Tjänsteutlåtande

Kommunstyrelsens förvaltning
Datum 2021-08-29
Dnr 2021/0189

Till Kommunstyrelsen

Svar på revisionsrapport - Granskning av IT- och informationssäkerhet

Sammanfattning

De förtroendevalda revisorerna i Österåkers kommun har under 2021 låtit PWC genomföra granskning av kommunens IT- och informationssäkerhetsgranskning.
Granskningen visar vid en sammantagen bedömning att vi kan förbättra vissa områden samt utöka vårt arbete med informationssäkerhet.
Digitaliseringsavdelningen har bemött revisorernas rekommendationer och föreslagit ett antal åtgärder som redogörs för i detta yttrande.

Beslutsförslag

Kommunstyrelsens arbetsutskott föreslår Kommunstyrelsen besluta

Som yttrande till de förtroendevalda revisorerna överlämna förvaltningens tjänsteutlåtande, daterat 2021-08-29.

Bakgrund

Revisionen har genomförts i syfte att bedöma om kommunen arbetar tillfredställande med IT och informationssäkerhet.
Frågan om informationssäkerhet är inte enbart en IT-teknisk fråga då många av frågeställningarna som utreds handlar om hur verksamheten hanterar sin information.
För att få med verksamhetens perspektiv bjöds kommunens största förvaltning, produktionsförvaltningen, in att delta i granskningsarbetet.

PWC använde sig av ramverket NIST (National Institute of Standards and Technology).
NIST ramverket ställer högra krav på organisationer ifråga om IT- och informationssäkerhet och mycket fokus i ramverket ligger på dokumentation, tydliga roller och dedikerade resurser och mindre fokus läggs på det operativa arbetet som faktiskt genomförs.

Således har revisionen genomförts baserat på intervjuer, granskningar av dokument och uppföljningsrutiner. Mycket av arbetet i detta område sker digitalt (inte statiska dokument) hos digitaliseringsavdelning, vilket inte riktigt har varit kompatibelt med NIST.
I revisionsrapporten sammanfattas ett flertal rekommendationer, som adresseras nedan.

Förvaltningens svar på PwC:s granskning

Rekommendation 1:
Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat. Säkerställ att samtlig dokumentation är uppdaterad och giltig och att all dokumentation

ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.

Åtgärdsförslag:
Dokumenthanteringsplanen bör uppdateras så att de viktigaste informationssäkerhetsprocesserna omfattas av denna. På så sätt kommer uppdateringsintervall att tydliggöras samt att det finns en central sammanhållning av dessa dokument.

Rekommendation 2:
Ta fram en formaliserad Disaster Recovery Plan. Säkerställ att eventuella systemägare med ansvar för att ta fram återställningsplaner är införstådda med detta ansvar.

Åtgärdsförslag:
Digitaliseringsavdelningen har inlett arbete med att ta fram en formell Disaster Recovery Plan. Arbetet omfattar planer för dels enskilda kritiska system, dels planer för den centrala driftmiljön. Digitaliseringsavdelningen har sedan tidigare arbetat fram dessa rutiner samt mycket teknisk infrastruktur med bland annat en sekundär driftsplats, men detta kommer nu formaliseras bättre.

Rekommendation 3:
Formalisera sårbarhetshanteringen med definierade processer för hantering att upptäcka sårbarheter.

Åtgärdsförslag:
Sårbarhetshanteringen som idag till stor del sköts med manuell hantering och rutiner av nyckelpersoner på avdelningen kommer kartläggas och processer och rutiner skapas för att minska personberoendet, upptäckta sårbarheter så att de hanteras och analyseras konsekvent och systematiskt.

Rekommendation 4:
Säkerställ att alla kommunalt anställda genomgår utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
Utred huruvida det finns ett behov av rollbaserade utbildningar och övningar baserat på arbetsuppgifter, ansvar och behörigheter.

Åtgärdsförslag:
Det finns ett behov av utbildningar och övningar för att säkerställa kompetens hos alla anställda kring informationssäkerhet. Detta arbete bedrivs redan idag, men behöver utökas. En kartläggning kommer göras över olika personalgrupper för att se om vissa grupper behöver riktade utbildningar utifrån de uppgifter som de utför.

Rekommendation 5:
Komplettera processkartan för incidenthantering med en tydlig incidenthanteringsplan.

Rekommendation 6:
Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.

Rekommendation 7:
Säkerställ att återföring av lärdomar efter samtliga informationssäkerhetsincidenter görs genom att

kravställa detta i relevant dokumentation, samt se till att det är känt inom organisationen och att det finns en dedikerad resurs som ansvarar för att detta sker.

Åtgärdsförslag (rekommendation 5, 6 och 7):
Digitaliseringsavdelningen tillsammans med dataskyddsombud och säkerhetschef bör starta ett projekt kring incidenthantering och ta fram en tydlig plan för hur incidenter hanteras. Detta innebär framför allt att ta fram en operativ incidenthanteringsplan med praktiska rutiner för olika delmoment i incidenthanteringen, bland annat kring utvärdering och återföring av information.
Återföring av lärdomar sker idag i första hand internt inom avdelningen, vilket behöver utökas till att hela organisationen får information på lämpligt sätt.

Rekommendation 8:
Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.

Åtgärdsförslag 8:
Idag är digitaliseringsavdelningen i relativt stor utsträckning personberoende, framförallt vid plötsligt/kortare personalbortfall. För att minska beroendet kommer ett arbete genomföras för att ta fram de mest kritiska beroendena och där göra insatser för att minska beroendet, bland annat genom utbildningar och informationsöverföring.

Förvaltningens slutsatser

Förvaltningen jobbar ständigt med att ha en så säker miljö som möjligt utifrån de tekniska arv och förutsättningar som finns. Revisionen påvisar dock att detta arbete behöver formaliseras och tydliggöras. Förvaltningen har gett åtgärdsförslag på revisionens åtta rekommendationer som bör genomföras.
Förvaltningen anser därför att arbetet kring IT- och informationssäkerhetsgranskningen är besvarad.

Bilagor

Revisionsrapport IT och informationssäkerhetsgranskning.

Staffan Erlandsson
Kommundirektör

Magnus Bengtsson
Ekonomidirektör

Stefan Nyberg
CIO

Expedieras
De förtroendevalda revisorerna
PWC
Akt

Digitala Signaturer

Signerad med: Anställda
Signerad av: Stefan Nyberg, CIO
Datum: 2021-09-07 09:07 +02:00

Signerad med: Anställda
Signerad av: Staffan Erlandsson, Kommundirektör
Datum: 2021-09-07 09:15 +02:00

Signerad med: Anställda
Signerad av: Magnus Bengtsson, Ekonomidirektör
Datum: 2021-09-07 11:47 +02:00