Uppföljande granskning av IT- och informationssäkerhet

Solna stad

Granskning av IT- och informationssäkerhet
Februari 2022

Anders Hägg (anders.hagg@pwc.com) - Uppdragsledare
Nur Nauti (nur.nauti@pwc.com) - Projektledare
Carl Nisser (carl.nisser@pwc.com) - Projektmedlem

1. Sammanfattning

De förtroendevalda revisorerna för Solna Stad har gett PwC i uppdrag att genomföra en granskning av stadens IT- och informationssäkerhet för att besvara ett antal övergripande revisionsfrågor kopplade till IT-och informationssäkerhet. Revisionsfrågorna som använts i granskningen är baserade dels på observationer från tidigare gjord sårbarhetsgranskning från 2018 av PwC, men också utifrån PwCs samlade praxis för hur organisationer bör organisera sitt löpande arbete inom IT- och informationssäkerhet.

Efter genomförd granskning är PwCs samlade bedömning att Solna Stad överlag har bra rutiner och arbetssätt på plats gällande IT och informationssäkerhet men att vissa delar har förbättringspotential. PwC ser att positiv utveckling skett hos Solna Stad de senaste året då de akuta säkerhetsbrister som identifierats av PwC 2018 är idag åtgärdade. PwC kan utöver detta se att Solna Stad arbetar systematiskt med IT- och informationssäkerhet utifrån ett framtaget ledningssystem för informationssäkerhet (LIS) enligt ISO 27001.

PwC har dock noterat ett antal områden som behöver förbättras för att uppnå en än högre nivå av säkerhet av stadens informationstillgångar. Detta berör att det finns en möjlighet att tydliggöra och således utvärdera möjligheten att inkludera relevanta kontroller som utförs i organisationen kopplat till IT och informationssäkerhet i stadens befintliga systemstöd för internkontroll för regelbundet återkommande IT- och informationssäkerhetsaktiviteter.

PwC noterade även ett par förbättringsområden i förhållande till stadens riskhantering. Då kommunstyrelsen är informationsägare och därmed även riskägare är det kommunstyrelsen som måste delegera och säkerställa att riskanalyser genomförs systematiskt och att risker åtgärdas. Idag finns det inte tillräcklig kontroll och uppföljning av att risker identifieras i verksamhetsspecifika system.

Vidare har PwC identifierat rekommendationer kopplat till incidenthantering och anlitande av externa leverantörer. I rapporten går det att läsa detaljerat material om samtliga dessa punkter, ett axplock presenteras här intill.

Nedan redovisar vi våra mest väsentliga rekommendationer:

PwC rekommenderar kommunstyrelsen att;

- Utvärdera möjligheten att inkludera relevanta kontroller som utförs i organisationerna kopplat till IT och informationssäkerhet i stadens befintliga systemstöd för internkontroll. För att få systematik i kontinuerligt förbättringsarbete kan staden använda sig av ett årshjul med aktiviteter kopplade till respektive månad. Varje aktivitet bör ha en beskrivning för vad aktiviteten omfattar samt vem som ansvarar för dess genomförande.
- Tydliggör och komplettera beskrivning av framtagna informationsklasser med krav kopplat till hanteringen.
- Säkerställa efterlevnad och genomförande av omfattande riskanalys på systemnivå i samtliga förvaltningar med bäring på IT- och informationssäkerhet. Det är förvaltningarna som ska ha ansvaret för att driva identifieringen av risker och de informationstillgångar som är relevanta att skydda, men att centrala funktioner tillhandahåller nödvändig resurser, mandat och tydliga roller för att stödja dess genomförande.
- Fortsätt arbetet med att utöka och formalisera anvisningar för hur hantering av IT-och informationssäkerhetsincidenter ska hanteras i en separat rutin. En sådan rutin bör innehålla en tydlig mottagare av incidentlarm, hanteringsregler för olika typer av incidenter, ett verktyg för att samla alla incidenter samt instruktioner för eventuell eskalering av ärenden. En viktig del i incidenthanteringen är att informera/utbilda användarna i att kunna identifiera och rapportera incidenter.
- Införa gemensam rutin för att regelbundet följa upp att kritiska driftleverantörer samt systemleverantörer för verksamhetskritiska system testar återläsning av säkerhetskopior. Testerna bör dokumenteras och tillhandahållas Solna Stad.

2. Inledning

2.1 Bakgrund

Allt fler allvarliga cybersäkerhetsincidenter har de senaste åren drabbat såväl privat som offentlig sektor, både i Sverige och runtom i världen. En gemensam beståndsdel i flera av de mest allvarliga fallen är information som på ett eller annat sätt kommit obehöriga tillhanda, antingen genom bristande rutiner och hantering eller genom yttre påverkan, i vissa fall en kombination av dem båda. Myndigheten för samhällsskydd och beredskap konstaterar att så gott som all brottslighet i det moderna samhället har koppling till IT.

Ett gott informations-och cybersäkerhetsarbete är beroende av en god styrning. Ledningen ska vara engagerad och ha kunskap om informations- och cybersäkerhetsarbetet. Ledningen ska vidare ge den strategiska inriktningen och säkerställa att det finns tillräckligt med resurser och mandat i organisationen för att kunna bedriva arbetet. Det är ledningens kravställning som ytterst styr verksamheten och det är därmed ledningen som ska säkerställa att det bedrivs ett cyber- och informationssäkerhetsarbete som är i linje med externa och interna krav.

Mot bakgrund av detta och som ett led i förverkligandet av Solna Stads revisionsstrategi har kommunen i sin riskbedömning för 2021 bedömt att en granskning av informations- och IT-säkerheten behöver genomföras för Solna Stad.

Granskningen genomförs enligt revisionsplan 2021 som baseras på revisorernas riskbedömning.

2.2. Syfte och revisionsfråga

Syftet med granskningen är att besvara revisionsfrågan:

Säkerställer kommunstyrelsen att den tar sitt informationsägaransvar på ett ändamålsenligt sätt?

För att svara på ovan fråga har följande underliggande revisionsfrågor beaktats:

- Finns det fastställda informationssäkerhetskrav (rutiner, tekniska skyddsåtgärder & kompetens) i befintliga avtal?
- Följs avtal upp?
- Har kommunstyrelsen säkerställt att kommunen har ändamålsenliga policys, rutiner och beskrivningar gällande informationssäkerhet?
- Finns det dokumenterade rutiner för att kontinuerligt identifiera och hantera risker?
- Finns det en adekvat övergripande styrning för ett systematiskt informationssäkerhetsarbete?

2.3. Revisionskriterier

Revisionskriterierna för denna granskning har hämtats ur följande:

- Kommunallagen
- Internationella standarder enligt ISO (International Organization for Standardization) avseende Informationsteknik, Säkerhetstekniker och Ledningssystem för informationssäkerhet (ISO 27001:2013)
- Internationella standarder enligt COBIT (Control Objective for Information and Related Technology Standards) avseende informationssäkerhet.

2. Inledning

2.4 Kontrollmål

Kontrollmålen och bedömningen av dessa möjliggör att revisionsfrågan kan besvaras. Följande kontrollmål har bedömts som viktiga för granskningen:

1. Hur har Solna stad fortsatt arbetat med identifierade sårbarheter baserat på tidigare genomförda sårbarhetsgranskningar (främst under 2018 genomförd intrångsgranskning)?
2. Finns det en tydlig roll- och ansvarsfördelning i staden kring den övergripande IT- säkerheten utifrån antagna riktlinjer och anvisningar?
3. Har kommunstyrelsen säkerställt att kommunen har ändamålsenliga policys, rutiner och beskrivningar gällande Informationssäkerhet?
4. Finns det dokumenterade rutiner för att kontinuerligt identifiera och hantera risker?
5. Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?
6. Finns formellt beskrivna rutiner för hantering av outsourcing till externa leverantörer, exempelvis former för kravställande och kommunikation, avtal och uppdatering av dessa, samt uppföljning av efterlevnad av avtal?

2.5 Metod

Granskningen har utförts enligt god revisionssed med utgångspunkt i ”Vägledning för verksamhetsrevision i kommuner och landsting” från Sveriges kommunala yrkesrevisorer (SKYREV). Granskningen av processer inom IT-säkerhet utfördes genom intervjuer med berörda personer samt granskning av relevant dokumentation.

Följande personer har varit intervjuade i granskningen:

Solna Stad:
- Helen Holst (IT-chef)
- Fredrik Hagnelöf (Tf IT-chef)
- Peter Adolfsson (Informationssäkerhetsansvarig)
- Hans Tideborg (Fd IT-säkerhetsansvarig)
- Elisabet Sundelin (Chef Omvårdnadsförvaltning)

Granskningen har genomförts under februari 2022 av Nur Nauti och Carl Nisser (PwC) och kvalitetssäkrats av Anders Hägg (Uppdragsledare) på PwC samt faktakontrollerats av företrädare i organisationen.

2.6 Avgränsningar

I tid avgränsas granskningen till år 2022 samt till granskningens kontrollfrågor. Då IT-säkerhetsgranskningen 2018 av Solna Stad genomfördes med hjälp av externa tester (blackbox-pentest) är det inte möjligt att tekniskt verifiera effektiviteten i genomförda åtgärder under denna granskning. Vidare har eventuella resultat från denna granskning inte validerats för att bedöma utförandet av kontrollerna i omfattningen. Bedömning och PwC:s synpunkt har baserats på den inkomna dokumentationen och de intervjuer som genomförts med identifierade intressenter.

3. Resultat av granskningen - uppföljande kontrollmål

Uppföljande kontrollmål från tidigare genomförd IT-säkerhetsgranskning

Under 2018 genomförde PwC en granskning av det externa och interna intrångsskyddet i Solna Stads IT-miljö där ett antal brister noterades samt där förslag på åtgärder presenterades.

Följande högrisk observationer som hittades innefattade:

1. Svag lösenordspolicy/antal domänadminstratörer
2. SMB V1 (MS17-010)
3. Applikationsserver med svaga autentiseringsuppgifter
4. Brist i design av tvåfaktorsautentisering
5. SMB signering krävs ej

Följande sidor innehåller en detaljerad beskrivning över bakgrundsförklaring till tidigare observerade sårbarheter från IT-säkerhetsgranskning genomförd 2018 med tillhörande statusuppdatering och bedömning.

3. Resultat av granskningen - uppföljande kontrollmål

3.1.1 Hur har Solna stad fortsatt arbetat med identifierade sårbarheter baserat på tidigare genomförda sårbarhetsgranskningar från 2018?

Iakttagelser - Svag lösenordspolicy och högt antal domänadministratörer

Under granskningen som genomfördes 2018 av PwC noterades att policyn i Active Directory saknade flera konfigurationer som skulle göra miljön säkrare. Lösenordspolicyn var svag och tillät lösenord som är 8 tecken. Mekanismen för utlåsning av konton tillåter 50 försök och låser ut kontot i 15 minuter. Detta möjliggjorde för en eventuell angripare att gissa lösenorden till konton, med god chans att inte låsa dem. Lösenordspolicyn tillåter även att lösenordet sätts till lättgissade lösenord. Det fanns även ett större antal domänadministratörer (120) än vad som normalt är nödvändig.

Status 2022:

I förhållande till svag lösenordspolicy och revidering av antalet domänadministratörer har Solna stad arbetat med att åtgärda identifierade sårbarheter. En ny lösenordspolicy i enlighet med best-practice är upprättad och antalet domänadministratörer är kraftigt reducerade. Vidare har Solna Stad implementerad behovsprövad tilldelning för höga behörigheter mht infrastrukturkomponenter.

Bedömning

Vår bedömning är att Solna Stad har uppnått en tillräcklig nivå gällande hantering av tidigare identifierad sårbarhet i förhållande till svag lösenordspolicy och minimera antal domänadministratörer.

3. Resultat av granskningen - uppföljande kontrollmål

3.1.2 Hur har Solna stad fortsatt arbetat med identifierade sårbarheter baserat på tidigare genomförda sårbarhetsgranskningar från 2018?

Iakttagelser - SMB V1 (MS17-010)

Under den sårbarhetsgranskning som genomfördes 2018 av PwC noterades att SMB V1 innehöll en sårbarhet vilken innebar att en oautentiserad angripare kunde skicka egentillverkade paket och på så vis tillskansa sig rätten att exekvera kod på systemet. Sårbarheten utnyttjades av det kända ransomware **WannaCry** vilket har fått stort utrymme i media på grund av dess förödande effekter hos företag och myndigheter.

***Status 2022*:**

Server Message Block (SMB) är ett nätverksprotokoll för applikationslager som vanligtvis används i Microsoft Windows för att ge delad åtkomst till filer och skrivare. Under granskningen framkom att Solna Stad har installerat de säkerhetsuppdateringar som Microsoft har släppt i förhållande till SMB V1 protokollet. Vidare har Solna Stad med hjälp av driftsleverantör infört förbättrad nätverkssäkerhet på samtliga platser där SMB V1 har förekommit. Vidare har, utöver driftleverantörens verktyg, interna analysverktyg implementerats i syfte att regelbundet scanna serverparker efter kända sårbarheter.

IT-avdelningen sammanträder tillsammans med driftleverantör en gång per månad där stående punkt på agenda är hantering av identifierade sårbarheter mht stadens serverpark.

Bedömning

Vår bedömning är att Solna Stad har uppnått en tillräcklig nivå gällande hantering av tidigare identifierad sårbarhet i förhållande till SMB V1 (MS17-010).

3. Resultat av granskningen - uppföljande kontrollmål

3.1.3 Hur har Solna stad fortsatt arbetat med identifierade sårbarheter baserat på tidigare genomförda sårbarhetsgranskningar från 2018?

Iakttagelser - Applikationsserver med svaga autentiseringsuppgifter

Under den sårbarhetsgranskning som genomfördes 2018 av PwC noterades att administratörsgränssnittet till applikationsservrar identifierades ha kvar de inloggningsuppgifter som tilldelats vid installation. En angripare skulle enkelt kunna autentisera sig som administratör och på så vis anskaffa sig fulla rättigheter att utnyttja systemet.

Som administratör har en angripare möjlighet att ladda upp egna applikationer med skadlig kod på servern.

Status 2022:

Under granskningen framkom att Solna Stad i förhållande till applikationsservrarne med svaga autentiseringsuppgifter bytt till unika och starka lösenord för berörda tjänster i enlighet med uppdaterad lösenordspolicy. Vidare framkom även att det inom IT-avdelningen har tagits fram checklistor för att säkerställa att standardkonfigurationer inte är aktiva då en server rullas ut i produktionsmiljö. Idag sker provisionering av servrar utifrån en framtagen standardiserad metod.

Bedömning

Vår bedömning är att Solna Stad har uppnått en tillräcklig nivå gällande hantering av tidigare identiferad sårbarhet i förhållande till applikationsserver med svaga autentiseringsuppgifter.

3. Resultat av granskningen - uppföljande kontrollmål

3.1.4 Hur har Solna stad fortsatt arbetat med identifierade sårbarheter baserat på tidigare genomförda sårbarhetsgranskningar från 2018?

Iakttagelser - Brist i design av tvåfaktorsinloggning

Under den sårbarhetsgranskning som genomfördes 2018 av PwC noterades att det var möjligt för en angripare att ändra telefonnumret som engångskoder skickas till i **Exchange**. En angripare som gissat lösenordet till ett konto med rättigheter till **Exchange** och **Citrix** kunde byta telefonnumret som engångslösenord skickas till. Detta gjorde att en angripare eventuellt kunde logga in på Citrixportalen och på det sättet nå det interna nätverket.

Status 2022:

PwC har under granskningen noterat att Solna Stad har tagit fram multifaktorslösningar för att hantera sårbarheten. För externa entreprenörer används numer BankID, medans internt används Windows Hello och Windows Authenticator. Det har även kommunicerats att ett MFA(multifaktorsautentisering) projekt är igångsatt för att än mer säkerställa att säker autentisering används i Solna stads IT-miljö.

Bedömning

Då bedömningspunkten är av ett sådan teknisk karaktär kan PwC inte ge ett definitivt utlåtande huruvida den tidigare funna bristen gällande Citrixportalen är åtgärdad. Givet informationen som kommit fram gör PwC ändå bedömningen att rimliga åtgärder har implementerats och att Solna Stad har uppnått en tillräcklig nivå gällande hantering av tidigare identifierad sårbarhet.

3. Resultat av granskningen - uppföljande kontrollmål

3.1.5 Hur har Solna stad fortsatt arbetat med identifierade sårbarheter baserat på tidigare genomförda sårbarhetsgranskningar från 2018?

Iakttagelser - Återanvänt lösenord för administratörskonto

Under den sårbarhetsgranskning som genomfördes 2018 av PwC kunde vi verifiera att ett flertal servrar på nätverket använder samma lösenord för det lokala kontot **Administrator**. Detta möjliggör för en angripare som har åtkomst till en av dessa servrar att få åtkomst till de servrar som har samma lösenord för kontot **Administrator**.

Status 2022:
Under granskningen noterades att administratörskonton och servicekonton numera inte delar lösenord. Utöver en förstärkt lösenordspolicy delgavs PwC information om att;

- Tjänstekonton skapas utanför IAM-systemet direkt i stadens tjänstekatalog.
- Lösenord är slumpgenererade och innehåller minst 14-tecken i enlighet med beslutad lösenordspolicy.
- Lokala adminstratörskonton är enbart kända av driftsleverantör och har unika lösenord per enskild server.

Ovan är samtliga åtgärder som vidtagits i syfte att adressera sårbarheten i förhållande till återanvändande av lösenord för administratörskonto.

Bedömning

Vår bedömning är att Solna Stad har uppnått en tillräcklig nivå gällande hantering av tidigare identifierad sårbarhet i förhållande till återanvänt lösenord för administratörskonton. För att ytterligare stärka Solna Stads säkerhetspositionering mht hantering av administratörskonton rekommenderar PwC kommunstyrelsen att:

- I enlighet med driftleverantörs rekommendation implementera “Restricted Groups” funktion i IAM-plattformen.
- Utvärdera behovet att häva behörighet “lokal admin” för personal inom Servicedesk.

Se område 3.1.5 i appendix för mer information om iakttagelser och rekommendationer.

3. Resultat av granskningen

3.2 Finns det en tydlig roll- och ansvarsfördelning i staden kring den övergripande IT- och informationssäkerheten utifrån antagna riktlinjer och anvisningar?

Iakttagelser

Solna Stad har i sina stadsövergripande anvisningar klargjort ansvarsfördelningen kring IT och informationssäkerheten inom staden. Identifierade nyckelroller är *Informationssäkerhetsansvarig*, *IT-säkerhetsansvarig*, och *IT-chef* med tillhörande ansvarsområden i förhållande till IT- och informationssäkerhet.

Ansvariga över IT-och informationssäkerhet är centralt lokaliserade i staden. Deras ansvarsområden inkluderar både strategiskt, operativt och taktiskt stöd för stadens övergripande IT- och informationssäkerhetsarbete. Vidare agerar även den centraliserade funktionen kravställare gentemot nämnderna som i sin tur ansvarar för de operativa informationssäkerhetsarbetet i sina respektive verksamheter.

Ansvarsområden i förhållande till ovan angivna roller innefattar bland annat:

- Upprätthållande av ledningssystem för informationssäkerhet
- Genomförande av utbildningar och andra medvetandehöjande åtgärder
- Uppföljning och metodstöd för nämndernas operativa informationssäkerhetsarbete

På verksamhetsnivå noterades under granskningen att informationsägare finns utpekade samt tillhörande dataskyddsombud för att hantera personuppgiftsrelaterade frågeställningar.

Bedömning

Vår bedömning är att Solna Stad i nuläget har en tillräcklig nivå kring ansvarsfördelning kring IT- och informationssäkerheten i staden.

3. Resultat av granskningen

3.3 Har kommunstyrelsen säkerställt att staden har ändamålsenliga policys, rutiner och beskrivningar gällande Informationssäkerhet?

Iakttagelser

Solna Stad har flera styrande dokument gällande IT- och informationssäkerhet. IT och informationssäkerhetspolicys har tagits fram och kommunicerats ut. Lejonparten av beskrivningar gällande informationssäkerhet finns konkretiserat i "Stadsövergripande anvisningar för IT och Informationssäkerhet" som bygger på ISO 27001-standarden för Ledningssystem för informationssäkerhet (LIS). I dessa framgår det i detalj hur Staden kräver att samtliga arbetar både på central nivå och ute i nämnder/förvaltningar mht till informationssäkerhet. PwC noterade dock att flertalet av framtagna policys, rutiner och beskrivningar gällande informationssäkerhet inte har reviderats på över 3 år, det framkom dock att dessa kontrolleras minst två gånger årligen och förslag till förändring hanteras vid behov som ett ärende till KS/KF. Styrdokument som gåtts igenom har fastställts av kommunfullmäktige och rutiner för uppföljning finns.

Vidare noterade PwC att det idag finns informella kontroller för IT- och informationssäkerhet. Staden har ett välfungerande styrsystem för internkontroll, däremot kunde PwC under granskningen inte verifiera att IT- och informationssäkerhetskontroller har inkluderats i stadens systemstöd för internkontroll (Stratsys).

Vad gäller arbetet med informationsklassificering noterades att Solna Stad har tillämpat KLASSA framtaget av Sveriges kommuner och regioner (SKR). Det finns en god kännedom om vart och inom vilka förvaltningar känsliga informationsmängder finns. Däremot noterades att det saknas tydliga hanteringsrutiner i relation till respektive informationsklass.

Bedömning

Vår bedömning är att Solna Stad i nuläget delvis har en tillräcklig nivå gällande styrande dokument. Vi noterade ett antal förbättringsmöjligheter för Solna Stad. Följande rekommendationer lämnas mot bakgrund till iakttagelserna:

PwC rekommenderar kommunstyrelse att;

- Formalisera och utvärdera möljighet att inkludera regelbundet återkommande arbetsmoment och kontroller mht IT- och informationssäkerhet i stadens befintliga systemstöd för internkontroll.
- definiera tydliga hanteringsrutiner för informationstillgångar kopplat till vilken klassning man tilldelats.

Se område 3.3 i appendix för mer information om iakttagelser och rekommendationer.

3. Resultat av granskningen

3.4 Finns det dokumenterade rutiner för att kontinuerligt identifiera och hantera risker?

Iakttagelser

Solna Stad har tagit fram etablerade och dokumenterade rutiner för riskanalyser som tillämpas både på stadsövergripande nivå och systemnivå. Kommunstyrelsen har därmed gett i uppdrag till stadsledningsförvaltningen samt fackförvaltningar att verkställa detta. Stadsövergripande riskanalyser mht IT-och informationssäkerhet genomförs årligen eller då förändringar genomförs. Vidare är det angett att riskanalyser på systemnivå mht IT-och informationssäkerhet ska genomföras.

Under granskningen noterades att det i dagsläget saknas uppföljning av riskanalys på förvaltningsnivå. Däremot noterades att det i kommande uppdateringar i KLASSA även kommer att inkluderas modul för riskanalyser samt en rapporteringsmodul vilket kommer skapa förutsättningar för förbättrad uppföljning och hantering av informationssäkerhetsrisker.

Under granskningen noterades att det inom Omvårdnadsförvaltningen inte har genomförts en heltäckande risk-och sårbarhetsanalys på systemnivå för förvaltningens verksamhetskritiska system. Den riskanalys som genomförts har enbart fokuserat på att säkerställa systemets tillgänglighet.

PwC noterade även under granskningen att det i förmedlade anvisningar inte framgår att Solna Stad tagit fram definierade kriterier för riskacceptans kopplat till IT- och informationssäkerhet.

Vidare noterades att Solna Stad har en kommunövergripande kontinuitetsplan och avbrottsplaner för verksamhetskritiska IT-system. Dessa har inte inkluderats som ett granskningmoment av PwC och således inte granskats i detalj.

Bedömning

Vår bedömning är att Solna Stad i nuläget delvis har en tillräcklig nivå gällande rutiner för att identifiera, hantera risker och hot då uppföljning inte görs av stadens centrala funktion.

PwC rekommenderar kommunstyrelsen att;

- Säkerställa efterlevnad och genomförande av mer omfattande riskanalys på systemnivå i samtliga förvaltningar med bäring på IT- och informationssäkerhet. Det är förvaltningarna som ska ha ansvaret för att driva identifieringen av risker och de informationstillgångar som är relevanta att skydda, men att centrala funktioner tillhandahåller nödvändig resurser, mandat och tydliga roller för att stödja dess genomförande.
- Säkerställa att riskhanteringsåtgärder har en ansvarig person utsedd, tidsram, finansiering och uppföljning i syfte att begränsa risken och uppfylla skyddskraven.
- Definiera kriterier för riskacceptans för Solna Stad.

Se område 3.4 i appendix för mer information om iakttagelser och rekommendationer.

3. Resultat av granskningen

3.5 Hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?

Iakttagelser

Solna Stad har en övergripande dokumenterad beskrivning för incidenthantering som stipulerar att systemägaren ansvarar för att upptäckta incidenter registreras och hanteras i enlighet med stadens incidenthanteringsprocess. Under intervjuer framkom att incidenter primärt rapporteras in via telefon eller via stadens avvikelsehanteringssystem. Inkomna incidenter hanteras och följs upp centralt i Servicedesk av tjänsteägare på central nivå.

Under intervju på förvaltningsnivå framkom att anställdas rapportering sker till närmaste chef som antingen rapporterar till Servicedesk om det är en IT-relaterad incident, eller till nämndens Dataskyddsombud om det är en personuppgiftsincident. Kriterier för när en incident anses vara kritisk finns definierade.

Under granskning framgick det att säkerhetsincidenter följs upp och granskas månadsvis tillsammans med Data Ductus. Det noterades dock att inga regelbundna incidentövningar har genomförts i närtid.

PwC noterade att Solna Stad inte har formaliserat ovan beskriven hantering i en separat incidenthanteringsrutin. Däremot har PwC blivit informerade om att arbetssättet för att hantera incidenter är väl inarbetat i organisationen och arbetsflödet finns till viss del beskrivet i stadens stadsövergripande anvisningar för IT- och informationssäkerhet. Vidare framkom under granskningen att det pågår ett arbete att förtydliga och utveckla befintlig anvisning för incidenthantering med underliggande rutin.

Bedömning

Vår bedömning är att Solna Stad delvis har en tillräcklig nivå gällande incidenthantering då det finns anvisningar för hur hantering av IT- och informationssäkerhetsincidenter ska ske samt välfungerande arbetssätt avseende incidenthantering.

PwC rekommenderar kommunstyrelsen att;

- Fortsätta arbetet med att utöka och formalisera anvisningar för hur hantering av IT-och informationssäkerhetsincidenter ska hanteras i en separat rutin. En sådan rutin bör innehålla en tydlig mottagare av incidentlarm, hanteringsregler för olika typer av incidenter, ett verktyg för att samla alla incidenter samt instruktioner för eventuell eskalering av ärenden. En viktig del i incidenthanteringen är att informera/utbilda användarna i att kunna identifiera och rapportera incidenter.
- Införa rutin för att regelbundet genomföra incidentövningar för att säkerställa att hanteringsregler och eskaleringsrutiner för olika typer av incidenter är aktuella och väl införstådda genomgående i staden.

Se område 3.5 i appendix för mer information om iakttagelser och rekommendationer.

3. Resultat av granskningen

3.6 Finns formellt beskrivna rutiner för hantering av outsourcing till externa leverantörer, exempelvis former för kravställande och kommunikation, avtal och uppdatering av dessa, samt uppföljning av efterlevnad av avtal?

Iakttagelser

Solna Stad har arbetssätt dokumenterade för vad som ska beaktas när man anlitar externa leverantörer (t.ex. upphandling av nytt IT-system) vilket bla inkluderar krav kring leverantörens arbete med informationssäkerhet, hur stöd vid incidenter av systemet ska se ut, och att möjligheten för tredjepartsrevision ska finnas. Under samtal på förvaltningsnivå har det framgått att det finns en central upphandlingsenhet som stödjer förvaltningarna med denna kravställning.

PwC noterade även att Solna Stad i sina stadsövergripande anvisningar stipulerat att avtal med IT-leverantörer ska reglera hur kontroll av avtalets uppfyllande ska ske, detta genom exempelvis tredjepartsrevision eller granskning genomförd av Solna stad. Vidare framkom under stadens anvisningar att det ska ske informationsklassificering innan upphandling av system-/IT-stöd för att informationssäkerhetskrav ska tillvaratas i kravställning på leverantörerna. Under intervjuer framkom att det i nuläget hålls möten med leverantörer för att diskutera eventuella avtalsförändringar i syfte att harmonisera med hur det fungerar i verkligheten. Ovan angiven arbetsprocess var muntligen delgiven, PwC noterade dock att inarbetat arbetssätt inte är formaliserat i rutiner eller instruktioner för stadens verksamhetskritiska system.

PwC noterade också under granskningen att Solna Stad idag inte har några rutiner för att regelbundet säkerställa att tjänsteleverantören genomför återläsningstester av säkerhetskopior. Staden har vidare inte säkerställt tjänsteleverantören har flera säkerhetskopior som är förvarade på olika platser för att säkerställa redundans.

Bedömning

Vår bedömning är att Solna Stad har en delvis tillräcklig nivå gällande outsourcing och upphandlingar kopplat till IT. Vid granskningen noterades en iakttagelser som bedöms som utgöra högrisk.

PwC rekommenderar att kommunstyrelsen att:

- Införa gemensam rutin för att regelbundet följa upp att kritiska driftleverantörer samt systemleverantörer för verksamhetskritiska system testar återläsning av säkerhetskopior. Testerna bör dokumenteras och tillhandahållas Solna Stad.

Se område 3.6 i appendix för mer information om iakttagelser och rekommendationer.

Appendix: Sammanställning avvikelser

På följande sidor redogör vi mer i detalj för de avvikelser och risker som vi har sett i vår granskning, kopplat till respektive kontrollmål. Vi ger även rekommendationer för noterade avvikelser.

Vi har gjort en prioritering av avvikelserna där L står för låg prioritet, M för medel och H för hög. Definitionen av denna klassificering visas nedan:

Prioritet	**Förklaring till prioritet**
Hög	Syftar på en svaghet som har stor inverkan på system, processer och relaterade kontroller och som kan utsätta enheten för större förluster, ineffektivitet och/eller kan resultera i allvarliga konsekvenser. Avvikelser som bedöms utgöra hög risk bör åtgärdas med hög prioritet.
Medel	Syftar på en situation eller arbetssätt som skiljer sig från vad PwC anser vara god praxis och som vi bedömer har en negativ inverkan på den interna kontrollen.
Låg	Syftar på en situation eller arbetssätt som enbart har en begränsad effekt på den interna kontrollen.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.1.5	M	PwC noterade under granskningen att Solna stad inte har implementerat funktionen "Restricted Groups" i IAM-plattformen. Vidare noterades att personal inom Servicedesk har behörigheten "Local admin".	*Risken med att icke-nödvändiga lokaladministratörer finns är att flertalet personer kan ladda ner program på IT-infrastruktur utan central tillstånd eller granskning. Missbruk av administrativa privilegier är en nyckelmetod som används av angripare för att få obehörig åtkomst till våra nätverk.* *Risken med att inte aktivera "Restricted groups" inom Active Directory är att hantering av priviligierade behörigheter blir svårhanterad och således ökar chansen för att ett konto felaktigt tilldelas grupptillhörighet i AD-strukturen.*	PwC rekommenderar kommunstyrelsen att; - Utvärdera behovet att implementera "Restricted Groups" funktion i IAM-plattformen. - Utvärdera behovet att häva behörighet "lokal admin" för personal inom Servicedesk.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	M	PwC noterade under granskningen att Solna Stad har ett välfungerande styrsystem för internkontroll, däremot kunde PwC under granskningen inte verifiera att IT- och informationssäkerhetskontroller har inkluderats i stadens systemstöd för internkontroll (Stratsys).	*Vid avsaknad av IT- och informationssäkerhetsrelaterade kontroller i stadens övergripande systemstöd för internkontroll finns det ett ökat personberoende vilket kan resultera i att kontroller ej genomförs vid personalförändringar, alternativt inte genomförs på förväntat sätt. Otydlighet i utförande av kontrollen kan resultera i försämrad kontrollkvalitét och brister i spårbarhet.*	För att få systematik i kontinuerligt förbättringsarbete kan staden använda sig av ett årshjul med aktiviteter kopplade till respektive månad. Varje aktivitet bör ha en beskrivning för vad aktiviteten omfattar samt vem som ansvarar för dess genomförande. Exempel på kontroller som kan ingå är: • Uppföljning av framtagen åtgärdsplan • Genomförande av riskanalys • Uppföljning av behörigheter • Sårbarhetsskanning • Utvärdera klassificering av kritiska IT-system • Återläsningstester av säkerhetskopior • mm, mm I sammanhanget rekommenderar PwC kommunstyrelsen att undersöka möjligheten att inkludera ovan exempel på relevanta kontroller som utförs i organisationerna kopplat till IT och informationssäkerhet i stadens befintliga systemstöd för internkontroll. Följande bör ingå i kontroll-ramverket: • Vilken risk hanteras genom kontrollen • På vilket sätt kontrollen skall utföras (kontrollaktivitet och design). • Varför ska kontrollen utförs (mål och syfte). • Vem som skall utföra kontrollen • Hur ofta skall kontrollen utföras. • Vilken dokumentation skall sparas för att verifiera genomförd kontroll (bevis för spårbarhet). • Vad skall göras om en kontroll uteblir eller är ineffektiv (Åtgärd).

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.3	M	PwC noterade att Solna Stad saknar en tydlig koppling mellan hanteringsrutiner för informationstillgångar kopplat till respektive informationsklass.	*Risken med att inte ha definierade och kommunicerade hanteringsrutiner är att verksamheten inte vet vilka skyddsåtgärder som är tillämpade för en specifik informationsmängd. Vidare är risken med avsaknad av hanteringsrutiner att information inte hanteras utefter sitt skyddsvärde och således ökar chanserna för att informationens riktighet, tillgänglighet eller konfidentialitet äventyras.*	PwC rekommenderar kommunstyrelsen att komplettera beskrivning av framtagna informationsklasser med krav kopplat till hanteringen. En bra utgångspunkt i arbetet är Myndigheten för samhällsskydd och beredskap (MSB:s) vägledning för informations- säkerhet avseende koppling av säkerhetsågärder till klassningsmodell (https://www.informationssakerhet.se/metodstodet/utforma/#klassningsmodell).

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.4	M	PwC identifierade under granskningen att Solna stad saknar uppföljning av riskanalyser mht IT-och informationssäkerhet som genomförs på nämndnivå. Det noterades dock att i kommande uppdateringar av verktyget KLASSA ingår modul för riskanalyser samt en rapporteringsmodul vilket kommer skapa förutsättningar för förbättrad uppföljning och hantering av informationssäkerhetsrisker.	*Om uppföljning och kontroll av förvaltningars riskarbete inte görs finns det en risk att analyser utförs fel vilket kan leda till att informationstillgångar utsätts för en oacceptabel riskexponering. Vidare är risken att nyuppkomna hot eller interna sårbarheter för verksamheten inte adresseras. Avsaknad av uppföljning kan även orsakar att potentiella risker i verksamheternas systemanvändning inte fångas upp och därmed inte beaktas vid utformning av relevanta informationssäkerhetskrav i befintliga och kommande avtal.*	PwC rekommenderar kommunstyrelsen att genomföra mer omfattande riskanalys på systemnivå i samtliga förvaltningar med bäring på IT- och informationssäkerhet. Det är förvaltningarna som ska ha ansvaret för att driva identifieringen av risker och de informationstillgångar som är relevanta att skydda, men att centrala funktioner tillhandahåller nödvändig resurser, mandat och tydliga roller för att stödja dess genomförande. I sammanhanget rekommenderar PwC att riskhanteringsåtgärder har en ansvarig person utsedd, tidsram, finansiering och uppföljning i syfte att begränsa risken och uppfylla skyddskraven.

Sammanställning avvikelser

Område	Prio	Avvikelse	Risk	Rekommendation
3.5	M	PwC noterade under granskningen att kommunen saknar separat dokumenterad rutin för incidenthantering och att incidentövningar inte genomförts i närtid. Under granskningen noterades dock att det pågår ett arbete i att förtydliga och utveckla befintlig anvisning för incidenthantering med underliggande rutin.	*Vid avsaknad av dokumenterade processer och rutiner finns det ett ökat personberoende vilket kan resultera i att aktiviteter/kontroller ej genomförs vid personalförändringar, alternativt inte genomförs på förväntat sätt.* *Eventuella incidenter som inträffar i verksamheten bör identifieras, rapporteras och hanteras så snart som möjligt annars riskerar verksamheten att skadas på olika sätt, beroende på vilken typ av incident som inträffar. Att inte omedelbart hantera vissa typer av incidenter kan få kostsamma följder. Om inte alla incidenter registreras på ett enhetligt sätt kan underlagen för uppföljning av incidenter bli missvisande. Det finns då en ökad risk att grundorsaker till en grupp incidenter inte identifieras och att resurser för att lösa återkommande incidenter felprioriteras, vilket kan leda till omotiverade kostnad.* *Risken med att inte genomföra kontinuerliga incidentövningar är att organisationen inte kan säkerställa effektiv beredskapshantering och ändamålsenliga hanteringsrutiner för kritiska incidenter.*	PwC rekommenderar kommunstyrelsen att utöka och formalisera anvisningar för hur hantering av IT-och informationssäkerhetsincidenter ska hanteras i en separat rutin. En sådan rutin bör innehålla en tydlig mottagare av incidentlarm, hanteringsregler för olika typer av incidenter, ett verktyg för att samla alla incidenter samt instruktioner för eventuell eskalering av ärenden. En viktig del i incidenthanteringen är att informera/utbilda användarna i att kunna identifiera och rapportera incidenter. PwC rekommenderar också att införa en rutin för att regelbundet genomföra incidentövningar för att säkerställa att hanteringsregler och eskaleringsrutiner för olika typer av incidenter är aktuella och väl införstådda genomgående i staden.

Sammanställning avvikelser

Om-råde	Prio	Avvikelse	Risk	Rekommendation
3.6	H	PwC noterade också under granskningen att Solna Stad idag inte har några övergripande formella rutiner för att regelbundet säkerställa att kritiska driftsleverantörer samt systemleverantörer för verksamhetskritiska system genomför återläsningstester av säkerhetskopior. Exempelvis noterades att det inom Omvårdnadsförvaltningen inte finns rutiner fastställda där återkoppling från kritiska systemleverantörer genomförs med hänsyn till återläsningstester av säkerhetskopior.	*Om man inte regelbundet testar att återläsning från säkerhetskopiorna fungerar på ett tillfredsställande sätt finns risk att de inte fungerar när det behövs, t ex vid en katastrofsituation.* *Utan fungerande säkerhetskopior från systemen kan återstarttiden för verksamheten bli orimligt lång vilket kan få allvarliga konsekvenser för verksamheten.*	PwC rekommenderar kommunstyrelsen att utöka och formalisera anvisningar för hur uppföljning av efterlevnad av säkerhetskrav i avtal med leverantörer ska ske. Dessa ska inkludera tydliga krav på förväntad leverans inom olika områden gällande exempelvis drift, avbrottsplanering och infrastruktur. Uppfyllande av dessa krav som finns ska även från leverantörens sida kunna påvisas, exempelvis i rapportform. Vidare rekommenderar PwC kommunstyrelsen att införa gemensam rutin för att regelbundet följa upp att kritiska driftsleverantörer samt systemleverantörer för verksamhetskritiska system testar återläsning av säkerhetskopior. Testerna bör dokumenteras och tillhandahållas Solna Stad. Återkoppling från leverantörer med hänsyn till återläsning av säkerhetskopior bör vara standardiserat och gällande oavsett form, storlek och väsentlighet.

Informationsresurser

En inblick i Sverige cybersäkerhet: Årsrapport för IT-incidentrapportering 2021
En inblick i Sveriges cybersäkerhet : årsrapport it-incidentrapportering 2021

Upphandla informationssäkert
Upphandla informationssäkert : en vägledning

Stöd för systematiskt informationssäkerhetsarbete i organisationer
Metodstöd för LIS