Granskning av Informationssäkerhet

Rapport

Kumla kommun

KPMG AB

2020-09-14

Antal sidor 15

Kumla kommun
Granskning av Informationssäkerhet

2020-09-14

Innehållsförteckning

Kumla kommun
Granskning av Informationssäkerhet

2020-09-14

1 Sammanfattning

KPMG har av Kumla kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och samtliga nämnders rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2020.

Vår bedömning är att kommunstyrelse och nämnder inte har säkerställt att det finns en ändamålsenlig organisation för informationssäkerhetsarbetet i kommunen. I nuläget sker inget systematiskt arbete för att uppnå god informationssäkerhet.

Arbetet är i en uppstartsfas och det saknas tillämpbara policys och riktlinjer som beskriver ansvar och hur arbetet ska bedrivas. Informationssäkerhetsarbetet är inte formellt organiserat men en informationssäkerhetsgrupp har bildats som leds av informationssäkerhetssamordnare.

Vi anser att informationssäkerhetssamordnarens roll behöver förtydligas och tilldelas resurser i form av tid för att arbetet ska kunna ordnas på ett systematiskt sätt och utgöra ett stöd i verksamheternas arbete. Vår bedömning är vidare att verksamheterna känner till sitt ansvar för informationssäkerheten men vi upplever inte att de fullt ut tagit sitt ansvar för att säkerställa en god säkerhet för de informationstillgångar de ansvarar för. Bland annat kvarstår arbete med att genomföra informationsklassning av verksamhetssystemen samt risk- och konsekvensbedömningar. Detta blir särskilt viktigt för de verksamheter som har identifierats och anmälts som samhällsviktiga funktioner och därigenom lyder under NIS-direktivet.

Rutiner och information om hantering av personuppgiftsincidenter finns men det saknas i nuläget rutiner och kunskap för hantering av informationssäkerhetsincidenter som inte avser personuppgifter.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Fastställa styrdokument som beskriver ansvar och hur arbetet med informationssäkerhet ska bedrivas i kommunen
- Besluta om en handlingsplan för informationssäkerhetsarbetet som är i enlighet med ett ledningssystem för informationssäkerhet för att arbetet ska kunna genomföras på ett systematiskt sätt
- Tydliggöra mandat och uppdrag för informationssäkerhetssamordnaren samt tillse att det finns tillräckliga resurser

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och samtliga nämnder att:

- Säkerställa att arbetet med informationsklassning genomförs för samtliga verksamhetssystem
- Säkerställa att risk- och konsekvensanalyser genomförs och dokumenteras så att vidtagna säkerhetsåtgärder står i relation till hot och risker
- Tillse att kunskap och rutiner finns för att anmäla, rapportera och åtgärda informationssäkerhetsincidenter

- Säkerställa att tillräcklig utbildning och information ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Kumla kommun
- Fastställa rapporteringsvägar för informationssäkerhetsarbetet till styrelse och nämnder

2 Bakgrund

KPMG har av Kumla kommuns förtroendevalda revisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens och samtliga nämnders rutiner för sitt informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2020.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Brister i hanteringen kan leda till förtroendeskada för organisationen.

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och måste skyddas mot obehörig åtkomst, såväl externt som internt. Vidtagna IT-säkerhetsåtgärder ska stå i relation till informationstillgångarnas värde och de risker och behov som ansvariga för informationen har fastställt. Detta då IT-säkerheten avser att säkra och trygga driften och hanteringen av kommunens kärnverksamheter.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informations-säkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att arbetet med informationssäkerheten behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen har syftat till att konstatera om kommunen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Granskningen har utgått från följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Sker en tillräcklig uppföljning att styrande dokument är kända och efterlevs?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?
- Finns ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheten?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

Granskningen har omfattat kommunstyrelsen och kommunens samtliga nämnder[1].

Granskningen omfattar år 2020.

Granskningen har genomförts av Jenny Thörn, verksamhetsrevisor. Andreas Wendin har deltagit i granskningen utifrån sin roll som kundansvarig för revisorerna i Kumla kommun.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Tillämpbara interna regelverk, policyer och beslut.
  Informationssäkerhetspolicy
  Säkerhetsinstruktioner
  Systemsäkerhetsplan
- MSB:s metodstöd avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

- Informationssäkerhetspolicy och tillhörande säkerhetsinstruktioner
- Systemsäkerhetsplan
- Rutiner för incidenthantering och exempel

Intervjuer med berörda tjänstepersoner:

- IT-chef
- Informationssäkerhetssamordnare
- Dataskyddssamordnare från förvaltningen för livslångt lärande, kommunledningsförvaltningen, kultur och fritidsförvaltningen och samhällsbyggnadsförvaltningen
- Från socialförvaltningen deltog medicinskt ansvarig för rehabilitering, MAR och utredningssekreterare
- Från förvaltningen för livslångt lärande deltog även enhetschef elevhälsa och enhetschef administration

Samtliga intervjuade har faktakontrollerat rapporten.

[1] Företrädare från lönenämnden och överförmyndarnämnden har inte deltagit i intervjuer för granskningen.

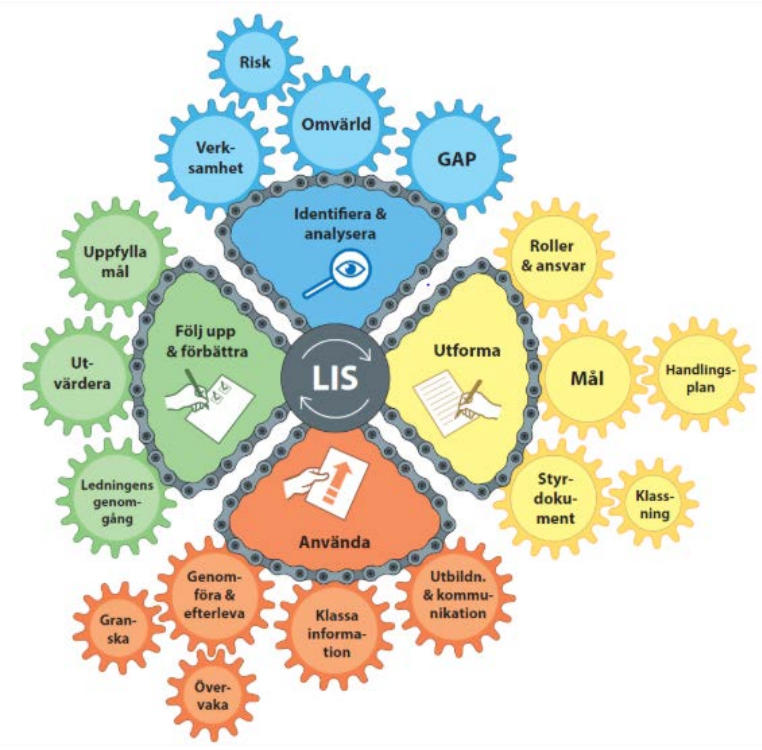
3 Inledning

Vi har med utgångspunkt i MSB:s metodstöd för informationssäkerhet och gällande standard inom området granskat om arbetet i Kumla kommun är strukturerat och ändamålsenligt.

3.1 MSB:s metodstöd för systematiskt informationssäkerhetsarbete

MSB[2] har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet är baserat på den internationella standard-serien för informationssäkerhet, ISO/ IEC 27000 och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.



Metodstödet och de fyra metodstegen med underliggande metoddelar.

I MSB:s metodstöd för systematiskt informationssäkerhetsarbete framgår hur ansvaret för arbetet med informationssäkerhet bör fördelas.

[2] Myndigheten för Samhällsskydd och Beredskap

Ledningens förståelse för och engagemang i informationssäkerhet är grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också oumbärlig för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära ledningen, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

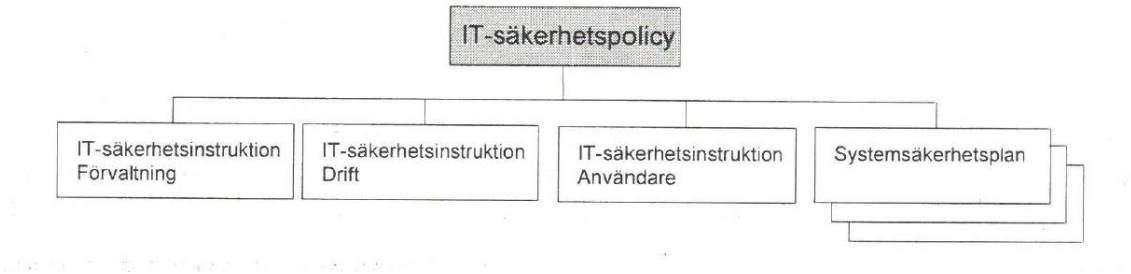
I de fall rollen är placerad i en strategisk IT-funktion såsom CIO-stab bör funktionen vara åtskild från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetsstrategen både ska granska och vara kravställande gentemot IT-driften och riskerar annars att brista i opartiskhet.

4 Resultat av granskningen

4.1 Styrdokument

I Kumla kommun finns styrdokument för informationssäkerhet i form av en informationssäkerhetspolicy för IT och tillhörande säkerhetsinstruktioner för drift, användare och förvaltning.

I policyn framgår följande hierarki för styrdokumenten:



Av dokumentgranskning går det inte att utläsa om styrdokumenten är fastställda av kommunfullmäktige eller kommunstyrelsen förutom för säkerhetsinstruktionen för användare. Den är beslutad av kommunfullmäktige 2006-03-20 och reviderad 2008-11-15. Enligt skrivelse i policyn ska dokumenten revideras löpande utifrån behov. Nuvarande policy utgår från en tidigare rekommendation som kallades BITS, Basnivå för informationssäkerhet, som inte stöds längre då arbetet med informationssäkerhet och tillhörande IT-säkerhet kontinuerligt utvecklas och förändras utifrån nya risker och behov av systematik i arbetet.

I intervjuer framkommer att styrdokumenten är föråldrade och behov finns av att upprätta och fastställa nya styrdokument för kommunens informationssäkerhetsarbete. De som finns idag används inte för att styra arbetet i kommunen. I andra sammanhang där kommunen har ansökt om att bli pilotkommun exempelvis för arbete inom digitalisering har policydokument och strategier efterfrågats varpå kommunen har blivit medvetna om att detta behöver ses över.

Det har också förtydligats genom ett mer systematiskt arbete med GDPR, att detta skulle förstärkas genom ett mer systematiskt arbete även med informationssäkerheten. Detta då delar av GDPR-arbetet styrs av mer övergripande rutiner och säkerhetsarbete.

4.1.1 Bedömning

Det finns framtagna styrdokument för kommunens informationssäkerhet i form av policy och tillhörande säkerhetsinstruktioner. Vår bedömning baserat på nuvarande styrdokument och intervjuades beskrivning är att flertalet av de styrande dokumenten

som finns tillgängliga är ofullständiga, föråldrade och inte tillämpbara i nuvarande form. Behov finns att ta fram nya styrdokument och förankra dessa i kommunens verksamheter för en tydligare styrning av informationssäkerhetsarbetet.

4.2 Organisation för informationssäkerhet

Då styrdokument inte är tillämpade i verksamheten har vi i granskningen utgått från den beskrivning som vi erhållit i intervjuer och inte de roller som finns beskrivna i styrdokumenten.

I Kumla kommun är säkerhetsarbetet organiserat inom kansliavdelningen som hör till kommunledningsförvaltningen under kommunstyrelsens ansvar. En informationssäkerhetssamordnare finns utsedd som arbetar ca 20 % med detta vid sidan om sitt uppdrag som dataskyddsombud (60 %) och utredare (20 %). I nuläget omfattas uppdraget som utredare av att utgöra dataskyddsombud i Lekebergs kommun. Övriga funktioner på kansliavdelningen är bland annat kommunledningssekreterare, kommunsekreterare, utvecklare/utredare, beredskapssamordnare, kommunjurist, kommunikatör och överförmyndarhandläggare.

För att informationssäkerhetssamordnaren ska kunna utgöra ett stöd och vara oberoende i granskning av arbetet krävs det att denna ska kunna agera med ett oberoende till IT och övriga förvaltningar och ha en placering i organisationen som medger detta.

Informationssäkerhetssamordnaren är inte formellt ansvarig för kommunens informationssäkerhet men bör enligt MSB:s rekommendationer ha en stödjande och kontrollerande roll där det ingår att granska att arbetet sker på ett systematiskt och riskbaserat sätt i förvaltningarna. Det finns enligt intervjuer ingen formaliserad organisation för informationssäkerhet men ansvaret följer det ordinarie ledaransvaret.

I intervjuer beskrivs att kommunens arbete med GDPR även har lett till ett ökat fokus på informationssäkerhetsfrågorna. Därigenom har den grupp som tillsattes i kommunen inför införandet av GDPR även tagit sig an informationssäkerhetsfrågorna, även om detta arbete inte sker på ett systematiskt sätt ännu. Det framgår i intervjuer att en prioritering skett av dataskyddsfrågorna men att det finns ambitioner att även ta sig an informationssäkerhetsfrågorna och att arbetet är i uppstartsfas. Nuläget beskrivs som att det finns stora behov av att utveckla informationssäkerhetsarbetet för att det ska ske på ett systematiskt och strukturerat sätt.

Informationssäkerhetssamordnaren deltog i januari 2020 på kommunledningsgruppen för att beskriva detta. Informationssäkerhet har även varit ett av huvudområden för projektet med att implementera Office 365, varav det har rapporterats löpande inom ramen för projektet där kommundirektörens ledningsgrupp varit styrgrupp.

I intervjuer framkommer att det inom exempelvis socialförvaltningen finns mycket kunskap om sekretess, dokumenthantering och personuppgifter då det hanteras löpande inom deras verksamhetsområde. Både förvaltningen själva och andra intervjupersoner framhåller socialförvaltningen som en föregångare i informationssäkerhetsarbetet. Socialförvaltningen efterfrågar metoder och stöd för att

utveckla arbetet med informationssäkerhet från centralt håll. I intervjuer framhålls särskilt ett behov av en gemensam metod för informationsklassning så att det finns ett stöd i genomförandet av klassning. De beskriver också att de önskar ett närmare samarbete med kommunjurist och IT-avdelningen då frågor uppkommer där de själva inte har kompetensen att avgöra vad som är bäst ur juridiskt och säkerhetsmässigt perspektiv, exempelvis i digitaliseringsarbetet och utvecklingen med välfärdsteknik.

I intervjuer beskrivs att arbetet tidigare utgick från IT-avdelningen och hade ett stort fokus på IT-säkerhet, vilket även informationssäkerhetspolicyn visar. IT-avdelningen består av elva personer som är indelade i två team, ett för support och ett för utveckling och drift. En av medarbetarna inom utveckling och drift har gått en utbildning inom IT-säkerhet och har en fördjupad kunskap inom området men alla i teamet har ett visst ansvar för säkerhetsfrågor inom sitt arbetsområde. I övrigt sker en regelbunden omvärldsbevakning och kunskapsdelning i arbetsgruppen för att tillgodose kunskap och informationsbehov.

Det framkommer vidare att det upplevts att ansvaret mellan kansliavdelningen och IT-avdelningen varit otydligt. Det uppmärksammades särskilt i inledningsfasen av projektet med att implementera Office 365, men har under projektets gång blivit allt tydligare hur var och ens ansvar ser ut i arbetet med informations- och IT-säkerhet.

Det är chefernas ansvar att säkerställa att medarbetare får den information och kunskap som behövs för att upprätthålla säkerheten. Intervjupersoner har beskrivit att kommunen genomfört en digital utbildning inom GDPR under 2018 och vissa enheter har även bjudit in dataskyddsombud och dataskyddssamordnare som hållit i intern utbildning. Det har inte genomförts någon utbildning inom informationssäkerhet. En utbildning i IT-säkerhet är obligatorisk för alla anställda och följs upp av ansvarig chef. Utbildningen är en del i det introduktionsprogram som nyanställda ska genomgå vid anställning.

Intervjupersoner informerar att kommunen har gjort bedömningen att de omfattas av NIS-direktivet[3] för verksamheterna inom hälso- och sjukvård samt Vatten och avfall. Att kommunen har identifierat och anmält dessa verksamheter som samhällspliktiga ställer ytterligare krav på ett systematiskt och riskbaserat arbete med informationssäkerhet. Det medför också att det finns behov av att genomföra en förstärkt utbildning över hur detta ansvar ska hanteras i kommunen.

NIS-direktivet trädde i kraft efter beslut i EU 2016. Anledningen var den utveckling som skett med attacker på digitala system för samhällsviktiga funktioner. Syftet med direktivet är att etablera en säkerhetsstandard inom den digitala världen som skyddar den infrastruktur som bygger upp samhälle och ekonomi. Lagstiftningen ställer främst krav på att arbeta systematiskt och riskbaserat med informationssäkerhet. Sverige har antagit direktivet genom Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

[3] The Directive on Security of Network and Information Systems

4.2.1 Bedömning

Vår bedömning är att kommunstyrelse och nämnder inte har säkerställt att det finns en ändamålsenlig organisation för informationssäkerhetsarbetet i kommunen.

Då styrdokument saknas eller inte tillämpas finns det inte något ansvar dokumenterat kring styrningen av informationssäkerhetsarbetet eller hur det ska bedrivas.

Vår bedömning är att det i nuläget saknas resurser för att säkerställa ett systematiskt arbete. Samtliga verksamheter anger i intervjuer att de har behov av någon som samordnar arbetet och kan utgöra ett stöd för hur de kan ta sig an informationssäkerhetsfrågorna, till exempel genom kommunövergripande beslut för klassningsmodell eller en plan för hur arbetet ska bedrivas så att det blir likvärdigt i förvaltningarna.

Vi anser att informationssäkerhetssamordnarens roll behöver utvecklas då vår bedömning är att det i nuläget inte finns tillräckliga resurser i form av tid för att stötta verksamheterna i ett systematiskt arbetssätt. Detta blir helt avgörande då kommunen bedömt att verksamheterna inom hälso- och sjukvård samt VA står under NIS-direktivet. Lagstiftning som direktivet omfattas av ställer just krav på ett systematisk och riskbaserat informationssäkerhetsarbete för att skydda samhällsviktiga funktioner.

Vår bedömning är vidare att verksamheterna känner till sitt ansvar för informationssäkerheten men vi upplever inte att de fullt ut tagit detta för att säkerställa en god säkerhet för de informationstillgångar de ansvarar för. Det finns till viss del en tydlighet mellan verksamheterna och IT-avdelningens ansvar, men i avsaknad av exempelvis utsedda systemansvariga och förvaltare saknar IT-avdelningen någon att ha dialog med om säkerhetsåtgärder. Det kan leda till att säkerhetsåtgärderna inte står i relation till hur skyddsvärd informationen är då IT har den tekniska kunskapen men kanske inte kännedom om vilken information som hanteras i verksamhetssystemet.

Arbetet med informationssäkerhet behöver ske med ett ägandeskap från de som innehar ansvar för informationstillgångarna i förvaltningarna så att risker kan bedömas och ligga till grund för de beställningar av IT-säkerhetsåtgärder som det finns behov av.

4.3 Informationssäkerhetsarbete

Ledningssystem för informationssäkerhet, LIS

Det finns inte något ledningssystem för informationssäkerhet i kommunen och i intervjuer framhålls det som att det skulle ta för lång tid att implementera fullt ut med de resurser som finns för arbetet i nuläget.

Därför har man istället beslutat att fokusera arbetet på risk- och konsekvensanalyser samt informationsklassning. Detta arbete har dock inte påbörjats vid granskningens genomförande.

En viktig del i ett ledningssystem är att säkerställa att ledningen får en regelbunden uppföljning av nuläge i arbetet med informationssäkerhet och behov av förbättringar för att kunna prioritera resurser för dessa åtgärder. Vi har i granskningen fått information i intervjuer att det i nuläget inte sker någon löpande rapportering till kommunstyrelse

eller nämnder för arbetet med informationssäkerhet. Kopplat till GDPR och personuppgiftsincidenter finns rutiner för rapportering.

Informationsklassning

För att tydliggöra att olika typer av information har olika värde för verksamheten bör en klassning av information och system genomföras. Kommunen kan därefter skapa förutsättningar för lämpliga skyddsnivåer.

Detta görs ofta utifrån en systemöversikt där ansvariga är identifierade och dels med stöd av någon metod för informationsklassning. I Kumla kommun har man inte beslutat om någon metod för klassning.

Inför implementeringen av Office 365 genomfördes en informationsklassning med hjälp av extern konsult. Så har även skett för system inom socialförvaltningen och förvaltning för livslångt lärande. Ambitionen i kommunen är nu att dra nytta av dessa exempel på genomförda informationsklassningar och genomföra klassning i egen regi på system som kvarstår. Det behöver även ske en ny klassning av de som är klassade då detta behöver ske med en regelbundenhet då hot och risker förändras över tid.

I intervjuer framkommer att kommunen har tittat på metoden KLASSA som är framtagen av SKR. Denna metod används av många kommuner.

Vid klassning bedömer verksamheten informationens värde avseende sekretess, riktighet och tillgänglighet. Utöver detta finns även lagliga krav att ta hänsyn till.

Enligt KLASSA ska tre aspekter bedömas i en informationsklassning:

- Konfidentialitet
- Riktighet
- Tillgänglighet

Utifrån varje aspekt ska informationen klassas utifrån följande nivåer:

- Nivå 0= ingen eller försumbar skada
- Nivå 1= måttlig skada
- Nivå 2= betydande skada
- Nivå 3= allvarlig skada
- Nivå 4= synnerligen allvarlig skada

Eftersom skadeverkningarna av bristande säkerhet uppstår hos informationsägaren, det vill säga verksamheten, är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning. Detta kan i vissa fall vara delegerat till systemförvaltaren.

I intervju framkommer att det finns behov av att utveckla systemförvaltningsarbetet inom kommunen. Det saknas i nuläget en beslutad förvaltningsmodell för att styra arbetet men initiativ har tagit för att använda den vedertagna modellen pm3 för systemförvaltning i kommunen. I nuläget pågår ett arbete för att kartlägga alla verksamhetssystem. När det är genomfört är planen att utse ansvariga och förvaltare för dessa som erhåller utbildning och kunskapshöjande insatser för att kunna bedriva ett aktivt systemförvaltningsarbete. I detta arbete ska även informationssäkerhet och informationsklassning ingå. Kommunen har tittat på metodstödet för Ledningssystem för informationssäkerhet via Myndigheten för samhällsskydd och beredskap, MSB. Det har dock inte skett något arbete utifrån detta.

Inom exempelvis socialförvaltningen finns anställda systemförvaltare som arbetar aktivt med förvaltningen av verksamhetssystem. I intervjuer framkommer att det har blivit en stor förändring och förbättring inom området med nuvarande systemförvaltare och att det lett till en större kunskap och förståelse för dokumenthantering och informationssäkerhet.

Efter klassningen ska åtgärdsplaner upprättas. Åtgärdsplanerna handlar om olika saker där IT-säkerhetsåtgärder rent tekniskt är en del. Det kan även vara att göra mer utförliga risk- och konsekvensanalyser, förbättra rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna. Bedömningen kan också resultera i att inga ytterligare åtgärder behövs.

Kommunen har gjort en IT-säkerhetsanalys med penetrations-tester och genomgång av IT-säkerheten under 2018. Enligt intervjuperson så visade analysen inget alarmerande och IT-avdelningen arbetar löpande med förbättringsåtgärder för IT-säkerheten. Segmentering av infrastrukturen är ett exempel och man kommer troligen etablera brandväggar även för intern trafik till skillnad från idag då det endast finns för extern trafik, alltså hot som kommer utifrån.

Behörighetshantering

Användarkonton skapas och utgår från kommunens personalsystem när en person anställs. Tilldelning av behörigheter till verksamhetssystem sker efter beslut och beställning av cheferna till systemförvaltare eller utsedd administratör som lägger in rätt behörighet i systemet.

Det finns tillfällen när rutinerna behöver frångås, exempelvis vid bemanningslösningar, vikariehantering eller externa konsulter. Då sker tilldelning manuellt. I intervjuer lyfts detta som en säkerhetsrisk då det frångår rutinerna och det är lätt att missa hur stor behörighet som ska tilldelas samt hur den ska hanteras vid avslut.

För verksamhetssystem som innehåller journalhantering, exempelvis inom elevhälsan, sker en loggkontroll för att säkerställa att endast behöriga har tillgång till uppgifter.

Risk- och konsekvensbedömning

Risk- och konsekvensanalyser har till viss del genomförts för enskilda system och information. I samband med implementeringen av Office 365 genomfördes en

klassning av ostrukturerad information för att se hur den skulle hanteras och vad som behövde lagras på kommunens servrar och vad som kunde flyttas till molnet.

I planeringen för kommande arbete med informationssäkerhet är riskanalyser ett prioriterat område. I intervjuer framkommer att man genom att börja arbetet med detta steg får en prioriteringsordning över åtgärder som behöver vidtas och en ökad tydlighet mellan var och ens ansvar. Riskanalyserna ska visa vilka IT-säkerhetsåtgärder som behövs för att skydda informationen som sedan verksamheterna kan bli en tydligare beställare av till IT-avdelningen.

Kommunledningen har gett informationssäkerhetssamordnare i uppdrag att ta fram en kommunövergripande gemensam rutin för hur risk- och konsekvensanalyserna ska genomföras för att det ska ske på ett likvärdigt sätt och förenkla för verksamheterna.

Incidenthantering och rapportering

I intervjuer anges att det finns rutiner för att hantera personuppgiftsincidenter för anställda och för dataskyddssamordnare och dataskyddsombud. Det är en större tveksamhet till vad som är informationssäkerhetsincidenter och om dessa ska hanteras enligt samma rutin.

En e-tjänst finns för att rapportera inträffade personuppgiftsincidenter. Under 2019 anmäldes mellan 20 till 30 incidenter. Det var ingen av dessa som bedömdes som allvarlig och ofta var orsaken den mänskliga faktorn, exempelvis där en medarbetare skickar e-post med personuppgift eller liknande.

Intervjupersoner uppskattar att det är ett stort mörkertal för incidenter som inte upptäcks och rapporteras, till stor del på grund av att medvetenheten är för låg i verksamheterna.

4.3.1 Bedömning

Vår bedömning är att det inte sker ett ändamålsenligt arbete för att uppnå god informationssäkerhet. Vi baserar vår bedömning på att det saknas styrdokument och organisation för arbetet samt att arbetet med informationsklassning och riskhantering har påbörjats men ännu inte bedrivs på ett systematiskt sätt.

Vi ser det som positivt att kommunen har gjort en IT-säkerhetsanalys för att bedöma införda säkerhetsåtgärder och genom det har haft möjlighet att följa upp behov av åtgärder för att höja säkerheten och skyddet för informationen.

Då styrdokument inte finns som är tillämpade i verksamheten och utbildning inte har genomförts finns risk att medvetenheten för kommunens informationssäkerhet inte är tillräckligt god. Den mänskliga faktorn är en stor säkerhetsrisk då enskilda medarbetare eller förtroendevalda genom ovarsam hantering eller med uppsåt kan utgöra ett hot mot säkerheten för informationstillgångarna och leda till förtroendeskada för kommunen. En låg medvetenhet leder ofta till att det inte finns tillräcklig kunskap om när informationssäkerhetsincidenter sker vilket leder till att dessa inte rapporteras i

tillräckligt hög grad och därigenom kan inte ett lärande och ständiga förbättringar ske för att detta inte ska hända igen.

Vi anser slutligen att kommunstyrelse och nämnder behöver fastställa rapporteringsvägar för informationssäkerheten för att ta del av det arbete som pågår och de eventuella brister som finns i organisationen för att kunna prioritera resurser och vidta de åtgärder som det finns behov av.

5 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelse och nämnder inte har säkerställt ett ändamålsenligt och systematiskt arbete med sin informationssäkerhet.

Arbetet är under uppstart och det finns ingen dokumenterad mål- eller handlingsplan för hur arbetet ska genomföras. Utbildning har endast delvis genomförts vilket medför en risk att medvetenheten för kommunens informationssäkerhet inte är tillräckligt god. Den mänskliga faktorn är en stor säkerhetsrisk då enskilda medarbetare eller förtroendevalda genom ovarsam hantering eller med uppsåt kan utgöra ett hot mot säkerheten för informationstillgångarna och leda till förtroendeskada för kommunen.

Det kvarstår arbete med informationsklassning och riskbedömningar och vår bedömning är att informationsansvariga i verksamheterna inte fullt ut har tagit sitt ansvar för informationssäkerhetsarbetet.

Att informationsklassning och riskanalyser genomförs är avgörande delar för ett systematiskt informationssäkerhetsarbete. Detta krav är förstärkt för de verksamheter som kommunen identifierat och anmält till MSB som samhällsviktiga. Utan informationsklassning och riskanalys vidtas IT-säkerhetsåtgärder utan att åtgärden sätts i relation till hur skyddsvärd informationen är.

5.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Fastställa styrdokument som beskriver ansvar och hur arbetet med informationssäkerhet ska bedrivas i kommunen
- Besluta om en handlingsplan för informationssäkerhetsarbetet som är i enlighet med ett ledningssystem för informationssäkerhet för att arbetet ska kunna genomföras på ett systematiskt sätt
- Tydliggöra mandat och uppdrag för informationssäkerhetssamordnaren samt tillse att det finns tillräckliga resurser

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen och samtliga nämnder att:

- Säkerställa att arbetet med informationsklassning genomförs för samtliga verksamhetssystem
- Säkerställa att risk- och konsekvensanalyser genomförs och dokumenteras så att vidtagna säkerhetsåtgärder står i relation till hot och risker
- Tillse att kunskap och rutiner finns för att anmäla, rapportera och åtgärda informationssäkerhetsincidenter
- Säkerställa att tillräcklig utbildning och information ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Kumla kommun
- Fastställa rapporteringsvägar för informationssäkerhetsarbetet till styrelse och nämnder

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Andreas Wendin
Kundansvarig