Tyresö kommun
Kommunstyrelseförvaltningen
Antonios Arvanitidis
IT-chef
08-57829026
antonios.arvanitidis@tyreso.se

Diarienummer
2019/KS 0158 016

Kommunledningsutskottet

Svar på revisionsrapport om granskning av Cybersäkerhet

Kommunstyrelseförvaltningens förslag till kommunledningsutskottet för beslut i kommunstyrelsen

- Kommunstyrelseförvaltningens skrivelse antas som kommunstyrelsens svar på revisionsrapporten "Granskning av cybersäkerhet"

Kommunstyrelseförvaltningen

Stefan Hollmark
Kommundirektör

Antonios Arvanitidis
IT-chef

Sammanfattning

EY har fått i uppdrag av de förtroendevalda revisorerna att ge en övergripande bild av Tyresö kommuns cybersäkerhet. En översiktlig granskning av 18 olika områden har genomförts under januari och februari 2019, med utgångspunkt i EYs Cyber Program Assessment-ramverk. För att genomföra analysen har dokument samlats in och ett arbetsmöte genomförts med IT-avdelningen, som är den funktion som främst jobbar med informationssäkerhetsfrågor.

Tyresö kommun bedöms i relation till andra offentliga organisationer av liknande storlek i förhållande till antal anställda och övergripande verksamhet. Revisionens övergripande slutsats är att Tyresö kommun har en förhållandevis låg mognadsgrad, men kommunen har ändå vissa tekniska lösningar och processer på plats för att hantera risker i IT-miljön. Mognadsgraden bedöms vara som högst inom drift, tredjepartsupphandling och nätverkshantering. Lägst är mognadsgraden inom hotbildshantering.

Kommunens största och viktigaste förbättringspunkter ligger i organisation, styrning och efterlevnad inom verksamheterna, samt inom hantering av hotbild och angrepp.

Beskrivning av ärendet

En så kallad Cybersecurity Program Assessment (CPA) har genomförts, vilket är EYs standardiserade ramverk och utarbetade metodologi för granskning och bedömning av mognadsgraden inom organisationers cybersäkerhet CPA-ramverket omfattar analys av 20 områden som delas in i fyra huvudkategorier: Organisation och styrning, tekniska plattformar, dagligverksamhet och hotbildshantering.

De 4 huvudkategorierna som granskats inom uppdraget är:

Organisation och styrning

Tekniska plattformar

Daglig verksamhet

Hotbildshantering

Tidsplanen för arbetet såg ut enligt följande:

- December 2018 – Förberedelser, planering och insamling av dokumentation.
- Januari 2019 – Dokumentanalys, utförande av arbetsmöte (10e januari) samt granskning av kompletterande dokumentation och uppföljningsfrågor.

Februari 2019 – Färdigställande av rapport, faktagranskning av kommunen, samt slutgiltig presentation för förtroendevalda revisorer.

Syftet med granskningen har varit att genomföra en övergripande kartläggning av mognadsgraden i Tyresö kommuns arbete med cybersäkerhet. Kommunen bedöms i relation till andra offentliga organisationer av liknande storlek i förhållande till antal anställda och övergripande verksamhet. Revisorernas övergripande bedömning är att Tyresö kommun har en förhållandevis låg mognadsgrad, med ett snitt på 1,75, på en femgradig skala, men kommunen har ändå vissa tekniska lösningar och processer på plats för att hantera risker i IT-miljön. Mognadsgraden bedöms vara som högst inom drift, tredjepartsupphandling och nätverkshantering. Lägst är mognadsgraden inom hotbildshantering.
Kommunens största och viktigaste förbättringspunkter ligger i organisation, styrning och efterlevnad inom verksamheterna, samt inom hantering av hotbild och angrepp. Vidare finns ett behov av att införa processer för uppföljning inom i stort sett samtliga av de undersökta områdena.

Revisorernas rekommendationer till kommunstyrelsen utifrån granskningens resultat

Organisation och styrning

Tyresö kommun rekommenderas att inleda ett arbete med strategisk cybersäkerhet, som är förankrad från politisk nivå hela vägen ner i verksamheterna. Det bör sättas av pengar specifikt för cybersäkerhet, baserat på rådande situation och hotbild. Från central nivå bör det också följas upp att verksamheten efterföljer de regler och policys som är fastställda. Medarbetares bristande medvetenhet är en mycket vanlig källa till informationssäkerhetsrelaterade incidenter och därför rekommenderas obligatorisk utbildning av nyanställda samt vidareutbildning och uppföljning av

befintliga medarbetare. I denna utbildning bör också ingå att ta del av informationssäkerhetspolicyn.

Tekniska plattformar

Det bör implementeras strategier, policys och instruktioner som täcker hela kommunens användande av tjänster som nås via en uppkoppling till internet, så kallade molntjänster, till skillnad från system som ligger internt inom kommunen. Vidare bör ett kommunövergripande system användas för hantering av samtliga mobila enheter som används för att hantera verksamhetsinformation, exempelvis e-post. Detta system bör ha omgivande strategier, policys och instruktioner.

Daglig verksamhet

Åtkomsthanteringen bör kompletteras med regelbundna granskningar av användare, vilket är särskilt viktigt för konton med priviligierad behörighet. Vidare bör en process finnas där närmsta chef godkänner alla behörigheter enligt en formaliserad process med spårbarhet.

Hotbildshantering

Kommunen bör avsätta resurser för att regelbundet analysera hotbilden och upptäcka angrepp. Vissa angrepp kan ha som syfte att synas, men de som inte vill bli upptäckta kan ha långt värre konsekvenser. Vidare bör det planernas för hantering av cyberincidenter och planerna bör också övas i syfte att berörda ska vara väl insatta i sina uppgifter, samt utvärdera och förbättra planen baserat på övningserfarenheterna.

Nr	Rekommendation	Kommentar		Start	Slut
1	*Organisation och styrning* Tyresö kommun rekommenderas att inleda ett arbete med strategisk cybersäkerhet, som är förankrad från politisk nivå hela vägen ner i verksamheterna.	1.1	Tyresö kommun avser att påbörja detta arbete under 2019 genom deltagande på av MSB anordnad informationssäkerhetsutbildning för roller på strategisk ledningsnivå, i första hand IT-chef.	April (om utbildningsplats kan säkras)	Maj (om utbildningsplats kan säkras)
		1.2	Tyresö kommun avser att påbörja detta arbete under 2019 genom deltagande på av MSB anordnad informationssäkerhetsutbildning för roller med ansvar för det systematiska informationssäkerhetsarbetet, i första hand informationssäkerhetssamordnare (tjänsten ej tillsatt vid datum för denna tjänsteskrivelse)	Avvaktar rekryterin g.	Avvaktar rekryterin g.
2	*Organisation och styrning* Det bör sättas av pengar specifikt för cybersäkerhet, baserat på rådande situation och hotbild.	2.1	En plan för hur informationssäkerhetsarbetet ska finansieras ska tas fram, ambitionen är att ha detta klart innan budget för 2020 är satt.	Mars	Juni
3	*Organisation och styrning* Från central nivå bör det också följas upp att verksamheten efterföljer de regler och policys som är fastställda.	3.1	En rutin för internkontroll av efterföljning av regler och policys ska tas fram.	Kvartal 3	Kvartal 4
4	*Organisation och styrning* Medarbetares bristande medvetenhet är en mycket vanlig källa till	4.1	En rutin för internkontroll ska tas fram kopplat till årlig utredning och	Kvartal 4	Kvartal 1 2020

	informationssäkerhetsrelaterade incidenter och därför rekommenderas obligatorisk utbildning av nyanställda samt vidareutbildning och uppföljning av befintliga medarbetare. I denna utbildning bör också ingå att ta del av informationssäkerhetspolicyn.		nyanställningar när det gäller utbildnings- och informationssatsningar. Webbutbildning och en lathund för användare är framtaget. Under 2019 är ambitionen är att alla medarbetare ska tillgodogöra sig webbutbildningen.		
5	*Tekniska plattformar* Det bör implementeras strategier, policys och instruktioner som täcker hela kommunens användande av tjänster som nås via en uppkoppling till internet, så kallade molntjänster, till skillnad från system som ligger internt inom kommunen	5.1	Styrande dokument för detta ska tas fram under 2019.	Kvartal 2	Kvartal 4
6	*Tekniska plattformar* Vidare bör ett kommunövergripande system användas för hantering av samtliga mobila enheter som används för att hantera verksamhetsinformation, exempelvis e-post. Detta system bör ha omgivande strategier, policys och instruktioner.	6.1	Den befintliga plattformen för hantering av mobila enheter behöver utökas så den inkluderar samtliga mobila enheter som hanterar verksamhetsinformation. Detta kräver utökade medel för systemdrift och licenser vilket det inte finns utrymme för under 2019. Budget för 2020 och framåt måste inkludera detta.	Kv1 2020	Kv4 2020
		6.2	En mobilitetspolicy ska tas fram under 2019.	Kvartal 2	Kvartal 4
7	*Daglig verksamhet* Åtkomsthanteringen bör kompletteras med regelbundna granskningar av användare, vilket är	7.1	En arbetsgrupp ska genomföra en förstudie för ett nytt system för identitet- och åtkomsthantering. Om	Kvartal 2	Kvartal 3

	särskilt viktigt för konton med priviligierad behörighet.		kostnad för nytt system ryms inom befintlig budget kommer en upphandling startas under 2019.		
8	*Daglig verksamhet* Vidare bör en process finnas där närmsta chef godkänner alla behörigheter enligt en formaliserad process med spårbarhet.	8.1	En generell process för hantering av behörigheter skall tas fram. Om processen går att säkerställa med hjälp av befintliga system skall detta göras annars avvaktas nytt system för identitets- och åtkomsthantering.	Kvartal 2	Kvartal 4
9	*Hotbildshantering* Kommunen bör avsätta resurser för att regelbundet analysera hotbilden och upptäcka angrepp. Vissa angrepp kan ha som syfte att synas, men de som inte vill bli upptäckta kan ha långt värre konsekvenser.	9.1	Detta blir delvis en uppgift för informationssäkerhetssamordnaren men IT kommer även planera för införande av system för analys och säkring av loggar samt verktyg för kontinuerliga sårbarhetsanalyser. Om möjligt inom ramen för befintlig budget kommer detta påbörjas under 2019, dock kommer det behövas ökade medel för detta arbete under kommande år.	Kvartal 2	Kvartal 4
10	*Hotbildshantering* Vidare bör det planernas för hantering av cyberincidenter och planerna bör också övas i syfte att berörda ska vara väl insatta i sina uppgifter, samt utvärdera och förbättra planen baserat på övningserfarenheterna.	10.1	En modell för ledning och styrning av it- och informationssäkerhetsincidenter ska tas fram som innefattar risk- och sårbarhetsanalyser samt övningar.	Kvartal 3	Kvartal 4