IT-säkerhet

Promemoria (PM)

Nora kommun

KPMG AB

2019-05-22

Antal sidor 5 (9 inkl. bilaga)

Antal bilagor 1 (sid 7 - 9)

Nora kommun
IT-säkerhet
Promemoria (PM)
2019-05-22

Innehållsförteckning

Nora kommun
IT-säkerhet
Promemoria (PM)
2019-05-22

1 Sammanfattning

Vi har av Nora kommuns revisorer haft i uppdrag att genomföra en granskning avseende kommunens IT-säkerhet. Granskningen har syftat till att bedöma om kommunens IT-säkerhet är baserad på de risker som finns inom kommunens olika verksamheter. Granskningen har genomförts genom dokumentstudier samt en utfrågning/hearing.

I granskningen konstateras följande.

- Kommunstyrelsen har inte tillsett att det finns aktuella styrande dokument, så-som policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet med IT-säkerhet ska bedrivas.
- IT-enheten saknar vid utfrågningstillfället en modern och verksamhetsanpassad uppdragsbeskrivning som anger eget och kommungemensamt ansvar för IT-säkerheten.
- Verksamhetsansvariga har ingen kontroll över om den information de ansvarar för hanteras korrekt enligt externa och interna regler. Vid utfrågningen uppfattar vi att inget av de verksamhetssystem som är i drift har informationsklassats.

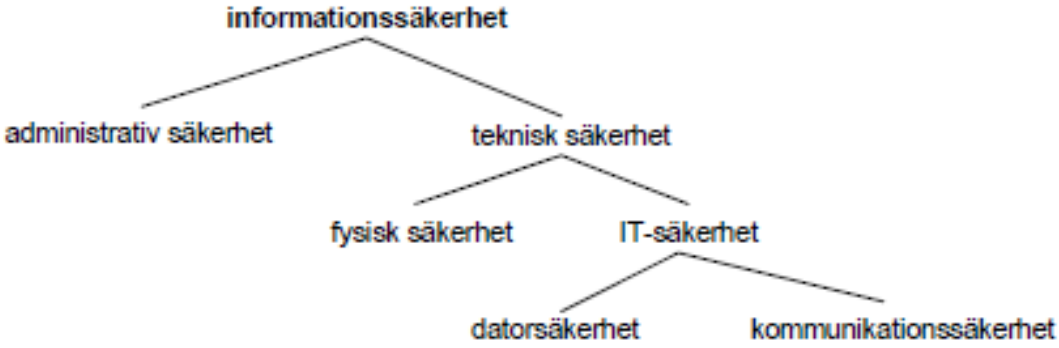
Mot bakgrund av ovanstående menar vi att kommunstyrelsen bör ge verksamhetsansvariga konkreta instruktioner om vilken nivå på informationssäkerhet och därmed IT-säkerhet som ska gälla.

Vidare bedömer vi det vara väsentligt att intentioner, roller, ansvar, resurser (personella likaväl som monetära), tidplan, prioriteringar och informations- samt utbildningsåtgärder dokumenteras och kommuniceras i samband med att kommunens informationssäkerhetspolicy omarbetas.

2 Bakgrund/inledning

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

Tidigare utförda granskningar har identifierat brister i kommunens styrning och kontroll av informationssäkerheten. Denna granskning inriktar sig mot IT-säkerhet. Nedanstående illustration förklarar förhållandet mellan begreppen informationssäkerhet och IT-säkerhet.



Av standarderna i ISO 27000-serien[1] 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[2].

Revisorerna utesluter inte, mot bakgrund av tidigare identifierade brister, att det finns risk för att införda IT-säkerhetsåtgärder inte står i relation till hur verksamhetsansvariga klassificerat den information de har ansvar för. Det bedöms även finnas risk för att ansvarsförhållandena avseende kommunens informationstillgångar inte är ändamålsenligt kända innebärande att respektive ansvariga inte beställer/styr den IT-säkerhet som tillhandahålls.

2.1 Syfte och revisionsfråga

Granskningen har syftat till att konstatera om kommunen har erforderlig kontroll över att de bedömningar och beställningar som införd IT-säkerhet grundar sig på är

[1] Serien innehåller över 40 olika standarder och det går att certifiera sin verksamhet i förhållande till en eller flera. SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet – Krav, SS-ISO/IEC 27002 Riktlinjer för styrning av informationssäkerhet, SS-ISO/IEC 27003 Vägledning för införande av ledningssystem för informationssäkerhet, SS-ISO/IEC 27004 Vägledning för mätning av informationssäkerhet och SS-ISO/IEC 27005 Riskhantering för informationssäkerhet är de som vanligast i ordning införs först.
[2] Ledningssystem för informationssäkerhet.

baserade på de risker och behov som ansvariga för informationen har identifierat och kommunicerat.

Granskningen/utfrågningen ska besvara följande revisionsfrågor:

- 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?

2.2 Avgränsning

Granskningen omfattar kommunstyrelsen.

2.3 Revisionskriterier

Vi har bedömt om etablerad IT-säkerhet uppfyller:

- Kommunallagen 6 kap. 6 §
- Interna regelverk samt policys med därtill hörande tillämpningsföreskrifter

2.4 Ansvarig nämnd

Granskningen avser kommunstyrelsen.

2.5 Metod

Granskningen har genomförts genom inledande dokumentstudier och därefter en utfrågning (hearing) vilken genomfördes 2019-04-26. Från kommunen deltog förutom tre förtroendevalda revisorer:

- Kommunstyrelsens ordförande och vice ordförande
- Kommundirektör
- Bildningschef
- Socialchef
- IT-chef

I bilaga 1 redovisas det frågekomplex som användes vid utfrågningen.

2.6 Projektorganisation

Utfrågningen utfördes av Lars Anteskog.

3 Resultatet av utfrågningen

3.1 Revisionsfrågorna

Kommunfullmäktige fastställde 2013-12-16 en IT-säkerhetspolicy. Av den framgår inledningsvis att: *”KBM:s rekommendationer om basnivå för IT-säkerhet (BITS) ska gälla som ramverk för IT-säkerhetsarbetet.”* Krisberedskapsmyndigheten (KBM) finns inte längre utan efter sammanslagningar av myndigheter blev den en del av MSB (Myndigheten för samhällsskydd och beredskap). Sedan några tillbaka utvecklar och underhåller MSB inte BITS. Tillämpningsföreskrifterna vi fått ta del av ansluter till policyn och är som den inaktuell och i behov av modernisering och kompletteringar. Kommunstyrelsen har därmed inte tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet med IT-säkerhet ska bedrivas.

Vid utfrågningen framkommer att det på chefsnivå pågår ett arbete med verksamhetsplaner. Som en del i det arbetet ingår att upprätta systemförvaltningsplaner. Vad vi förstår är IT-enheten involverad i arbetet. För arbetet finns dock inget definierat projekt med dokumenterade mål, resurser, prioriteringar och tidplaner där det framgår hur IT-säkerheten ska hanteras. IT-enheten saknar därmed vid utfrågningstillfället en modern och verksamhetsanpassad uppdragsbeskrivning som anger eget och kommungemensamt ansvar för IT-säkerheten.

Följaktligen så saknas det vid utfrågningstillfället former för att säkerställa effektiviteten av utförda IT-säkerhetsåtgärder.

3.2 Från utfrågningen i övrigt

Våra frågor var i förväg kortfattat besvarade av IT-chef. Kompletterande svar avseende GDPR[3] lämnades av medarbetare på kommunförvaltningen.

Utfrågningen gav följande information:

- För att säkerställa IT-säkerheten i kommunens fortsatta digitala utveckling redovisades det insikt om att det krävs ordning, reda och tydligt definierade ansvar. Metoden för detta är att upprätta verksamhetsplaner som i sin tur kan/ska leda fram till systemförvaltningsplaner. Vid utfrågningstillfället uppges det att det senare ska baseras på pm[3][4]. Det är en väl känd och anpassningsbar modell som används av flera kommuner.

[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[4] pm³ är en styrmodell med sin grund i systemförvaltningen men som över tid utvecklats till en modell som används för styrning av verksamhetsutveckling i stort.

- Enligt uppgift så har det påbörjats ett arbete med verksamhetsplaner inom skolverksamheten. Vi har inte haft tillgång till några dokumenterade mål, metoder och tidplaner för detta arbete.
- Oavsett om styrande dokument finns i någon utsträckning eller inte är det nödvändigt att de datoriserade verksamhetsstöden informationsklassas. Utan det underlaget anordnas IT-säkerhetsåtgärderna på ett sätt som IT-avdelningen upplever som nödvändigt utifrån sina förutsättningar. Verksamhetsansvariga har följaktligen ingen kontroll över om den information de ansvarar för hanteras korrekt enligt externa och interna regler. Vid utfrågningen uppfattar vi att inget av de verksamhetssystem som är i drift har informationsklassats.
- Det behövs, och vi uppfattar att det ska, säkerställas i vilken omfattning kommunen har förmåga att efterleva GDPR. Det behovet finns inte enbart ur IT-säkerhetsperspektivet.
- NIS-direktivet[5] trädde i kraft 2018-08-01. Kommunen har vid utfrågningstillfället inte tagit formell ställning till i vilken omfattning man omfattas av direktivet. IT-avdelningen har därmed inga instruktioner eller uppdrag för att anpassa sin verksamhet för att säkerställa någon omfattning av efterlevnad.

3.3 Kommentarer

Det bedöms som nödvändigt att kommunstyrelsen ger verksamhetsansvariga tydliga konkreta instruktioner om vilken nivå på informationssäkerhet och därmed IT-säkerhet som ska gälla. Det uppges att informationssäkerhetspolicyn ska omarbetas. I det sammanhanget bedömer vi att det är väsentligt att intentioner, roller, ansvar, resurser (personella likaväl som monetära), tidplan, prioriteringar och informations- samt utbildningsåtgärder dokumenteras och kommuniceras.

Parallellt med att informationssäkerheten får sin styrning och utformning bedömer vi det som praktiskt, och ur ett riskperspektiv nödvändigt, om IT-avdelningen dokumenterat delger verksamheterna vilka IT-säkerhetsåtgärder som är införda och planeras att införas för kommunen. En sådan redovisning gör det möjligt för verksamhetsansvariga att justera åtgärderna till en för dem acceptabel risknivå.

[5] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Direktivet ställer krav på säkerhet i nätverk och informationssystem. Reglerna omfattar leverantörer av samhällsviktiga tjänster och vissa digitala tjänster som kan finnas i både privat och offentlig sektor. Under hösten 2018 gav myndigheten för samhällsskydd och beredskap (MSB) ut fem föreskrifter kopplade till NIS-regleringen. Den 1 november trädde föreskrifter om anmälan och identifiering av samhällsviktiga tjänster samt föreskrifter om informationssäkerhet för samhällsviktiga tjänster i kraft. Föreskrifterna om incidentrapportering för samtliga NIS-leverantörer träder i kraft 1 mars 2019.

Nora kommun
IT-säkerhet
Promemoria (PM)
2019-05-22

2019-05-22

KPMG AB

Andreas Wendin — Biträdande uppdragsledare

Lars Anteskog — Projektansvarig

Styrande dokument och annan dokumentation

1. Finns det systemförvaltningsplaner (baserad på pm3, ITIL eller egenutvecklad organisation) för de datoriserade verksamhetsstöd kommunen använder?
2. Oavsett om det finns systemförvaltningsplaner eller inte finns det en systemförteckning som redovisar driftsatta system där det framgår vem som innehar de olika ansvar som identifierats?
3. Finns det en aktuell informationssäkerhetspolicy för kommunen med tillhörande tillämpningsföreskrifter?
4. Finns det särskilda tillämpningsföreskrifter avseende IT-säkerheten?
5. Finns det ett ledningssystem för informationssäkerhet (LIS) infört eller planeras det för ett sådant?
6. Är LIS certifierat eller finns det planer på att certifiera sig efter standarder i ISO 27000-serien?
7. Finns det en uppdragsbeskrivning för IT-avdelningen som anger eget och kommungemensamt ansvar för IT-säkerheten?
8. I eventuell avsaknad/inte ännu fastställda/planering av strategier och uppdragsbeskrivning vilka styrdokument anser IT-enheten att man verkar utifrån vad gäller IT-säkerheten?
9. Oavsett om det finns en aktuell informationssäkerhetspolicy eller inte vilket ansvar anser/upplever IT-enheten sig ha för informationssäkerheten (kommunen i allmänhet och IT-enheten i synnerhet) och IT-säkerheten? Finns detta ställningstagande motiverat, dokumenterat och kommunicerat? Vem/Vilka har mottagit ställningstagandet och vilken respons/reaktion har erhållits?
10. Oavsett styrande dokument eller inte finns det i någon omfattning en informationsklassning utförd och på vilket sätt har den påverkat de IT-säkerhetsåtgärder som införts?
11. Finns det servicenivåöverenskommelser (SLA) mellan IT-avdelningen och verksamhetsansvariga? På vems/vilkas initiativ är de framtagna. Vi önskar får ett eller flera exempel på ett SLA.
12. Både NIS-direktivet och GDPR gäller från och med första halvåret 2018. Vilka instruktioner/uppdrag/ansvar har IT-avdelningen erhållit för att anpassa sin verksamhet för att säkerställa efterlevnad för kommunen i allmänhet och IT-avdelningen i synnerhet?
13. I eventuell avsaknad av instruktioner/uppdrag/utpekat ansvar vilka åtgärder har IT-enheten utfört för att efterleva NIS-direktivet och GDPR? Finns det dokumenterade bedömningar om eventuella brister som kan innebära skada (verksam-

het och/eller ekonomisk) för kommunen? Finns det en brist- och/eller prioriteringslista där det framgår vad som eventuellt ännu inte åtgärdats, vilka konsekvenser det kan få och när samt hur de planeras vara åtgärdade?

14. Har IT-enheten tagit stöd/involverats av kommunens dataskyddsombud (ett eller flera) under anpassningen till GDPR?
15. 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).
16. Finns det dokumenterade manuella rutiner/kontinuitetsplaner/katastrofplaner innefattande IT-säkerhetsåtgärder som testats någon gång(er) under de senaste två åren?

IT-säkerhetsåtgärder (Oavsett om de framgår av de styrande dokumenten eller inte)

17. 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 2020.
    c. Planeras sättas i drift efter årsskiftet 2020.
    d. Planeras förändras och/eller avvecklas.
18. Finns det vid utfrågningstillfället IT-säkerhetsrisker där kompenserande åtgärder inte är i drift eller där befintliga åtgärder är eller bedöms bli bristfälliga?
19. Anser IT-avdelningen att de vid utfrågningstillfället har de resurser (ekonomi och kunnig intern och/eller extern personal) som behövs för att uppnå den IT-säkerhet som beskrivits ovan ställd fråga? Kan svaret även gälla för 2020?
20. Är det IT-avdelningens uppfattning att bemanning och kunskap avseende IT-säkerheten möter de behov och krav som framställs av överordnade funktioner (politisk- och tjänstemannanivån) och verksamheten i övrigt?
21. Vem/Vilka rapporterar IT-enheten till avseende IT-säkerheten? Med vilken periodicitet? Finns i närtid genomförd rapportering dokumenterad behöver vi den innan utfrågningen.
22. I vilka grupperingar (arbets- samordning-, samverkans- etc.) medverkar personer från IT-avdelningen när informationssäkerhet diskuteras/planeras/införs?

23. Finns det en dokumenterad och fastställd utbildningsplan för IT-avdelningen där IT-säkerhet ingår och är den fullföljd? Finns det en behovsanalys som underbygger utbildningsplanen och är andra än IT-avdelningens personal involverad i analys, prioriteringar och beslut avseende utbildning?

Några exempel på specifika IT-säkerhetsåtgärder (Oavsett om de framgår av de styrande dokumenten eller inte)

24. DNSSEC är en funktion som gör internet säkrare genom att försvåra manipulation av den information domännamnssystemet. Vad kan meddelas om hur det fungerar i Nora kommun?
25. Bortsett från standarder i ISO 27000-serien mäter och utvärderar kommunen sin IT-säkerhetmed i förhållande till andra standarder t.ex. NIST[6]?
26. Har det identifierats intrångsförsök till kommunens infrastruktur och/eller system under 2018 eller 2019? Vad blev effekten?
27. Har det utförts och/eller planeras det för penetrationstest av kommuns skydd mot intrång?
28. Hur hanteras hotet från utpressningsvirus eller phishing? Har kommunen drabbats dessa eller andra virus under 2018 eller 2019 och vad blev effekten?
29. Är Drive-by download[7] ett uppmärksammat problem som drabbat kommunen?

[6] NIST SP 800 är en samling standarder och rekommendationer inom i IT-säkerhet utgivna av Computer Security Resource Center inom National Institute of Standards and Technology. En enhet knuten till USA:s handelsdepartement.
[7] En nedladdning av skadlig kod utan att användaren själv uppfattar att den medverkat.