www.pwc.se

Revisionsrapport

Cybersäkerhet – övergripande granskning

Ljusdals kommun

Robert Bergman
Fredrika Jönander

December 2018

pwc

Innehåll

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Ljusdals kommun har PwC granskat om kommunstyrelsen har säkerställt att den interna kontrollen avseende kommunens cybersäkerhet är tillräcklig. Granskningen har skett utifrån NIST-ramverket som belyser organisationers mognadsgrad och förmågor inom följande fem kategorier;

Identifiera - Skydda – Upptäcka – Respondera - Återställa

Utifrån genomförd granskning är vår sammanfattade revisionella bedömning att den interna kontrollen avseende kommunens cybersäkerhet är bristande. Bedömningen baseras bl.a. på följande iakttagelser:

- Det har nyligen anställts en säkerhetssamordnare som kommer arbeta med bland annat IT- och informationssäkerhet.
- Det saknas genomgående aktuell och ändamålsenlig dokumentation i form av planer, policys, rutiner, instruktioner och processer. De planer som finns är inte implementerade i kommunen.
- Arbetet med identifiering av risker, riskbedömningar och riskhantering samt systemöversikt för att identifiera brister i IT-säkerheten behöver utvecklas.
- Informella arbetssätt inom organisationen medför att arbetet inte bedrivs på ett systematiskt eller enhetligt sätt.
- Roll- och ansvarsfördelning när det gäller hantering av incidenter är ett område som behöver utvecklas och dokumenteras.

Utifrån genomförd granskning och vår sammanfattande bedömning lämnar vi följande rekommendationer till kommunstyrelsen i syfte att utveckla verksamheten.

- Kommunstyrelsen säkerställer att planer uppdateras/revideras samt kompletteras med rutiner, instruktioner och riskbedömningar för att utveckla hur informationssäkerhetsarbete ska bedrivas. Risker/hot kopplat till information- och IT-säkerhet samt kontinuitetsplanering bör särskilt beaktas i kommunens kommande risk- och sårbarhetsanalys avseende mandatperioden 2019-2022.
- I syfte att öka förmågan att upptäcka avvikelser behöver kommunstyrelsen säkerställa att identifiering och rapportering av risker i kommunens IT-miljö utvecklas. IT-system med hög driftsäkerhet och starkt skydd mot externa attacker är av mycket stor vikt för säkerheten i samhället och för möjligheterna att hantera olika krisförlopp.
- Kommunstyrelsen säkerställer att övningar och utbildningar genomförs i syfte att öka kännedomen kring kommunövergripande styrning/ramverk för informationssäkerhet samt för IT-säkerhet. Övningar och utbildningar kan med fördel även syfta till att öka verksamheternas/användarnas kännedom om vilka risker som finns kopplat till användning av IT.

1. Inledning

1.1. Bakgrund

Kommunens revisorer har med hänsyn till risk och väsentlighet bedömt det angeläget att göra en granskning inom ovan rubricerat område.

All kommunal verksamhet bedrivs idag med IT-stöd. Det är därför av stor vikt att IT-stödet är driftssäkert. Kommunernas förtroende och verksamhet står inför stora utmaningar i samband med att cyberrelaterade incidenter ökar kraftigt, medan arbetet med att stärka cybersäkerhetsförmågan ofta står stilla.

Medborgarna kommer framöver kräva allt fler digitala lösningar från sina kommuner, tillgänglighet är a och o i dagens samhälle, samtidigt som toleransen för otillgänglighet och avbrott minskar.

Revisionsobjekt i granskningen är kommunstyrelsen.

1.2. Syfte och revisionsfråga

Revisorernas uppdrag regleras i kommunallagen kapitel 9. Granskningen ska besvara följande revisionsfråga: *Har kommunstyrelsen säkerställt att den interna kontrollen avseende kommunens cybersäkerhet är tillräcklig?*

Granskningen fokuserar på processer, personal och teknik inom granskningsområdet utifrån följande kategorier:

- *Identifiera*: Fokus på IT-tillgångar, processer och policy, styrning, riskanalys och riskhanteringsstrategi
- *Skydda*: Fokus på behörighetskontroll, utbildning och övning, IT-/dataskydd, informationssäkerhet, förvaltning och tekniskt skydd
- *Upptäcka*: Fokus på anomalier/händelser, kontinuerlig övervakning och processer att upptäcka händelser
- *Respondera/Agera*: Fokus på incidenthantering, incidentrespondering, krishantering/kommunikation, analys, IT-incidenthantering och erfarenhetsåterföring
- *Återställa*: Fokus på kontinuitetsplanering, avbrottsplanering, erfarenhetsåterföring och varumärkesskydd

Revisionskriterier i denna granskning utgörs av kommunallagen 6 kap § 6 samt kommuninterna styrdokument som rör granskningsområdet. I övrigt hänvisas till ovan fem kontrollområden.

1.3. Avgränsning och metod

I tid avgränsas granskningen i huvudsak till år 2018. I övrigt hänvisas till syfte, revisionsfråga och granskningens fem kontrollområden.

Kommunens övergripande IT- och informationssäkerhetsmognad har granskats utifrån vissa anpassade funktioner ur ramverket NIST Cyber Security Framework samt PwC *best practice* och referensdata. Granskningens resultat ger en bild om vilka förmågor som är mer respektive mindre mogna inom kommunen, vilket skapar förutsättningar för planering, prioritering och utveckling av området. Granskningen inkluderar även en benchmark mot andra liknande verksamheter, vilket ger ytterligare en dimension om hur pass mogen kommunen är jämfört med andra.

Bedömningen av NIST-ramverkets fem kontrollområden sker i förhållande till vad som anses vara adekvat mognadsnivå för organisationen och dess förutsättningar. Rimlig mognadsnivå för en organisation som Ljusdals kommun är låg-medel (2) på en 4-gradig skala. Detta mot bakgrund av att det, i jämförelse med exempelvis bankinstitut, inte finns samma höga krav på cybersäkerhet.

Granskningen genomförs genom analys av för granskningen relevant dokumentation samt två workshops. Den ena workshopen genomfördes med kommunchefens ledningsgrupp inklusive bl.a. förvaltningschefer, personalchef, ekonomichef samt kommunens säkerhetschef. Den andra genomfördes med IT-chef och tekniker. Samtliga som varit med vid respektive workshop har fått möjlighet att sakgranska rapporten.

2. *NIST Cyber Security Framework*

NIST cybersäkerhetsramverket omfattar en riskbaserad sammanställning av riktlinjer som syftar till att hjälpa organisationer att identifiera, genomföra och förbättra säkerhetspraxis och skapa ett gemensamt språk för intern och extern kommunikation av säkerhetsproblem. Ramverket är en repetitiv process utformad för att utvecklas i synkronisering med förändringar när det kommer till säkerhetshot, processer och lösningar. Som ett resultat av detta skapar ramverket förutsättningar för en effektiv och dynamisk säkerhetsloop som inkluderar alltifrån hot till lösningar. Ramverket introducerar inga nya standarder eller koncept, snarare integrerar det redan etablerade standarder[1] och praxis. Ramverket består vidare av fem funktioner; *Identify, Protect, Detect, Respond* och *Recover*.

Ramverket tillhandahåller en utvärdering av mekanismer som möjliggör för verksamheten att bestämma dess nuvarande cybersäkerhetsförmåga, sätta individuella mål och etablera en plan för åtgärder och upprätthållandet av cybersäkerhetsprogram. Implementationsnivåerna bidrar till att skapa en kontext vilken möjliggör för organisationen att förstå hur dess nuvarande säkerhet och riskhanteringsförmåga ser ut i förhållande till andra aktörer i samma bransch. Nivåerna (som beskrivs nedan), varierar mellan 1 – 4, där 1 indikerar att medvetenheten om risker är låg, medan 4 indikerar att processer och program har etablerats och blivit väl implementerade i verksamheten. Organisationer rekommenderas att sträva mot att uppnå nivå 3 eller 4.

Nivåer av mognad kopplad till cybersäkerhet

Nivå 1	Låg	Ad hoc riskhantering. Låg riskmedvetenhet, inget samarbete med andra organisationer.
Nivå 2	Låg-medel	Riskhanteringsprocesser och riskhanteringsprogram är etablerade men är inte integrerade i hela organisationen. Organisationen har insett värdet av samarbete men saknar formella förmågor.
Nivå 3	Medel-hög	Formella policys för riskhanteringsprocesser och riskhanteringsprogram är integrerade genom hela organisationen. Visst samarbete med externa organisationer sker.
Nivå 4	Hög	Riskhanteringsprocesser och riskhanteringsprogram baseras på erfarenhetsåterföring och utgör en del av organisationskulturen. Ett proaktivt samarbete med andra organisationer äger rum.

[1] Exempel på standarder och ramverk; COBIT, ISO, ISA.

3. Iakttagelser och bedömningar

3.1. Roller och ansvar

Kommunstyrelsen ansvarsområden regleras främst i reglementen. Utifrån ett cybersäkerhetsperspektiv kan vi konstatera följande ansvar och roller för kommunstyrelsen:

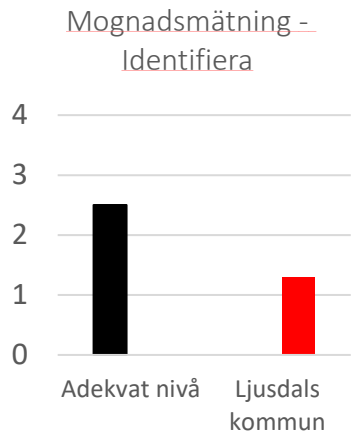
Kommunstyrelsen	• Har huvudansvaret för säkerhetsarbetet. Till kommunstyrelsens hjälp finns Ljusdals kommuns koncernledningsgrupp (KLG) som leds av kommunchef. Varje förvaltning och kommunalt bolag ansvarar sedan för säkerhetsarbetet inom sitt område enligt lagen om skydd mot olyckor och lagen om extraordinära händelser. • Bereder ärenden till kommunfullmäktige, leder och samordnar kommunens olika verksamheter, ansvarar för kommunens ekonomi och verkställer kommunfullmäktiges beslut. • Har övergripande ansvar och samordning av IT. Beställare och ägare av gemensamma system samt ansvarar för utveckling av handlingsplaner för gemensamma system. • Fattar beslut i kommunövergripande IT-frågor.

3.2. *Identifiera*

Identifiera, omfattar Ljusdals kommuns förmåga att identifiera kritiska informationstillgångar och data, det nuvarande läget för styrning och övergripande riskhantering när det kommer till cybersäkerhet. Som ett led i detta har granskningen bland annat sett till vilka processer som finns kopplade till riskhantering samt klassificering av tillgångar. Nedan redovisas iakttagelser och bedömning av mognad/förmåga som vi har gjort i samband med workshops och genomgång av relevanta underlag.

3.2.1. *Iakttagelser - Identifiera*

Granskningen visar att kommunens generella mognadsgrad för området *identifiera* uppgår till mognadsnivå 1,3 (låg) på en 4-gradig skala. Adekvat nivå för området är 2,5. Till grund för denna bedömning är följande iakttagelser:



- Inventering sker av både hård- och mjukvara. Processen är samma för all uppkopplad mjukvara och hårdvara. Inventeringsprocesserna sker ad hoc, t.ex. vid förnyelse av licenser. Inventeringsprocessen sköts med hjälp av systemet Alitris. Den inkomna informationen hanteras inte på ett strukturerat eller formaliserat sätt.
- Det är IT-enheten som kollektivt är ansvariga för kommunens system, det genomförs dock inte inventeringar av samtliga system. Inventeringen är till stor del automatiserad och sker ungefär en gång i månaden.
- Det sker ingen prioritering av tillgångar. En prioriteringsordning har efterfrågats och det finns en medvetenhet kring vikten av det inom kommunledningen. Vidare konstateras att det saknas rutiner och dokumentation för prioritering av tillgångar. Det finns ingen formell process för att klassificera och prioritera tillgångar.
- I dagsläget uppfyller inte Ljusdals kommun de krav som ställs i GDPR, men det är ett pågående arbete i respektive förvaltning. Det finns ingen strategi i form av riktlinjer, men det sker en inventering av personuppgiftsbehandlingar samt utbildningar för personal. Det har även anställts ett externt dataskyddsombud som håller i utbildningar.
- Det saknas formella processer för riskhantering. Riskinventeringar sker endast i begränsad utsträckning och det saknas även rutiner hur och när dessa ska ske.
- Brandväggar och antivirusskydd ger viss bild av hot som organisationen utsätts för. Det sker dock ingen dokumentation/sammanställning av hotbilden. Antivirus ställer in sig automatiskt när det finns en större hotbild och det är överlag mycket som är automatiserat.

I sammanhanget noteras att Ljusdals kommun har anställt en säkerhetschef som bland annat har till uppgift att förbättra informationssäkerhet, skapa policys samt arbeta med krishantering och krisberedskap samt att det finns en funktion i kommunens ledningsgrupp som arbetar med strategiska delar av IT. Det finns ett stort behov av uppdatering och revidering av befintliga planer och även kompletterande dokumentation. Det har

skapats en samhällsövergripande risk- och sårbarhetsanalys, men arbetet med sårbarheter sker på verksamhetsnivå snarare än på strategisk nivå/ledningsnivå. Undantag från detta råder för GDPR.

De förbättringsområden som vi har konstaterat i denna granskning är följande:

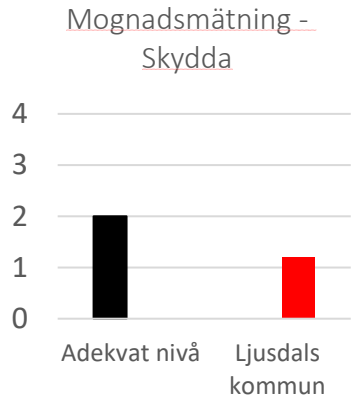
- Befintlig dokumentation bör uppdateras och revideras för att säkerställa att den är aktuell och tillämpar. Dokumentationen behöver sedan implementeras i verksamheten
- Grundläggande säkerhetsdokumentation behöver uppdaterats, fördelaktligen efter en ny risk- och sårbarhetsanalys eller en konsekvensanalys som fokuserar mer på IT och informationssäkerhet.
- Det behöver tas fram en rutin för att klassa information för att därefter skapa en prioriteringsordning för befintliga system. Fokus bör ligga på kritiskhet och kartläggning av information. Genomlysningen bör efterföljas av planarbete hur driften av kommunens mest kritiska system säkerställs.
- Granskningen visar på att det finns en låg medvetenhet kring ramverksuppbyggnaden inom kommunen. Användare skulle med fördel informeras om, och utbildas i de policys, regelverk och andra styrdokument som finns inom kommunen.

3.3. Skydda

Området *Skydda* fokuserar på kommunens nuvarande förmåga att skydda kommunens information samt avskräcka från hot. Denna kategori inbegriper även förmågan att hantera behörighetskonton samt säkerhet kopplad till data. Nedan redovisas iakttagelser och bedömning av mognad/förmåga som vi har gjort i samband med workshops och genomgång av relevanta underlag.

3.3.1. Iakttagelser - Skydda

Granskningen visar att kommunens generella mognadsgrad för området *skydda* uppgår till 1,2. Adekvat nivå för området är 2,0. Till grund för bedömningen ligger följande iakttagelser:



- Standardbehörighet saknas och behörighetsförändringar sker ad hoc. Det saknas även ett enhetligt och systematiserat arbetssätt kring behörighetshantering. Identitets- och accesshantering sker väldigt informellt och är i hög grad personberoende. Rutinen är dock att närmsta chef ska godkänner behörigheten som ska tilldelas användaren. Vidare konstateras att det saknas rutiner för gallring och radering av behörighet.
- Passersystem används för begränsning av fysisk åtkomst. Detta testas sporadiskt.
- Den nu gällande IT-strategin är inte implementerad i IT-verksamheten.
- Det genomförs inga säkerhetsutbildningar, inte heller några introduktionsutbildningar. Det finns inget utbildningsprogram för säkerhetsmedvetande. Däremot går chefer igenom övergripande riktlinjer.
- Forum på ledningsnivå finns som diskuterar IT-frågor. Strategier för att skydda information och tillgångar diskuteras däremot inte i detta forum.
- Det tillämpas nätverkssegregering för att skydda nätverkets integritet och riktighet. IT har inte fått några direktiv angående kontroller för att skydda data ”in transit” då dessa typer av frågor inte diskuteras på ledningsnivå.
- Säkerställande av medvetenhet kring cybersäkerhetsrelaterade roller och ansvar ser olika ut beroende på verksamhetsområde. Om något inte fungerar i informationshanteringen rapporteras avvikelser till ledning där det revideras.
- Säkerhetskopiering sker regelbundet efter bedömning av IT-enheten. Säkerhetskopieringarna testas inte mer än sporadiskt.
- För att skydda organisationen mot dataläckor sker övervakning av vissa klienter och via virusskydd.
- Standard images används för att lägga till systemapplikationer. Översyn av konfigureringar sker ad hoc då det saknas rutiner för detta, dock görs det ungefär en gång i månaden.

- Sårbarhetsplan och sårbarhetsanalys anses vara ett utvecklingsområde då sårbarhetsscanningar inge genomförs. Loggar förs, men detta sköts manuellt. Logghantering är något som är under arbete och målet är att det automatiskt ska flagga vid anomalier/avvikelser. Det är IT-enheten som granskar loggarna vid behov och inte enligt rutin.

I sammanhanget noteras att det även brister när det kommer till skydd av befintlig/liggande data hos mobila enheter samt skydd mot dataläckor, något som IT på eget initiativ har påbörjat arbete för att åtgärda.

De förbättringsområden som vi har konstaterat i denna granskning är bl.a. följande:

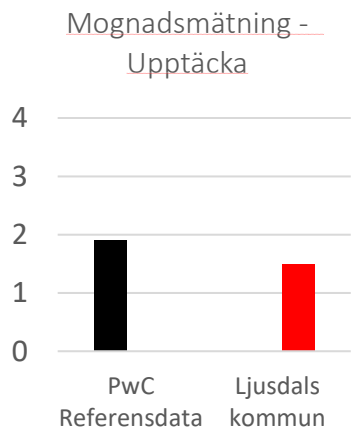
- Arbetet med IT-säkerhet har i låg utsträckning formaliserats, däribland styrning av hur utrustning ska hanteras på ett säkert sätt. Granskningen visar att det finns en säkerhetsplan-IT, en informationsplan för extraordinära händelser samt en IT-strategi. Denna dokumentation är dock i stort behov av uppdatering och komplettering. Kommunen saknar även kontinuitetsplaner.
- Det saknas ett implementerat program för obligatorisk säkerhetsutbildning. Det saknas även regelbundna övningar med fokus på informations- och cybersäkerhetsrelaterade scenarion.
- Penetrationstester och sårbarhetsscanning genomförs inte i den utsträckning som anses adekvat.
- I och med den relativt slimmade IT-organisationen finns en risk för nyckelpersonsberoende.

3.4. Upptäcka

Upptäcka, inkluderar bland annat Ljusdals kommuns förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverksövervakning, sökning efter skadlig kod och sårbarheter. Nedan redovisas iakttagelser och bedömning av mognad/förmåga som vi har gjort i samband med workshops och genomgång av relevanta underlag.

3.4.1. Iakttagelser - Upptäcka

Granskningen visar att kommunens generella mognadsgrad för området *upptäcka* uppgår till 1,5. Adekvat nivå för området är 1,9. Till grund för bedömningen ligger följande iakttagelser:



- Viss förmåga att upptäcka anomalier och händelser finns. *Network operations* tillämpas för att upptäcka anomalier gällande nätverksbelastning. Detta är dock inte systematiserat och sker ad hoc och inte i nivå med vad som ses som *god praxis*.
- Implementerade rutiner för risk och hot saknas, vilket gör det svårt att skapa en god förmåga att upptäcka händelser.
- Upptäckta händelser analyseras ad hoc när det kommer till att skapa förståelse för attackers mål och metod. Processen är informell och dokumenteras inte.
- Det finns inte fastställda rutiner för incidentrapportering. Utvärdering av tröskelvärden sköts muntligt och är inte formaliserat.

I sammanhanget noteras att anställdas aktiviteter till viss del övervakas i syfte att upptäcka cybersäkerhetshot. Granskning, av t.ex loggar, sker dock sporadiskt. Rutiner för hur uppföljning och analys ska ske saknas. Sökningar på loggar sker när det föreligger misstanke om brott.

De förbättringsområden som vi kan konstatera är bl.a. följande:

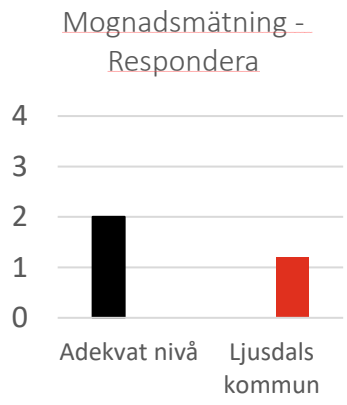
- Dokumenterad styrning inom händelsedetektering saknas, dvs. vad som utgör en incident, vilket innebär att arbetet genomförs ad hoc. Detta kan leda till att händelser inte klassas som incidenter förrän de redan utvecklats till än, vilket innebär att arbetet blir reaktivt snarare än proaktivt. Det saknas även definitioner på krav för händelsedetektering, inklusive krav på efterlevnad av legala krav och regleringar.
- Intrusion Prevention System (IPS) eller Intrusion Detection System (IDS) tillämpas inte, vilket bland annat innebär att kommunen saknar möjlighet att övervaka trafik internt.
- Det sker ingen dokumentation eller kommunikation från IT till verksamheten vid en upptäckt händelse, det genomförs inte heller någon konsekvensanalys i efterhand.

3.5. Respondera/Agera

Respondera syftar till Ljusdals kommuns rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat kriminalteknisk undersökning (forensik) och incidenthantering. Nedan redovisas iakttagelser och bedömning av mognad/förmåga som vi har gjort i samband med workshops och genomgång av relevanta underlag.

3.5.1. Iakttagelser – Respondera/Agera

Granskningen visar att kommunens generella mognadsgrad för området *respondera* uppgår till 1,2. Adekvat nivå för området är 2,0. Till grund för bedömningen ligger följande iakttagelser:



- Dokumenterad incidenthanteringsplan samt definition på vad som utgör en incident saknas. Även tydlig dokumenterad rollbeskrivning, i syfte att klargöra t.ex roller eller ordning för åtgärder, saknas.
- Vid misstanke om brott har IT historiskt gått in och till viss del bedrivit forensik för att därefter återrapportera till den chef som efterfrågat analysen. Detta kan endast efterfrågas av förvaltningschef. Det finns dock ingen dokumenterad ordning för hur detta skall göras och Ljusdals kommun har inte använt forensik mer än ett fåtal gånger. Vanligtvis kontaktas Polisen direkt och då involveras inte IT-avdelningen.
- Strategi för vilka åtgärder som ska vidtas för att mitigera/hindra incidenter saknas. Beslut för åtgärder fattas på plats beroende på situation och händelse. De informella åtgärdsstrategier som finns följs inte upp eller granskas på ett systematiskt sätt.
- IT-enheten har kontaktpersoner för att effektivt kunna få ut viktig information.

I sammanhanget noteras att kommunens låga mognadsnivå, i förhållande till adekvat nivå för området, beror främst på att det saknas dokumenterade riktlinjer som bland annat definierar en incident. Trots att det saknas formaliserade processer finns det en operativ förmåga att svara på incidenter. Det finns en medvetenhet kring vikten av utvärderingar och identifiering av lärdomar, däremot genomförs inte detta arbete på ett strukturerat sätt i dagsläget. IT-enheten reviderar och uppdaterar interna processer när de anser att de inte fungerar och tester genomförs ad hoc i samband med framtagning av nya processer. Incidenthanteringen är i hög grad händelsestyrd.

De förbättringsområden som vi kan konstatera är bl.a. följande:

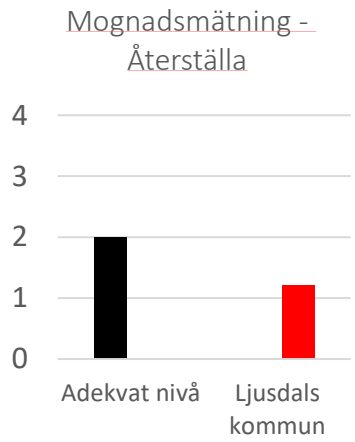
- Det saknas aktuell styrning i form av riktlinjer, planer och rutiner som reglerar hur en incident ska hanteras och vad som utgör en risk.
- Tester av processer för respons och krishantering, exempelvis genom övningar, sker inte.

3.6. Återställa

Återställa handlar om processer för kontinuitetshantering och förmågor relaterade till robusthet och återhämtning efter hantering av incidenter. Kommunikation och publika relationer (PR) inkluderas även i denna kategori. Nedan redovisas iakttagelser och bedömning av mognad/förmåga som vi har gjort i samband med workshops och genomgång av relevanta underlag.

3.6.1. Iakttagelser – Återställa

Granskningen visar att mognadsgraden för området *återställa* är betydligt lägre, 1.2, jämfört med adekvat nivå, 2.0. Till grund för bedömningen ligger bl.a. följande iakttagelser:



- Det finns ingen dokumenterad (katastrof)återställningsplan, utan beslut om återställning till normalläge fattas i linjen.
- Utvärdering och identifiering av lärdomar genomförs på ett informellt sätt. Tidigare händelser har utvärderats av externa aktörer. Vid mindre incidenter har lärdomar följts upp vid exempelvis utbildningar. Ansvaret för att revidera rutiner är förskjutet till verksamheterna.
- Ledningen arbetar mycket med kommunikation, från att tidigare endast ha fokuserat på information. Detta har dock inte skett strukturerat, utan ad hoc-mässigt.
- Roller och ansvar för PR är otydligt reglerat och det finns en osäkerhet när det kommer till ansvarsfördelning.
- Det finns en krisinformationsplan för Ljusdals kommuns ledning som ska användas vid informationsinsatser vid extraordinära händelser och vid krissituationer.

I sammanhanget noteras att den i huvudsak låga mognadsnivå beror till stor del på att det saknas strukturerade återställningsplaner som på kommunövergripande nivå beskriver hur organisationen ska återgå till normalt läge efter en incident. Det förekommer en mycket begränsad användning av PR, främst till följd av att roller och ansvar inom området inte är tydliga. Vissa situationer hanteras endast internt och fokus ligger snarare på information än kommunikation, dock har ledningen börjat fokusera mer på kommunikation.

De förbättringsområden som vi kan konstatera är bl.a. följande:

- Det finns ingen dokumenterad (katastrof)återställningsplan. En eventuell incident hanteras ad hoc utifrån den kunskap som medarbetarna i dagsläget har. Det finns inte några dokumenterade krav på återställningskunskap hos medarbetarna.
- Återställningsprocesser har inte dokumenterats. Incidenter och återställning av exempelvis förlorad data sker ad hoc och utifrån medarbetarnas nuvarande kunskaper. Det finns inte heller några tröskelvärden för när hanteringsfasen ska gå över till återställningsfasen.

- Översiktlig roll- och ansvarsfördelning vid större incidenter är bristfällig. Det är inte tydligt reglerat vilket ansvar som åligger olika roller i kommunen samt vilken ordning åtgärder ska vidtas i händelse av en incident.

4. Revisionell bedömning

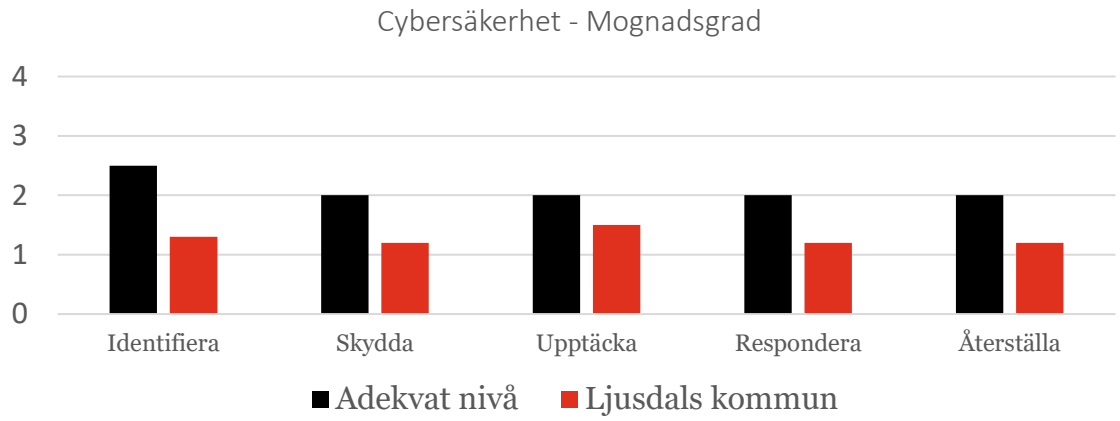
Granskningen ska besvara följande revisionsfråga: *Har kommunstyrelsen säkerställt att den interna kontrollen avseende kommunens cybersäkerhet är tillräcklig?*

Granskningen har fokuserat på processer, personal och teknik inom granskningsområdet utifrån följande kategorier; *identifiera, skydda, upptäcka, respondera och återställa.*

Bedömningen av mognadsnivå kopplat till cybersäkerhet har skett utifrån följande skala:

Nivå 1	Låg
Nivå 2	Låg-medel
Nivå 3	Medel-hög
Nivå 4	Hög

I nedan figur sammanfattas resultatet av granskningen:



Vår sammanfattande revisionella bedömning är att den interna kontrollen avseende kommunens cybersäkerhet är bristande. Bedömningen baseras på följande:

Vår granskning visar att kommunens mognadsgrad avseende cybersäkerhet inte är i adekvat nivå. Granskningen visar på bristande dokumentation och låg systematik inom granskat område. Det finns en viss operativ förmåga att skydda sig mot samt svara på incidenter, men detta arbete är i hög grad händelsestyrt och därmed kan cybersäkerheten inte säkerställas. Vidare konstateras att behörighetskontroller och lösenordshantering bedrivs på ett informellt sätt, vilket inte utgör grund för en sund IT- och cybermiljö.

Utifrån vår granskning kan vi konstatera att det i låg utsträckning finns formell styrning i form av planer, policys och riktlinjer som är aktuell och implementerad i organisationen. Granskningen visar även på att riskbedömningar, systemöversikt samt roll- och ansvarsfördelning för incidenthantering är förbättringsområden.

4.1.1. Rekommendationer

Utifrån genomförd granskning och vår sammanfattande bedömning lämnar vi följande rekommendationer till kommunstyrelsen i syfte att utveckla verksamheten.

- Kommunstyrelsen säkerställer att planer uppdateras/revideras samt kompletteras med rutiner, instruktioner och riskbedömningar för att utveckla hur informationssäkerhetsarbete ska bedrivas. Risker/hot kopplat till information- och IT-säkerhet samt kontinuitetsplanering bör särskilt beaktas i kommunens kommande risk- och sårbarhetsanalys avseende mandatperioden 2019-2022.

- I syfte att öka förmågan att upptäcka avvikelser behöver kommunstyrelsen säkerställa att identifiering och rapportering av risker i kommunens IT-miljö utvecklas. IT-system med hög driftsäkerhet och starkt skydd mot externa attacker är av mycket stor vikt för säkerheten i samhället och för möjligheterna att hantera olika krisförlopp.

- Kommunstyrelsen säkerställer att övningar och utbildningar genomförs i syfte att öka kännedomen kring kommunövergripande styrning/ramverk för informationssäkerhet samt för IT-säkerhet. Övningar och utbildningar kan med fördel även syfta till att öka verksamheternas/användarnas kännedom om vilka risker som finns kopplat till användning av IT.

2018-12-13

	Robert Bergman
Uppdragsledare	*Projektledare*