NACKA KOMMUN

2017-11-27

KFKS 2017/563

Revisorerna

Yttrande över revisionsrapport nr 3/2017 angående IT- och informationssäkerhet

Revisorerna har låtit göra en granskning av kommunens arbete med informationssäkerhet. Det har resulterat i en rapport från EY och en revisionsskrivelse. I detta yttrande ges svar på de konkreta frågorna i revisionsskrivelsen.

Inledningsvis noterar kommunstyrelsen att granskningen visar att Nacka kommun i stort har goda förutsättningar för ett ändamålsenligt arbete med IT-och informationssäkerhet. Kommunstyrelsen ser arbetet med informationssäkerhet som mycket högt prioriterat och det har blivit än viktigare med tanke på de attacker som sker mot system och informationstillgångar samt de brister som identifierats hos andra myndigheter. Kommunstyrelsen har under året ökat kraften i arbetet med informationssäkerhet väsentligt.

Den första frågan i revisionsskrivelsen är att den decentraliserade organisationen ställer krav på att ansvaret för informationssäkerhet tydliggörs. Enligt revisorerna har kommunen inte uppmärksammat detta tillräckligt. Frågan ställs var den centralt placerade personen som är ytterst ansvarig finns. Svaret på frågan är att administrativa direktören är ytterst ansvarig. Denne har varit med vid ett flertal tillfällen med revisorerna från EY i granskningen, och hållit ihop hela arbetet under det granskningen genomfördes. Det har påpekats att denne varit med, men det har inte tagits med i rapporten. Om det nu är oklart vem den centralt ansvarig personen är kunde revisorerna ha intervjuat delar av kommunstyrelsen och/eller stadsdirektören.

I granskningen har revisorerna kommit fram till att kommunen saknar standardiserade och definierade rutiner och processer kring informationssäkerhet samt styrning av dessa. Detta innebär enligt revisorerna en risk att organisationens olika ansatser inom informationssäkerhet inte genomförs på ett enhetligt och målinriktat sätt och utan en övergripande struktur. Det rekommenderas att centrala riktlinjer skapas och sprids för att säkerställa en enhetlig informationssäkerhetsbild. Svaret på detta är att det har genomförts kartläggningar kring informationssäkerhet och medvetenheten i organisation har höjts. Detta redovisades i samband med granskningen. Kommunstyrelsen kommer att se till att det tas fram vägledningar

NACKA
KOMMUN

för hur informationssäkerhet ska bedrivas, så att det sker på ett enhetligt och målinriktat sätt och efter en övergripande struktur. Detta kommer att vara klart före nyår. Noteras kan att dokumentet "Samverkansmodell Nacka" beskriver hur samverkan ska ske mellan kommunen och systemleverantörer.

Vidare tas upp att kommunen inte har uppdaterat sin informationssäkerhetspolicy på tre år, vilket skulle innebära en risk att den inte är anpassad efter förändrade omständigheter i organisationen och omvärlden. Det rekommenderas att policyn ses över löpande, åtminstone en gång per år. Svaret är att policyn kommer att ersättas av en informationssäkerhetsstrategi som kommer att uppdateras regelbundet, dock inte årligen utan vid behov. Samtidigt bör påpekas att varje gång den tillämpas, sker indirekt en prövning av att den är aktuell. Policyn är ett övergripande inriktningsdokument. Kommunstyrelsen ser vikten av arbetet med att informationssäkerhet hålls aktuell på högsta ledningsnivå. Det kan dock ske genom att årligen följa upp arbetet med informationssäkerhet och uppdatera policyn om det kommer fram att det finns behov av det i uppföljningen.

I den fjärde frågan tas upp att kommunen inte genomför några utbildningsinsatser inom informationssäkerhet. I och med detta riskerar bristande kunskap och medvetenhet exponera och utsätta organisationen för informationssäkerhetsrisker. Det rekommenderas att ett strukturerat utbildningsinitiativ startas. Utbildningsinsatser genomförs nu och omfattar alla förtroendevalda, chefer och medarbetare.

Ett område där brister noteras är att kommunen saknar tillräckliga incidenthanteringsrutiner och processer kring informationssäkerhet, samt en gedigen incidentshanteringsplan. Detta medför risk för att eventuella brister eller incidenter ej åtgärdas. Det rekommenderas att riktlinjer, rutiner och processer etableras och sprids genom organisationen. Kommunstyrelsen kommer att tillse vägledningar, rutiner och processer för hantering av informationssäkerhetsincidenter kommer att tas fram och implementeras. Detta kommer att vara klart under innevarande år.

I skrivelsen lyfts fram att kommunen i nuläget har roller med ansvar inom informationssäkerhet, dock är dessa spridda i organisationen. Det saknas däremot dedikerad avdelning eller grupp som äger dessa frågar och driver dem fullt ut – med t.ex. kompletta rutinbeskrivningar samt etablering av behörighetsadministrationsprocesser. Som tidigare sagts så ser kommunstyrelsen arbetet med informationssäkerhet som högt prioriterat. Ett bevis på det är att kommunen nyligen som en av de första kommunerna i landet anställt en medarbetare som har uppdraget som dataskyddsombud. Det är en roll som kommer att krävas när dataskyddsförordningen träder i kraft i maj 2018. Detta innebär både en utökning i omfattning och kompetens när det gäller informationssäkerhetsarbetet. Vidare kan sägas att arbetet med informationssäkerhet både handlar om att se till att lagar och regler efterlevs, att kompetensutveckling genomförs och att kommunens system är säkra. Därför har kommunstyrelsen valt att lägga ansvaret för det gemensamma arbetet med informationssäkerhet på

NACKA KOMMUN

både juridik- och kanslienheten samt digitaliseringsenheten. Ett nära samarbete mellan medarbetare på dessa enheter borgar för minst lika bra arbete som från en centralt placerad grupp. Sedan är det viktigt att notera att grundansvaret för informationssäkerheten ligger på nämnder, verksamheter och informationsägare.

Den sista frågan tar upp att kommunen inte genomför några penetrationstester utan förlitar sig helt på tredjepartsleverantörer och verksamhetsenheter inom den decentraliserade organisationen. Penetrationstester syftar till att identifiera tekniska sårbarheter som kan vara blottade för en eventuell angripare. Kommunen genomför i dagsläget inga externa penetrationstester, dvs. tester utifrån ett externt angreppsutfall, och inga interna penetrationstester, dvs. tester utifrån ett insiderperspektiv. Svaret på detta är att kommunen avsiktligen har valt att ha avtal med en av landets välrenommerade företag inom informationssäkerhet för att genomföra denna typ av tester istället för att göra dem med interna resurser. Det är svårt att upprätthålla egen kompetens inom området. Efter arbetet med revisionsrapporten avslutades har administrativa direktören beslutat det regelbundet och systematisk genomföra penetrationstester. Detta arbete har redan påbörjats. Som ett led att öka kommunens förmåga att hantera den försämrade omvärldsbilden och hotbilden kommer kommunstyrelsen i samarbete med nämnder och verksamheter att framgent genomföra övningar kopplade till informationssäkerhet.

Avslutningsvis ser kommunstyrelsen fram emot den aviserade dialogen med revisorerna om arbetet med informationssäkerhet.

FÖR KOMMUNSTYRELSEN

Mats Gerdau
Ordförande

Mats Bohman
Administrativ direktör