Granskning av kommunens IT-säkerhet

Rapport

Ragunda kommun

KPMG AB

2020-03-16

Antal sidor 10

Antal bilagor 1

Ragunda kommun
Granskning av kommunens IT-säkerhet

2020-03-16

Innehållsförteckning

1	Sammanfattning	2
2	Inledning/bakgrund	3
2.1	Syfte, revisionsfråga och avgränsning	3
2.2	Revisionskriterier	4
2.3	Metod	4
3	Resultat av granskningen	5
3.1	Organisation	5
3.2	Styrande dokument	5
3.3	Redovisning av förberedande frågor	7
3.4	Svar på revisionsfrågorna	9
4	Slutsats och rekommendationer	10
4.1	Rekommendationer	10
Bilaga 1		12

1 Sammanfattning

Vi har av Ragunda kommuns revisorer fått i uppdrag att granska kommunens arbete med IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Granskningen har syftat till att konstatera om kommunen har kontroll över att införda IT-säkerhetsåtgärder är baserade på de risker och behov som informationsansvariga inom förvaltningarna har bedömt som nödvändiga utifrån informationstillgångarnas värde. Då IT-säkerheten är en avgränsad del av det större begreppet informationssäkerhet så utgår arbetet från styrdokument och organisering för informationssäkerheten.

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens informationssäkerhet vilket påverkar IT-säkerheten. Vår bedömning baseras bland annat på följande:

- kommunstyrelsen har inte tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas.
- det saknas politiska beslut och uppdrag till verksamheten för att säkerställa arbetet med kommunens informationssäkerhet.
- då informationsansvariga inom förvaltningarna inte har genomfört någon informationsklassning utgår i nuläget IT-säkerhetsåtgärder på bedömningar som IT-enheten har gjort ur ett tekniskt perspektiv utifrån risk och sårbarhet och inte utifrån informationstillgångarnas värde
- det saknas idag dokumentation avseende rutiner för kontinuitetsplanering och incidenthantering vilket gör detta personberoende och sårbart vid organisations- eller personalförändringar.

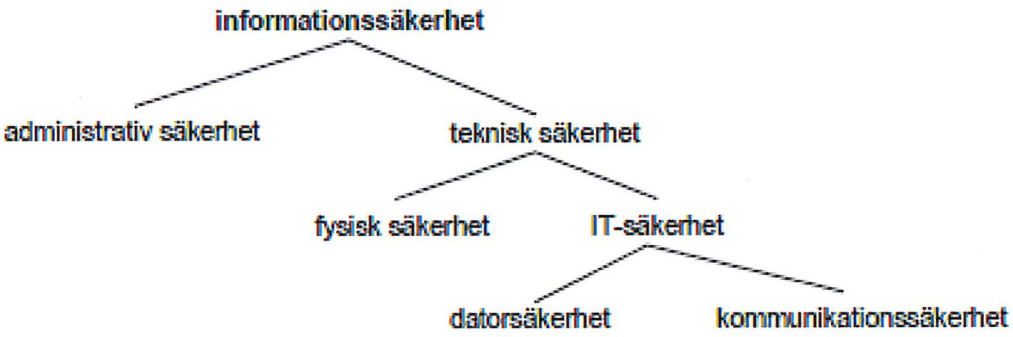
Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- Säkerställa att det finns tillräckliga resurser för att bedriva ett systematiskt informationssäkerhetsarbete.
- Säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs av ansvariga inom förvaltningarna för att beställd IT-säkerhet ska baseras på informationstillgångarnas värde.
- Utveckla arbetet med systemförvaltning så att ansvar tydliggörs och att en dialog kan ske mellan verksamheten och IT.
- Ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i prioriterade system och processer.

2 Inledning/bakgrund

Vi har av Ragunda kommuns revisorer fått i uppdrag att granska hur kommunen med underlag av sina styrande dokument avseende informationssäkerhetsrutiner anordnat sin IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Med IT-säkerhet avses en väl avgränsad del av det större begreppet informationssäkerhet och består av delarna datorsäkerhet och kommunikationssäkerhet. Bilden nedan illustrerar förhållandet mellan informationssäkerhet och IT-säkerhet.



Av standarderna i ISO 27000-serien kan utläsas att IT-säkerhet är underordnad informationssäkerheten. Placeringen innebär att beslut om IT-säkerhet styrs av de beslut som tas av system och/eller objektägare som har att efterleva beslutad informationssäkerhetspolicy med tillhörande tillämpningsföreskrifter. Alternativt tillämpar kommunen ett LIS[1].

Revisorerna utesluter inte att det finns risk för att införda IT-säkerhetsåtgärder inte står i relation till hur verksamhetsansvariga klassificerat den information de har ansvar för. Det kan i sin tur innebära att ansvarsförhållandena avseende kommunens informationstillgångar inte är tillräckligt kända och respektive ansvariga inte beställer/styr den IT-säkerhet som tillhandahålls.

Uppdraget ingår i revisionsplanen för år 2019.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen har syftat till att konstatera om kommunen har kontroll över att införda IT-säkerhetsåtgärder är baserade på de risker och behov som ansvariga för informationen (objektägare/systemägare inom förvaltningarna) har bedömt som nödvändiga utifrån informationstillgångarnas värde.

Granskningen ska besvara följande revisionsfrågor:

[1] Ledningssystem för informationssäkerhet

— Har kommunstyrelsen tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
— Har kommunstyrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?
— Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?

Granskningen avser kommunstyrelsen.

2.2 Revisionskriterier

Vi har bedömt om etablerad IT-säkerhet uppfyller interna regelverk samt policys med tillhörande tillämpningsföreskrifter.

2.3 Metod

Granskningen har genomförts genom inledande dokumentstudier och därefter en utfrågning (hearing) med deltagande av förtroendevalda, förtroendevalda revisorer och tjänstemän på förvaltningsledningsnivå och inom IT och säkerhetsarbete.

I bilaga 1 redovisas det frågekomplex som har använts vid utfrågningen.

Rapporten är faktakontrollerad av enhetschef för kommunikation och verksamhetsansvarig IT.

3 Resultat av granskningen

3.1 Organisation

Informationssäkerhetsarbetet och IT-säkerheten är organiserade inom kommunledningsförvaltningen. Kommunchef är tillika förvaltningschef och det finns tre enhetschefer som ansvarar för avdelningarna inom förvaltningen. Ansvarig för kommunens informationssäkerhetsarbete är i nuläget säkerhetssamordnaren då annan utsedd person saknas. Verksamheten har i budgetplanering bett om resurser för att tillsätta en tjänst för att bedriva informationssäkerhetsarbetet men det finns inget beslut om att tillsätta en sådan funktion i nuläget.

IT-enheten består av tre tekniker, en samordnare och en verksamhetsansvarig. Ansvar för IT-säkerheten har verksamhetsansvarig IT som är underställd enhetschef på kommunikationsavdelningen.

Avdelningarna lyder under kommunstyrelsens ansvarsområde.

Bedömning

Vår bedömning är att det saknas resurser för att det ska finnas förutsättningar att bedriva ett systematiskt och strukturerat informationssäkerhetsarbete. Det saknas även en informationssäkerhetssamordnare/ansvarig med uppdrag att leda arbetet. Då många insatser behövs för att organisera arbetet med informations- och IT-säkerhet anser vi att det finns en risk att det utan dessa resurser och någon som planerar och leder arbetet inte finns tillräckliga förutsättningar för att säkerställa kommunens informationssäkerhetsarbete.

3.2 Styrande dokument

3.2.1 IT-strategi 2017–2021

Kommunens IT-strategin ska ge stöd och vägledning i planering och genomförande av verksamheternas insatser på IT-området. Strategin är fastställd i kommunstyrelsen 2017-01-31.

IT-strategin anger kommunens förhållningssätt för användning och utveckling av informationsteknik. Strategin syftar till att förbättra kommunens förutsättningar för utveckling av e-förvaltning genom att peka ut gemensamma mål och insatsområden.

3.2.2 IT-säkerhetspolicy

Verksamhetsansvarig IT har påbörjat framtagandet av en policy för IT-säkerhet. Den är dock inte så långt kommen att det har varit möjligt för oss att ta del av den i granskningen. Att ta fram policyn är inte ett uppdrag från kommunstyrelsen utan självpåtaget av verksamheten då det upplevs saknas tydliga instruktioner över hur arbetet ska bedrivas.

3.2.3 Dataskyddspolicy

En dataskyddspolicy har beslutats av kommunstyrelsen 2019-12-10 och går vidare i ärendehanteringen för att fastställas av kommunfullmäktige vid kommande sammanträde.

Policyn ska leda arbetet för dataskydd i kommunen och kan kompletteras med riktlinjer för ytterligare tydliggörande.

3.2.4 Säkerhetsinstruktion för datoranvändare

Det finns en säkerhetsinstruktion för användare från 2007. Den innehåller delar som hantering av lösenord, lagring, användning av internet och e-post mm. Av dokumentet framgår:

> *Information är en viktig tillgång för vår organisation. För att skydda de värden informationen representerar krävs ett säkerhetsmedvetande hos alla medarbetare.*
>
> *Du som användare har alltså en del av ansvaret för säkerheten i informationshanteringen. För att du skall kunna leva upp till de säkerhetskrav som ställs på dig måste du känna till:*
>
> - *vilket ansvar du har*
> - *vad du skall göra vid olika incidenter*
> - *var du kan få stöd och hjälp*

Dokumentet innehåller behörighetsbeställning för användare som fylls i av närmaste chef samt en försäkran från användaren att de tagit del av utbildning för IT-säkerhet och tagit del av säkerhetsinstruktionen. Underskriven försäkran sparas i personakt och kan därigenom kontrolleras och följas upp att medarbetarna har fått information om sitt ansvar.

Bedömning

Vår bedömning är att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet med informationssäkerheten och den underliggande IT-säkerheten ska bedrivas.

Det saknas Informationssäkerhetspolicy och tillhörande anvisningar. Det saknas även IT-säkerhetspolicy eller riktlinjer för det arbetet. Under hearing framkom att IT-säkerhetspolicy är under framtagande men det finns ingen tidsplan för när den ska vara klar eller plan för implementering i verksamheten.

Den instruktion för användare som finns är föråldrad och i behov av en revidering utifrån nuvarande förutsättningar. Vi anser dock att det är positivt att instruktionen hänger samman med behörighetshantering för medarbetare och att alla ska underteckna en försäkran att de tagit del av informationen kring IT-säkerhet och IT-användning. Genom det kan uppföljning ske att alla medarbetare har fått information och grundläggande kunskap inom området och om sitt ansvar.

3.3 Redovisning av förberedande frågor

I bilaga 1 finns de frågor som vi använt i denna granskning. Enhetschef samt säkerhetssamordnare har svarat skriftligt på samtliga frågor och vi (KPMG) har också diskuterat utvalda frågor vid den hearing som genomfördes 2019-12-06 i Ragunda.

3.3.1 Roller och ansvar för IT-säkerheten

Under hearingen bad vi att få en beskrivning över hur kommunen byggt upp sitt arbete och sin organisering av Informationssäkerheten och gränsdragningen till IT-säkerheten. Det finns ingen i kommunen som driver informationssäkerhetsarbetet i nuläget då resurser saknas. IT-enheten upplever sig ha stort ansvar för IT-säkerheten och beskriver att verksamheterna ansvarar för sin information och sina verksamhets-system.

I IT-strategin finns en beskrivning av roller och ansvar men vid hearingen framkommer att dokumentet är en ”hyllvärmare” som inte används i verksamheten. Planen är att roller ska dokumenteras i IT-säkerhetspolicyn som är under framtagande.

Där det finns systemförvaltare fungerar dialogen bra men för övriga system är det IT som får ta ansvaret. Det försvårar arbetet då IT-enheten inte har inblick i vilken information som hanteras och hur behörigheter ska hanteras.

IT-enheten upplever inte att de har tillräckliga resurser (ekonomi och kompetens internt och/eller externt) som behövs för att uppnå den IT-säkerhet som erfordras i den kommunala verksamheten.

3.3.2 Dokumentation och rutiner för IT-säkerhet

IT-chefen uppger att Ledningssystem för informationssäkerhet (LIS) saknas men att en upphandling pågår där detta är inkluderat. Det finns för närvarande inga planer på att certifiera kommunens arbete efter standarder i ISO 27000-serien.

Det finns en systemförteckning över kommunens IT-system och i hearing framkommer att systemägare och systemförvaltare framgår av förteckningen men att flertalet system saknar detta och då blir IT- enheten ansvarig för dessa system. Det leder till en högre informationssäkerhetsrisk då IT får göra bedömningar utan ha den kunskap som krävs över vilken information som hanteras och hur skyddsvärd den är. Det finns inga dokumenterade systemförvaltningsplaner.

Det planeras för att införa en mer automatiserad hantering av behörigheter så att detta är kopplat till medarbetarens anställningsinformation i personalsystemet. Med den hanteringen kan kommunen säkerställa att medarbetare har behörigheter i rätt system och under rätt tid då det följer anställningsavtal. Genom det kan även en mer strukturerad kontroll genomföras över vilka som har behörigheter i system för att uppdatera detta när förändringar uppstår.

Vad gäller NIS-direktivet[2] och GDPR har inte IT-enheten fått något uppdrag eller ansvar för att vidta åtgärder för att hantera dessa frågor för kommunen i stort. Till viss del hanteras GDPR i samband med dokumenthanteringsplaner som är ett arbete som pågått under 2019.

3.3.3 IT-säkerhetsåtgärder

Bedömning av vilka säkerhetsåtgärder som ska vidtas är i nuläget en diskussion från fall till fall med förvaltningarna. IT-enheten jobbar efter best practice i branschen.

Under hearingen bad vi att få en beskrivning över de säkerhetsåtgärder som är i drift. Ett flertal av de mer vanliga säkerhetsåtgärderna finns, bl.a. brandväggar, e-postfilter, kryptering m.m. Man har också infört tvåfaktors-autentisering som en säkerhetsåtgärd och det finns åtgärder direkt kopplade till klienterna (datorer i verksamheten).

Kommunen arbetar inte med några löpande kontroller av sin säkerhet för att på så sätt identifiera eventuella brister för att ha möjlighet att åtgärda dessa innan det skadar kommunens informationstillgångar. Det har genomförts en sårbarhetsscanning av attackytor och vissa åtgärder har vidtagits.

Kommunen har varit utsatta för DDOS-attacker[3]. Så kallade phishing-mail är vanligt förekommande som går ut på att en avsändare via e-post utger sig för att vara en trovärdig person eller organisation och efterfrågar anställdas inloggningsuppgifter eller annan värdefull information. Inga allvarliga konsekvenser har drabbat kommunen genom dessa intrång.

Kunskap finns inom IT-enheten över rutiner för incidenthantering men det är osäkert hur stor kunskap det finns om detta inom förvaltningarna. När IT-enheten upptäcker incidenter rapporteras detta till säkerhetssamordnaren och i förekommande fall även till tillsynsmyndighet.

Det saknas i nuläget dokumenterade kontinuitetsplaner som säkerställer återställningsrutiner vid ev. händelser. Övningar har genomförts där kommunen iscensatt exempelvis dammbrott för att se hur händelsen skulle kunna påverka IT-miljön. Inget finns dokumenterat kring åtgärder och planering vilket innebär att om en händelse sker så hanteras den utifrån erfarenhet och kunskap hos personen som är i tjänst vid händelsens tidpunkt.

Alla medarbetare genomgår i samband med anställning en IT-introduktion hos medarbetare inom IT. Utbildning av GDPR har genomförts. Informationsinsatser sker vid behov.

---

[2] NIS-direktivet genomfördes i Sverige 2018 och ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster.

[3] DDOS-attacker är en form av överbelastningsattack i syfte att sabotera server- eller förbindelsekapacitet för en verksamhets nätverk, webbplats eller datorsystem.

Bedömning

Vår bedömning är att det finns brister i arbetet för att säkerställa en tillräcklig kontroll över kommunens Informationssäkerhet. I nuläget baseras inte säkerhetsåtgärderna på risker och behov som ansvariga för informationen har fastställt. Utan det underlaget anordnas åtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sin kunskap och sina förutsättningar. Dialog och samverkan mellan förvaltningarna och IT för arbetet med systemförvaltning, informationsklassning och servicenivåer för att säkerställa en god IT-säkerhet behöver därför utvecklas.

3.4 Svar på revisionsfrågorna

Har kommunstyrelsen tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?

Vår bedömning är att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas.

Har kommunstyrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?

Arbetet med IT-säkerheten är ett kontinuerligt arbete som till sin struktur beskrivs i styrdokument som utgår från kommunens informationssäkerhetspolicy. Oavsett om styrande dokument finns eller inte är det nödvändigt att informationstillgångarna klassas för att bedöma värdet på dessa. Utan det underlaget anordnas IT-säkerhetsåtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sin kunskap och sina förutsättningar. Vid granskningen uppfattar vi att inget av de verksamhetssystem som är i drift har informationsklassats och det går därför inte att bedöma om tillräckliga och relevanta säkerhetsåtgärder är vidtagna. IT-enheten har utefter vad som är möjligt inom deras ansvar för IT-säkerheten genomfört risk- och sårbarhetsanalys och vidtagit åtgärder.

Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?

Det finns olika former för att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Av denna anledning har kommunen ett antal säkerhetsanordningar för att försvåra intrång och om det ändå sker, att upptäcka och åtgärda. De säkerhets-anordningar som finns på plats i nuläget är i form av brandväggar, antivirus, spam-filter m.m. Inga regelbundna penetrationstester eller intrångsförsök är genomförda för att se om en tillräcklig säkerhet för kommunens informationstillgångar är vidtagen men en sårbarhetsscanning har genomförts.

Det saknas kontinuitetsplan som beskriver de reserv-, återställning- och återgångs-rutiner som krävs för att säkerställa kontinuiteten i system eller processer, utifrån vad som har inträffat.

Trots alla tekniska skydd och varningssystem är det människor som ska efterleva den beslutade IT-säkerheten. För detta krävs en viss kunskapsnivå och en viss insikt i vikten av informations- och IT-säkerhet. Detta har man tagit fast på i Ragunda kommun och alla anställda i kommunen får gå en introduktionsutbildning hos medarbetare på IT. En säkerhetsinstruktion för användare gås igenom och medarbetaren får underteckna en försäkran som sparas i personakten.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens Informationssäkerhet vilket påverkar arbetet med IT-säkerheten. Vi baserar detta på att kommunstyrelsen inte har tillsett att det finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas. Det saknas även resurser för att arbeta med informationssäkerhet på ett systematiskt sätt för att säkerställa en tillräcklig organisering av arbetet. Utan att informationsansvariga inom förvaltningarna har genomfört en informationsklassning av den information som de ansvarar för kan inte en bedömning om tillräckliga IT-säkerhetsåtgärder är vidtagna göras. Utan informationsklassning vidtas åtgärder av IT-enheten utifrån en teknisk bedömning av risk och sårbarhet och baseras inte på en bedömning av informationstillgångarnas skyddsvärde.

4.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- Säkerställa att det finns tillräckliga resurser för att bedriva ett systematiskt informationssäkerhetsarbete.
- Säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs av ansvariga inom förvaltningarna för att beställd IT-säkerhet ska baseras på informationstillgångarnas värde.
- Utveckla arbetet med systemförvaltning så att ansvar tydliggörs och att en dialog kan ske mellan verksamheten och IT.
- Ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i prioriterade system och processer.

Ragunda kommun
Granskning av kommunens IT-säkerhet

2020-03-16

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Anneth Nyqvist
Certifierad kommunal revisor

Ragunda kommun
Granskning av kommunens IT-säkerhet

2020-03-16

Bilaga 1

Förberedande frågor inför hearing om IT-säkerhet

Styrande dokument och annan dokumentation

1. Finns det en aktuell informationssäkerhetspolicy för kommunen med tillhörande tillämpningsföreskrifter?
2. Finns det särskilda tillämpningsföreskrifter avseende IT-säkerheten?
3. Finns det ett ledningssystem för informationssäkerhet (LIS) infört eller planeras det för ett sådant?
4. Är LIS certifierat eller finns det planer på att certifiera sig efter standarder i ISO 27000-serien?
5. Finns det en uppdragsbeskrivning för IT-enheten som anger eget och kommungemensamt ansvar för IT-säkerheten?
6. Om ovan nämnda dokument inte finns framtagna, vilka styrdokument anser IT-enheten att man verkar utifrån vad gäller IT-säkerheten?
7. Finns det systemförvaltningsplaner (baserad på pm3, ITIL eller egenutvecklad organisation) för de datoriserade verksamhetsstöd kommunen använder?
8. Finns det en systemförteckning som redovisar driftsatta system där det framgår vem som innehar de olika ansvar som identifierats?
9. Vilket ansvar anser/upplever IT-enheten sig ha för informationssäkerheten och IT-säkerheten? Finns detta ansvar dokumenterat och kommunicerat?
10. Har kommunen utfört någon informationsklassning och på vilket sätt har den påverkat de IT-säkerhetsåtgärder som införts?
11. Finns det servicenivåöverenskommelser (SLA) mellan IT-enheten och verksamhetsansvariga? På vems/vilkas initiativ är de framtagna? Vi önskar få ett eller flera exempel på ett SLA om detta finns.
12. Både NIS-direktivet och GDPR gäller från och med första halvåret 2018. Vilka instruktioner/uppdrag/ansvar har IT-enheten erhållit för att anpassa verksamheten för att säkerställa att kommunen efterlever dessa?
13. Har IT-enheten tagit stöd/involverats av kommunens dataskyddsombud (ett eller flera) under anpassningen till GDPR?
14. Finns det kunskap om och etablerade rutiner för:
    a. Incidenthantering som innefattar rapportering till överordnade, politiken, berörd verksamhet, anställda och kommunmedborgare?

b. Incidenthantering som innefattar rapportering till berörda myndigheter så som Datainspektionen (Integritetsskyddsmyndigheten), Myndigheten för samhällsskydd och beredskap (MSB).

15. Finns det dokumenterade manuella rutiner/kontinuitetsplaner/katastrofplaner innefattande IT-säkerhetsåtgärder som testats någon gång(er) under de senaste två åren?

IT-säkerhetsåtgärder

16. Vi behöver en beskrivning av samt motivet (analysen) för de IT-säkerhetsåtgärder som vid utfrågningstillfället:
    a. Är i drift.
    b. Planeras sättas i drift innan årsskiftet 2019.
    c. Planeras sättas i drift efter årsskiftet 2019.
    d. Planeras förändras och/eller avvecklas.
17. Finns det vid utfrågningstillfället IT-säkerhetsrisker där åtgärder inte är i drift eller där befintliga åtgärder är bristfälliga?
18. Har det identifierats något intrångsförsök till kommunens infrastruktur och/eller system under 2018–2019? Vilken form av intrång och vad blev effekten?
19. Vilka åtgärder har vidtagits efter detta?
20. Har det utförts eller planeras det för penetrationstest av kommuns skydd mot intrång?
21. Anser IT-enheten att de har de resurser (ekonomi och kompetens internt och/eller extern personal) som behövs för att uppnå den IT-säkerhet som erfordras den kommunala verksamheten?
22. Vem/Vilka rapporterar IT-enheten till avseende IT-säkerheten? Med vilken periodicitet? Finns rapportering för 2018–2019 dokumenterad tar vi gärna del av den.
23. I vilka grupperingar (arbets- samordning-, samverkans- etc.) medverkar personer från IT-enheten när informationssäkerhet diskuteras/planeras/införs?
24. Finns det en dokumenterad och fastställd utbildningsplan för IT-enheten där IT-säkerhet ingår och är den fullföljd?
25. Finns det en fastställd utbildningsplan för kommunens övriga medarbetare avseende deras ansvar för kommunens IT-säkerhet på en grundläggande nivå?