagit fram en riskbild utifrån sex kategorier; teknisk infrastruktur och försörjningssystem, sociala risker, naturolyckor och väderhändelser, olyckor, smittspridning samt information och kommunikation. Riskerna har bedömts utifrån sannolikhet och konsekvens. I dokumentet identifieras samhällsviktig verksamhet inom kommunens geografiska område och för att en verksamhet ska anses samhällsviktig ska ett av nedanstående två kriterier vara uppfyllda;

1. Bortfall eller svår störning i verksamheten kan på kort tid leda till en svår störning i samhället.
2. Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig samhällsstörning ska kunna hanteras med så få konsekvenser som möjligt.

Dokumentet innehåller även en riskidentifiering i kommunens förvaltningar fördelat på områdena tekniska försörjningssystem och infrastruktur, sociala risker, naturolyckor och väderhändelser, olyckor samt smittspridning. För de risker som är identifierade genomförs en riskanalys där sannolikhet och konsekvens bedöms.

Inom ramen för denna granskning är riskerna *Störningar i elektroniska kommunikationer Allvarliga informationsincidenter samt Cyberattack* aktuella. Sannolikheten att en störning kan inträffa bedöms som mycket hög medan konsekvenserna kan bli betydande.

Baserat på kommunens kritiska beroenden, genomförd riskanalys, bedömning av sårbarheter och brister i krishanteringsförmåga föreslås i slutet av dokumentet ett antal åtgärder för nuvarande mandatperiod.

- Utreda vilka kritiska system och lagring av data som kommunens samhällsviktiga verksamheter är beroende av under år 2020.
- Kompetenshöjande utbildning inom cybersäkerhet för nyckelpersoner inom kommunen.
- Identifiera kritiska beroenden till system och tjänster för informationshantering som är av central betydelse för kommunens verksamhet.
- Utreda behov och ta fram kostnadskalkyl för ett samlat incidenthanteringssystem som övervakar IT-incidenter i kommunens system som är kritiska beroenden för samhällsviktig verksamhet

[3] Myndigheten för samhällsskydd och beredskap (MSB)

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

Krisledningsplan för hantering av samhällsstörningar och extraordinära händelser

Syftet med kommunens *krisledningsplan for hantering av samhällsstörningar* är att säkerställa att kommunen har en god krishanteringsförmåga samt klargöra kommunens organisation, uppgifter och ansvarsförhållanden vid en samhällsstörning. Dokumentet är kommunövergripande och reglerar den kommunövergripande krishanteringen. Förvaltningarna ansvarar for att ta fram lokala krisledningsplaner.

Policy för informationssäkerhet[4]

Det övergripande syftet med policyn är enligt dokumentet att redovisa kommunfullmäktiges viljeinriktning och övergripande mål för informationssäkerheten i kommunen. Syftet är också att beskriva ansvar, roller och principer för informationssäkerhetsarbetet. Vidare gäller policyn för all verksamhet som kommunen ansvarar för och i tillämpliga delar även de kommunala bolag och all information oavsett om den finns i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system så handlar informationssäkerhet, enligt policyn, även om tekniska aspekter såsom exempelvis IT-utrustning, programvaror (IT-system) och nätverk. Enligt dokumentet ska policyn tas fram av informationssäkerhetssamordnaren och fastställas i kommunfullmäktige.

Efterlevnaden av informationssäkerhetspolicyn och andra styrande dokument inom informationssäkerhet ska enligt policyn följas upp regelbundet och bör revideras inom 3–5 år.

Rutin för informationssäkerhetsklassning[5]

Informationssäkerhetsklassning är en grundläggande komponent i informationssäkerhetsarbetet. Genom att klassa information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet skapar man förståelse för och kan styra vilket skydd som krävs för olika informationsmängder. Rutinen berör alla som ska genomföra en informationssäkerhetsklassning inom kommunen.

Rutin för riskanalys utifrån informationssäkerhet[6]

En risk definieras i rutinen som *en oönskad händelse som, om den inträffar, skadar vår information i olika konsekvensnivåer utifrån säkerhetsaspekterna tillgänglighet, riktighet och konfidentialitet*. Information är en viktig tillgång för kommunen och måste enligt rutinen hanteras säkert. Informationen kan vara talad, skriven, tryckt på papper eller elektroniskt/digital. Enligt rutinen ska det finnas rätt skydd på informationstillgångarna utifrån; informationen ska finnas när den behövs, informationen ska vara korrekt och inte manipulerad eller förstörd, och slutligen ska endast behöriga personer kunna ta del av informationen. Rutinen gäller för hela kommunen och berör alla som ska genomföra en riskanalys med utgångspunkt i informationssäkerhet. Informationssäkerhetssamordnaren är ansvarig för att rutinen

[4] Daterad 2018-11-22. Dnr 2018/1212
[5] Daterad 2020-03-05
[6] Daterad 2020-03-05

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

uppdateras vid behov och att rutinen kommuniceras ut. Enligt rutinen ska en riskanalys framför allt genomföras vid ny eller uppdatering av informationstillgång, om ny risk upptäcks, om nytt IT-stöd upphandlas/införs eller vid organisationsförändringar. Enligt rutinen finns mall för riskanalysen vilken ska användas samt sparas på hänvisad plats. Riskanalysunderlaget ska sparas i skyddad mapp. Därefter ska riskerna enligt rutinen bedömas och åtgärdsförslag ska tas fram samt ansvarig, datum för åtgärdens genomförande samt datum för uppföljning.

Informationssäkerhet – Modell för informationssäkerhetsklassning[7]

Modellens syfte är enligt dokumentet att hjälpa till att *”tänka på hur man värderar konsekvenser*” samt att ha en kommunövergripande bedömning för hur skyddsvärd information informationssäkerhetsklassas. Skyddsvärd information är enligt dokumentet sådan information som kommunen anser är värd att skydda med hänsyn taget till konsekvensen av vad skadan kan bli. Dokumentet riktar sig till samtliga anställda inom Bodens kommun.

Informationssäkerhet – Regler för användare[8]

Dokumentet riktar sig till samtliga anställda inom Bodens kommun och även externa användare som jobbar på uppdrag av kommunen och har användarbehörigheter till kommunens IT-system och som hanterar kommunens information. Enligt dokumentet är information en av kommunens viktigast tillgångar och för att skydda dessa krävs ett säkerhetsmedvetande. Dokumentet reglerar bland annat hantering av IT-utrustning, användning av sociala medier och internet samt E-post. Vidare har alla användare skyldighet att anmäla incidenter (avvikelser, fel eller brister) som misstänks medföra negativ påverkan på kommunens information. Det kan enligt dokumentet röra sig om tex: IT-angrepp/intrång, skadlig kod, oskyddad känslig information, stulen dator med mera.

Riktlinje för styrning av behörighet[9]

Enligt riktlinjen ska styrning av behörigheter säkerställa att endast behöriga har tillgång till information och lokaler och därmed förhindra att obehörigas ges åtkomst. Kraven på behörighet ska baseras på vilka arbetsuppgifter den anställda har, och behörighetprocessen ska ha tydliga vägar hur man söker behörighet, vem som beslutar, vem som genomför behörigheten och hur man avslutar behörighet. Varje förvaltning inom kommunen ska enligt riktlinjen tillse att det finns behörighetsägare för respektive område (IT-system, lagringsytor och kommunens lokaler). Riktlinjen definierar roller och ansvar gällande styrning av behörighet.

[7] Daterad 2019-01-31
[8] Daterad 2022-02-25
[9] Daterad 2019-02-20

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

Rutin för eskalering av incidenter i IT-miljön[10]

Rutinen syftar till att beskriva hur Bodens kommun eskalerar och hanterar informationssäkerhetsincidenter i IT-miljön där hanteringen behöver samordnas inom kommunen. Rutinen gäller för alla verksamheter inom kommunen.

Anmälan om incident kan komma från leverantör av IT-stöd, medborgare, medarbetare, elever och externa utförare. Incident manager (IM), en på IT-kontoret utsedd person som har ansvaret för incidenthanteringen, bedömer om incidenten är allvarligt och därigenom en prio 1. Om så är fallet bedömer IM tillsammans med säkerhetschef och/eller informationssäkerhetssamordnaren om incidenten ska eskaleras och att det ska sammankallas till ett avstämningsmöte. I de fall incidenten inte bedöms som är allvarlig men att det finns ett samordningsbehov, då kan incident manager kontakta säkerhetschef eller informationssäkerhetssamordnare för att få hjälp med samordning. När incidenten är löst ska enligt rutinen sammanställas i en publik incidentrapport där det ska framgå förutom beskrivning av incidenten, genomförda åtgärder samt framtida åtgärder.

Rutin för incidenter som faller under NIS-direktivet inom Bodens kommun[11]

En NIS-incident är en händelse med faktisk negativ inverkan på säkerheten i nätverk och informationssystem, där konsekvensen av incidenten innebär att den samhällsviktiga tjänsten inte levereras i förhållande till normalt tillhandahållande.

Inom Bodens kommun och kommunala bolag så är det enligt rutinen inom energiförsörjning, drickvattensförsörjning samt hälso- och sjukvård som berörs av NIS-direktivet. Incidenter inom dessa områden ska rapporteras till MSB. Enligt rutinen finns ett incidentrapporteringsverktyg på MSB:s webbsida som ska användas för att anmäla incidenter som faller under NIS. Varje förvaltning har fått en utsedd tjänsteperson som har tillgång till incidentrapporteringsverktyget.

Kontinuitetshantering

Vi har tagit del av en Power-Point presentation som redogör för vad kontinuitetshantering innebär. Det framkommer att det är viktigt att ”ha en plan B för din verksamhet”. Detta åstadkoms genom att;

- Kartlägga viktiga verksamheter och processer.
- Identifiera beroenden av resurser.
- Bestämma vad som är acceptabla avbrottstider.
- Genomföra åtgärder som minskar risken för störningar.
- Skapa planer för att hantera de störningar som ändå kan uppstå.

Genom att kartlägga, analysera och vidta åtgärder stärks förmågan att upprätthålla samhällsviktig verksamhet oavsett typ av störning. Enligt dokumentet ger arbete med

[10] Daterad 2020-02-26
[11] Daterat 2020-02-13

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

kontinuitetshantering även effekter såsom; *insikt om beroenden till andra aktörer*, *skapar underlag för kravställningen gentemot leverantörer*, *ger prioriteringsunderlag till riskreducerande och robusthöjande åtgärder*, *reducerar konsekvenserna av ett avbrott genom tex dokumenterade och övade reservrutiner* samt *ökad medvetenhet hos personal avseende risker och kritiska beroenden*. Det medföljer en mall som stöd för arbetet med kontinuitetshantering.

3.2 Hantering av större IT-störningar

Central nivå

I Bodens kommun ansvarar IT-enheten, som ligger organisatoriskt under Kommunledningsförvaltningen, för utveckling, support, förvaltning och drift av kommunens IT-miljö. I samband med omorganisationen beslutades att flytta all systemförvaltning till kommunledningsförvaltningens IT-enhet. Ett projekt för detta pågår där IT-enheten samtidigt inför ett metodstöd (PM3) för systemförvaltning. Projektet beräknas enligt verksamhetsföreträdare vara klart under 2023.

Enheten Demokrati, kommunikation och säkerhet (DKS) är direkt underställd kommunchef och tillhör organisatoriskt kommunledningsförvaltningen. Enheten har olika ansvarsområden; demokrati, kommunikation och säkerhet. Inom säkerhet så finns bl.a. områdena informationssäkerhet och krisberedskap, där samordnas arbetet med verksamheterna med målet att öka kommunens förmåga att hantera olika händelser, stora som små samt stärka skyddet av kommunens egendomar. Enheten ska se till att kommunens viktiga verksamheter fungerar, oavsett vad som inträffar i kommunen.”
Vid intervju med verksamhetsföreträdaren framkommer att det inte finns något sammanställt dokument med prioritetslista system för system för att starta i gång system efter ett större IT-avbrott. Verksamhetsföreträdarna lyfter att det har haft diskussioner med verksamheterna och att det finns en gruppering av systemen, nivå 1, 2 och 3 som anger viss prioriteringsordning. Verksamhetsföreträdarna anser att de har en bra bild av vilka system som bör prioriteras och startas i gång först.

Detta finns med i upphandling av externa systemleverantörer och dessa driftleverantörer vet därmed vilka system som är högst prioriterade vid ett eventuellt avbrott. Då utvecklingen idag går mot att antalet molntjänster ökar och är det viktigt enligt verksamhetsföreträdarna att detta framkommer vid upphandling. Tidigare fanns både system och information på servrar fysiskt placerade hos kommunen.

När felanmälningar gällande IT-störning kommer in till kundservice hanteras dessa av driftleverantören. Ärendena prioriteras mellan 1-5 med utgångspunkt i hur det påverkar verksamheten och hur angeläget systemet är. Grupperingarna hanteras både med olika återkopplings- och hanteringstider. Ett ärende kan till exempel få en prio 3 inledningsvis men om det ringer in fler med samma problem så prioriteras ärendet om.

Incidentrapporter tas slutligen fram enligt en mall. Incidentrapporten är enligt verksamhetsföreträdarna en sammanställning på vad som hänt, konsekvensbedömning,

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

om det hänt tidigare, vad som löste incidenten, loggning på händelseförloppet, om det är en personuppgiftsincident, framtida åtgärder, framgångsfaktorer och om det rapporterats in till andra myndigheter (ex. IMY, MSB, Polisen).
Innan pandemin hade DKS påbörjat ett övergripande arbete gällande kontinuitetsplaneringen vilket dock fick stå tillbaka när pandemin bröt ut. Arbetet har återupptagits och ett stödpaket har tagits fram vilket i närtid kommer att presenteras för kommunledningsgruppen. Verksamhetsföreträdarna känner till att vissa verksamheter påbörjat, och en del har kommit ganska långt, gällande kontinuitetshantering men att vissa verksamheter inte påbörjat arbetet. Det pågående arbetet med kontinuitetshantering innehåller enligt verksamhetsföreträdarna förslag till ramverk med process och mål för perioden 2023-2028 där verksamheterna ska ha fastställda kontinuitetsplaner för prioriterade samhällsviktiga verksamheter utifrån scenario totalt IT-avbrott. Ansvariga för samhällsviktig verksamhet ska också fastställt en rutin (identifiera nya kritiska resurser, följa upp, revidera) och ha infört ett systematiskt arbetssätt för kontinuitetshantering.”

Bodens kommun är tillsammans med övriga 13 kommuner i Norrbotten anslutna till en gemensam datacenterlösning via det gemensamma regionala fibernätet. Satsningen ska enligt verksamhetsföreträdarna höja säkerheten och tillgängligheten samt minska sårbarheten. En stor del av IT-infrastrukturen är idag redundant genom samarbetet med IT-Norrbotten (Polarix regionnät och internetförbindelse) och e-Nämnden (DCBD). Det gäller exempelvis kommunikationsvägar mellan kommunen och DCBD, brandväggar, centrala routerfunktioner, internetåtkomst, servermiljö, lagring och backup. I samband med migreringen till DCBD genomfördes tester av redundansen för att säkerställa tillgänglighet och robusthet genom att simulera avbrott på fiber, bortfall av brandväggsnoder och router.

Enligt verksamhetsföreträdarna så har mindre test genomförts vid några skarpa tillfällen dock endast avbrott i enstaka program/tjänster. Pandemin har medfört att medarbetarna övat på att nå varandra. Oavsett typ av störningen så ska medarbetarna känna sig trygga i att kommunikationen fungerar.

Bedömning

Vår bedömning är att intervjuade centrala tjänstepersoner har kännedom om och följer styrande dokument såsom *Rutin för eskalering av incidenter i IT-miljö*.

3.3 Kritiska verksamhetsområden vid IT-avbrott

Informationen från respektive nämnd och bolag/stiftelse återfinns i bilagor enligt nedanstående hänvisningar. Bilagorna omfattas av sekretess enlig OSL kap 18 §13.

Kommunstyrelsen

Se bilaga B

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

Socialnämnden

Se bilaga C

Miljö och byggnämnden/ Samhällsbyggnadsnämnden

Se bilaga D

Kultur-, fritids- och ungdomsnämnden

Se bilaga E

Arbetsmarknads- och utbildningsnämnden

Se bilaga F

Överförmyndarnämnden

Se bilaga G

Bodens Energi

Se bilaga H

Bodens Business Park

Se bilaga I

Bodens Näringsfastigheter

Se bilaga J

Stiftelsen Bodenbo

Se bilaga K

3.3.1 Bedömning

Vi bedömer att det inom verksamheterna organiserade under kommunstyrelsen har påbörjats kartläggning och riskanalys gällande områden som anses kritiska kopplat till IT-störning. Verksamhetsområdena har kommit olika långt och så vitt vi kan bedöma finns fortfarande ett arbete kvar att göra inom samtliga verksamhetsområden inom kommunledningsförvaltningen. Vi anser att det till exempel saknas skriftliga rutiner för hur arbetet ska genomföras i avsaknad av IT-stöd.

Vi bedömer att det inom socialnämndens verksamhetsområden har genomförts en analys av vilka verksamhetsområden som är kritiska. Det finns också krishanteringspärmar framtagna för de olika verksamhetsområdena där kritiska aktiviteter finns noterade samt eventuella åtgärder för att kunna hantera verksamheten vid någon form av störning. Överlag är vår bedömning att arbetet har kommit långt inom socialnämndens verksamheter och inom några verksamheter finns kontinuitetsplaner och rutiner framtagna fullt ut.

Vi konstaterar att det inom miljö- och byggnämnden samt samhällsbyggnadsnämndens verksamhetsområden inte har genomförts någon riskanalys och att prioriteringsordning för hur de olika systemens ska prioriteras vid ett återställande saknas. Det saknas också

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

skriftliga rutiner för hur förvaltningen ska arbeta vid it-avbrott samt hur information från verksamhetsområden ska nå ut till medborgarna om något av systemen ligger nere en längre tid.

Vi konstaterar att det inom arbetsmarknads- och utbildningsnämndens verksamhetsområden har analyserats och identifierats områden som anses vara kritiska kopplat till IT-störning. Informations- och säkerhetsdokumentation har sammanställts däremot saknas dokumenterade rutiner för verksamheten. Krishanteringspärm finns framtagen och varje enskild enhet har enligt verksamhetsföreträdarna denna kontroll. Däremot saknas en övergripande kontroll och uppföljning inom området.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

4 Andra väsentliga områden

4.1 Verksamhetsområden

I detta avsnitt bedöms huruvida det finns lösningar för ett antal verksamhetsområden som revisionen bedömer är väsentliga att granskning med anledning av IT-störningar. Informationen från respektive verksamhetsområde återfinns i bilagor enligt nedanstående hänvisningar. Bilagorna omfattas av sekretess enlig OSL kap 18 §13.

Äldreomsorg/Hemtjänsten

Se bilaga C

Kostverksamheten

Se bilaga F

Läkemedelshantering

Se bilaga C

Trygghetslarm

Se bilaga C

Försörjningsstöd

Se bilaga C

4.1.1 Bedömning – andra väsentliga områden

Vår bedömning gällande de utvalda verksamhetsområdena ovan är att det inom samtliga områden finns en medvetenhet gällande IT-avbrott och dess eventuella konsekvenser och det finns också till övervägande del fungerande arbetssätt samt dokumentation i form av till exempel riktlinje eller checklista för vilka åtgärder som ska vidtas om ett IT-avbrott skulle inträffa.

5 Slutsats och rekommendationer

Vår bedömning är att det hos samtliga intervjuade verksamheter finns en medvetenhet gällande IT-avbrott och dess eventuella konsekvenser. Det finns också mer eller mindre fungerande arbetssätt, om än inte alltid dokumenterade, om ett IT-avbrott skulle inträffa.

Vår sammantagna bedömning är dock att kommunen *på nämndnivå* endast *delvis har ändamålsenliga rutiner* för att kunna upprätthålla verksamheter vid större IT-störningar. Det grundar sig i att skriftliga rutiner i de flesta fall helt saknas och i något fall delvis saknas, se tabell nedan.

Vår sammantagna bedömning gällande granskade *bolag/stiftelse* är att de *till övervägande del* har *ändamålsenliga rutiner* för att kunna upprätthålla verksamheter vid större IT-störningar. Det grundar sig i att skriftliga rutiner i ett fall helt saknas och i något fall delvis saknas, se tabell nedan.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

Nedanstående tabell sammanfattas bedömningen av verksamheter per nämndområde samt för de bolag/stiftelse som blivit intervjuade och/eller granskade ur ett IT-störningsperspektiv. Grön =ja, Gul = delvis, Röd = nej.

Verksamheter	Finns medvetenhet om avbrott och dess konsekvenser?	Finns fungerande arbetssätt om störningar inträffar?	Finns förvaltnings-/bolagsspecifika rutiner?	Samman-tagen bedömning
Kommunstyrelsen				
Ekonomi				
HR/Lön				
Kansli- och service				
Socialnämnden				
Miljö- och byggn samt samhällsbyggn				
Kultur-, fritids- och ungdomsnämnd				
Arbetsmarknad- och utbildningsnämnd				
Överförmyndarnämnd				
Bodens Energi				
Bodens Business park				
Bodens Närings-fastigheter				
Stiftelsen Bodenbo				

Vår bedömning gällande de utvalda verksamhetsområdena i avsnitt 4 är att det inom samtliga områden finns en medvetenhet gällande IT-avbrott och dess eventuella konsekvenser och det finns också till övervägande del fungerande arbetssätt samt dokumentation i form av till exempel riktlinje eller checklista för vilka åtgärder som ska vidtas om ett IT-avbrott skulle inträffa. Nedanstående tabell sammanfattar bedömningen av utvalda verksamheter som blivit intervjuade och/eller granskade ur ett IT-störningsperspektiv. Grön =ja, Gul = delvis, Röd = nej.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

Verksamheter	Finns medvetenhet om avbrott och dess konsekvenser?	Finns fungerande arbetssätt om störningar inträffar?	Finns förvaltningsspecifika rutiner?	Samman-tagen bedömning
Äldreomsorg/ hemtjänst				
Kostverksamhet				
Läkemedelshantering				
Trygghetslarm				
Försörjningsstöd				

Utifrån vår bedömning och slutsats rekommenderar vi;

- kommunstyrelsen, miljö- och byggnadsnämnden, kultur-, fritids och ungdomsnämnden och samhällsbyggnadsnämnden att säkerställa att det finns planering av hur verksamheternas väsentligaste uppgifter ska lösas vid eventuellt IT-avbrott.
- kommunstyrelsen, socialnämnden, miljö- och byggnadsnämnden, kultur-, fritids och ungdomsnämnden, samhällsbyggnadsnämnden, överförmyndarnämnden samt arbetsmarknads- och utbildningsnämnden att arbeta fram/färdigställa skriftliga riktlinjer/rutiner där det framgår hur arbetet inom de väsentligaste verksamhetsområdena ska bedrivas vid eventuellt IT-avbrott.
- Bodens Energi, Bodens Näringsfastigheter samt Stiftelsen Bodenbo att arbeta fram/färdigställa skriftliga riktlinjer/rutiner där det framgår hur arbetet inom de väsentligaste verksamhetsområdena ska bedrivas vid eventuellt IT-avbrott.

Datum som ovan

KPMG AB

Eva Henriksson
Certifierad kommunal revisor

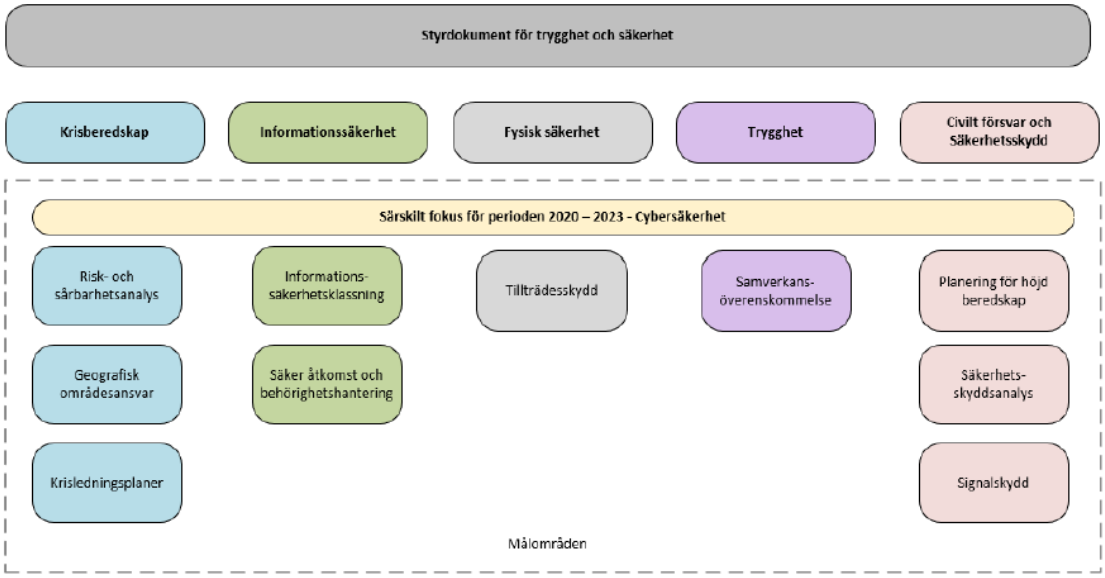
Christopher Karlsson
Kommunal revisor

Detta dokument har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.

© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public

A Bilagor



© 2023 KPMG AB. All rights reserved.

Document classification: KPMG Public