KS § 9:6 Dnr. KS 2018/0165

Svar på revisionsrapport - Granskning av intrångsskydd

Kommunstyrelsens beslut

Godkänna kommunstyrelsens kontors handlingsplan enligt tjänsteutlåtande 2018-08-22.

Sammanfattning

Under första kvartalet 2018 genomfördes en granskning av intrångsskyddet av PwC på uppdrag av kommunens revisorer. För att höja IT-säkerheten föreslår revisorerna att kommunstyrelsen tar fram en handlingsplan med begäran om svar senast den 30 september 2018.

Beslutsunderlag

- Kommunstyrelsens arbetsutskott har behandlat ärendet 2018-09-05, § 7:3.
- Kommunstyrelsens kontors tjänsteutlåtande daterat 2018-08-22.

Förslag till beslut

Michaela Fletcher (M) yrkar bifall till arbetsutskottets beslutsförslag innebärande att godkänna kommunstyrelsens kontors handlingsplan enligt tjänsteutlåtande 2018-08-22.

Propositionsordning

Ordföranden frågar om Kommunstyrelsen beslutar enligt Michaela Fletchers (M) yrkande och finner att så är fallet.

Expedieras

- Förtroendevalda revisorerna
- PWC
- Kommunkansliet

Österåker

Tjänsteutlåtande

Kommunstyrelsens kontor
Datum 2018-08-22
Dnr 2018/0165

Till Kommunstyrelsen

Svar på KS 2018/0165-01 - Revisionsrapport - Granskning av intrångsskydd

Sammanfattning

Under första kvartalet 2018 genomfördes en granskning av intrångsskyddet av PwC på uppdrag av kommunens revisorer. För att höja IT-säkerheten föreslår revisorerna att kommunstyrelsen tar fram en handlingsplan med begäran om svar senast den 30 september 2018.

Beslutsförslag

Kommunstyrelsens arbetsutskott föreslår kommunstyrelsen besluta
Godkänna kommunstyrelsens kontors handlingsplan enligt tjänsteutlåtande 2018-08-22

Bakgrund

IT enheten har under 2017 påbörjat arbetet med att kartlägga sårbarheter i IT säkerheten, bland annat genom att tillsammans med kommunens säkerhetsstrateg genomföra informationssäkerhetsklassning på kommunens verksamhetssystem för att kartlägga skyddsbehovet på de enskilda systemen. I december 2017 genomfördes en granskning av intrångsskyddet med hjälp av en extern leverantör för att kartlägga tekniska sårbarheter.
Utifrån det påbörjades en åtgärdsplan 2017 av IT enheten som bland annat innefattar

- Nytt utökat skalskydd (Brandvägg)
- Verktyg baserat på AI (Artificiell Intelligens) för att upptäcka systemavvikelser
- Uppdateringar av rutiner vid extern anslutning mot system.

IT-enhetens svar på PwC:s granskning

- IT-avdelningen uppmärksammade PwC:s angrepp och notifierade PwC att de blivit upptäckta cirka en timme efter att försöken påbörjades, vilket är mer än godkänt.

  Svar: IT-enheten vill tydliggöra att som rapporten visar så upptäcktes intrångsförsöket snabbt varpå larm skickades ut och kommunens säkerhetsstrateg informerades. Det hade normalt resulterat i åtgärder från vår sida, dvs. det är inte alls omöjligt att deras fullbordade intrång hade misslyckats.

- Under PwC:s tester hanterades den upptäckta incidenten på ett ändamålsenligt sätt. Det finns en muntlig process för hur incidenter skall hanteras och vilka som skall informeras.

Tyvärr finns inte rutinen dokumenterad.

Svar: Arbete med att dokumentera rutiner och riktlinjer är påbörjat, vilket kan ses i bilaga handlingsplan IT-säkerhet.

- IT-säkerheten håller en låg nivå och säkerheten avseende intrång av extern och intern aktör behöver prioriteras för att minimera framtida incidenter. PwC kunde skaffa högsta behörighet i domänen vilket inte borde vara möjligt

Svar: Som man kan läsa i den sekretessbelagda tekniska beskrivningen (*Intrångsanalys* avsnitt *Internt penetrationstest* sidan 9) skedde intrånget med en anslutning direkt till vårt administrativa nät, i våra låsta lokaler innanför brandväggen.
Det intrång som gjordes hade inte varit möjligt att fullborda utan dessa förutsättningar, vilket i normala fall skulle begränsa intrånget till att utföras av/genom anställd eller person med fysisk tillgång till våra lokaler.

De sårbarheter som upptäcktes tillgängliga externt, dvs utanför våra lokaler, eller från internet kunde inte ge åtkomst till information eller annan behörighet, utan endast för att skapa en bättre bild av vår IT-miljö och eventuellt utnyttjas för överbelastningsattacker.

De sårbarheter med riskgradering hög beror också på tidigare val gjorda av våra verksamheter, ett exempel är vårt tidigare ekonomisystem Visma RoR som lever kvar och är enbart till för våra revisorer och ekonomisk historik. Det finns inget supportavtal kvar på RoR och vi kan således inte uppdatera servern.
Vi är väl medvetna om dessa och har begränsat dessa system så mycket som möjligt för extern åtkomst. Helst skulle vi vilja stänga ned dessa, men det blir då på bekostnad av verksamheternas IT-stöd.
För att stävja liknande beslut framgent upprättades 2016 en IT-styrgrupp för att bland annat ge IT-enheten möjlighet att styra vilka systemval som görs av verksamheterna så att vi bygger en IT-miljö så att vi bygger en homogen IT-miljö som ges möjlighet att förvalta och underhålla på ett ändamålsenligt sätt.

- PwC har inte kunnat ta del av någon roll- eller ansvarsfördelning som avser kommunens IT-säkerhetsarbete.

Svar: Det har under året upprättats en Dataskyddsorganisation inom kommunen, främst för att stödja arbetet med nya dataskyddsförordningen GDPR. Men den nya organisationen kommer arbeta med att granska och övervaka efterlevnaden av

organisationens strategier i dataskyddsfrågor.

- PwC har inte kunnat ta del av någon dokumentation eller information som beskriver kommunens förebyggande arbete kring IT-säkerhet.

  Svar: Arbete med att förebygga risker kring IT-säkerheten är uppgifter som ingår i det dagliga arbetet varpå särskild dokumentation inte finns i nuläget, vi har dock tagit till oss av PwCs rutiner och arbetet med att tydliggöra rutiner och riktlinjer är påbörjat.

- Det finns inte några skrivna rutiner eller riktlinjer idag. Enligt uppgift pågår ett arbete med att dokumentera processen.

  Svar: Arbete med att förebygga risker kring IT-säkerheten är uppgifter som ingår i det dagliga arbetet varpå särskild dokumentation inte finns i nuläget, vi har dock tagit till oss av PwCs rutiner och arbetet med att tydliggöra rutiner och riktlinjer är påbörjat.

Förvaltningens slutsatser

IT-enheten jobbar ständigt med att ha en så säker miljö som möjligt utifrån de tekniska arv och förutsättningar som finns. I den sekretessbelagda tekniska rapport som IT-enheten har fått av PwC framgår att

- **7 st av de 8 sårbarheterna som är riskgraderade som hög genomfördes när PwC var direkt anslutna till det interna nätet**
- **IT-enheten fick av loggsystem larm inom en timme att det förekom avvikande aktiviteter i systemmiljön vilket i normala fall hade resulterat i åtgärder.**
- **Den sårbarhet som klassas som riskgrad hög vid det externa penetrationstestet kommer åtgärdas under början av hösten, arbetet är påbörjat.**
- **IT-enheten jobbar vidare med att dokumentera de inarbetade rutinerna som enligt PwC uppenbarligen fungerar.**
- **Utökning av skalskydd (brandvägg och redundant internetuppkoppling) är ett pågående arbete som kommer slutföras under hösten 2018.**
- **Det penetrationstest som beställdes av IT-enheten i december visar på en riskmedvetenhet och att IT-säkerhetsarbetet är ett kontinuerligt arbete som ständigt förändras där vi nyttjar expertis för att kartlägga sårbarheter.**

Tjänsteutlåtande

Förvaltningen anser med ovanstående redovisning att arbetet kring IT-säkerheten och revisorernas granskning är besvarad.

Bilagor

1. Handlingsplan IT-säkerhet

Jan-Olof Friman
Kommundirektör

Stefan Nyberg
IT-chef

Österåker

Handlingsplan IT säkerhet

1. Handlingsplan

IT-enheten har under 2017 och 2018 genomfört en del åtgärder som upptäcktes under de båda granskningarna av intrångsskydd, bland annat har de säkerhetshot som bedömdes som hög åtgärdats. De berodde på att gamla servrar hade startats under tiden för granskningen för att utföra ett test hos IT-enheten. Rutiner kring start av äldre system har uppdaterats.

Nedan följer handlingsplan av planerade åtgärder, IT-säkerhet är ett fortlöpande arbeta varpå handlingsplanen uppdateras allt eftersom arbetet fortlöper.

Åtgärd	Status	Ansvarig	Slutdatum
Uppdatering rutiner drift	Slutförd	IT-enheten	Maj 2018
Dataskyddsorganisation	Slutförd	Kommunledning	Augusti 2018
Lösenordspolicy systemkonton	Pågående	IT-enheten	Oktober 2018
Riktlinje extern anslutning	Slutförd	IT-enheten	Augusti 2018
Uppdatering IT styrdokument	Pågående	IT-enheten	December 2018
Uppdatering brandvägg	Upphandling pågår	IT-enheten	November 2018
Informationssäkerhetsklassning	Slutförd	Säkerhetsstrateg	Maj 2018
Redundant internetkoppling	Upphandling pågår	IT-enheten	Oktober 2018
Säker inloggning webmail	Pågående	IT-enheten	Oktober 2018
Anslutning eIDAS	Pågående	IT-enheten	September 2018