..

Granskning av it-säkerhet inom kollektivtrafiken

Rapport

Region Skåne

KPMG AB

2023-11-22

Antal sidor 15

Region Skåne
Granskning av it-säkerhet inom kollektivtrafiken

2023-11-22

Innehållsförteckning

1 Sammanfattning

KPMG har av Region Skånes revisorer fått i uppdrag att granska it-säkerheten inom kollektivtrafiken. Uppdraget ingår i revisionsplanen för år 2023.

Vår samlade bedömning utifrån granskningens syfte är att Region Skåne inte har säkerställt en tillräcklig it-säkerhet inom Skånetrafikens it-system.

Region Skåne har ett ledningssystem för informationssäkerhet som inkluderar fastställda styrdokument i form av policys och riktlinjer för informationssäkerhetsarbetet som alla förvaltningar har att efterleva.

Ledningssystemet för informationssäkerhet är inte etablerat i tillräcklig utsträckning inom Skånetrafiken vilket har genererat en bristfällig kännedom om gällande styrdokument och krav. Det saknas därigenom etablerade processer och aktiviteter för it-säkerhetsarbetet i enlighet med den struktur och systematik som arbetet ska bedrivas inom. Den ansvarsfördelning som är dokumenterad omsätts inte i praktiken och roller avseende it-säkerheten för de system som nyttjas inom kollektivtrafiken är inte tydligt definierad.

Mot bakgrund av de brister i efterlevnad av styrande dokument som vi identifierat och avsaknad av uppföljning och åtgärder bedömer vi att kollektivtrafiknämnden inte har säkerställt att it-säkerhetsarbetet bedrivs på ett ändamålsenligt sätt inom Skånetrafiken.

I det följande redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Revisionsfråga	Bedömning: Delvis	Rekommendationer
Finns det ändamålsenliga styrdokument för it-säkerheten och säkerställer ansvarig nämnd att dessa efterlevs?	Regionstyrelsen har fastställt riktlinjer och instruktioner för it-säkerhetsarbetet och vi bedömer att dessa delvis är ändamålsenliga Styrdokumenten är i behov av revidering. Kollektivtrafiknämnden har inte säkerställt en tillräcklig efterlevnad av styrande dokument. Uppföljning har inte genomförts i enlighet med krav i styrdokument och vi kan konstatera att kännedom om styrdokumenten och de krav som ställs är bristfällig.	**Vi rekommenderar regionstyrelsen att:** - Revidera styrdokument så att dessa är aktuella och utgör en ändamålsenlig styrning av informationssäkerhetsarbetet i Region Skåne. - Säkerställa att ledningssystemet för informationssäkerhet etableras i samtliga verksamheter och att aktiviteter genomförs i enlighet med den systematik som beslutats. **Vi rekommenderar kollektivtrafiknämnden att:** - Säkerställa att informationssäkerhetsarbetet genomförs i enlighet med beslutade krav och metoder.

Revisionsfråga	Bedömning: Nej	Rekommendationer
Finns det ändamålsenliga kontinuitetsplaner för störningar och avbrott, **Har övningar genomförts för att säkerställa att kontinuitetsplaneringen är tillräcklig?**	Vi bedömer att kontinuitetsplaner för störningar och avbrott saknas inom Skånetrafiken. I avsaknad av kontinuitetsplaner har övningar och granskning som ska säkerställa att kontinuitetsplaneringen är aktuell och ändamålsenlig inte genomförts.	**Vi rekommenderar kollektivtrafiknämnden att:** - Säkerställa att kontinuitetsplaner för störning och avbrott upprättas för it-system inom Skånetrafiken samt att övning och granskning genomförs i syfte att säkerställa ändamålsenlighet, aktualitet och kunskap.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Är ansvarsfördelning och roller tydligt definierade gällande it-säkerheten för de digitala system som används inom Skånetrafiken?	Ansvarsfördelning och roller gällande it-säkerheten för de digitala system som används inom Skånetrafiken är inte tydligt definierade. Ansvar för system är dokumenterat i styrande dokument men mot bakgrund av den låga kännedomen om styrande dokument genomförs inte de uppgifter som hör till de olika rollernas ansvar.	**Vi rekommenderar kollektivtrafiknämnden att:** - Säkerställa att roll- och ansvarsfördelning tydliggörs och etableras inom kollektivtrafiknämndens verksamheter.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Finns ett systematiskt arbete med informationsklassning och riskanalyser? **Har vidtagna tekniska skyddsåtgärder utvärderats genom tekniska test eller it-säkerhetsanalyser?**	Det saknas ett systematiskt arbete med informationsklassning och riskanalyser. I nuläget saknas bedömningar för att anpassa säkerhetsåtgärder i relation till det skyddsvärde som informationstillgångarna har. Vår bedömning är att utvärdering av tekniska skyddsåtgärder endast gjorts i begränsad omfattning genom de penetrationstest som omfattat delar av system och it-miljö. Det finns därigenom risk att sårbarheter inte har identifierats så att dessa har minimerats eller eliminerats.	**Vi rekommenderar kollektivtrafiknämnden att:** - Säkerställa att informationsklassning och riskanalyser genomförs systematiskt på de informationstillgångar som hanteras i verksamheten samt att åtgärdsplaner upprättas utifrån erhållet resultat. - Säkerställa att säkerhetsåtgärder vidtas i syfte att skydda informationstillgångar och för att minimera eller eliminera risker som identifierats samt att dessa utvärderas regelbundet.

Revisionsfråga	Bedömning: Delvis	Rekommendationer
Hanteras och dokumenteras it-säkerhetshot och incidenter på ett ändamålsenligt sätt?	It-säkerhetshot och incidenter hanteras och dokumenteras delvis. Förbättringsbehov finns för att hanteringen ska vara ändamålsenlig. Incidenthanteringsrutinerna behöver etableras tydligare i syfte att säkerställa att incidenter hanteras i enlighet med dessa. It-enheten har etablerat ett antal säkerhetsåtgärder för övervakning som delvis säkerställt att it-säkerhetshot kan hanteras. Det har dock skett ett antal incidenter med påverkan på verksamheten vilket leder till att vi inte kan utesluta att säkerhetsåtgärder saknas i syfte att hantera it-säkerhetshot och incidenter på ett ändamålsenligt sätt i förhållande till aktuella hot och risker.	**Vi rekommenderar kollektivtrafiknämnden att:** - Säkerställa att gällande incidenthanteringsrutiner etableras samt att inträffade incidenter utgör del i uppföljning och förbättringsarbete så att väsentliga brister kan identifieras och åtgärdas.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Har nämnden säkerställt en tillräcklig uppföljning och återrapportering av it-säkerhetsarbetet och vidtas åtgärder vid behov?	Kollektivtrafiknämnden har inte säkerställt en tillräcklig uppföljning och återrapportering av it-säkerhetsarbetet. Den rapportering som sker till nämnden utifrån risk i internkontrollplanen bedömer vi inte vara tillräcklig som uppföljning. Nämnden har inte beslutat om uppdrag eller åtgärder för att stärka it-säkerheten. Åtgärder har dock vidtagits inom it-enheten i syfte att stärka it-säkerheten och förmåga att motstå säkerhetshot och incidenter.	**Vi rekommenderar kollektivtrafiknämnden att:** - Säkerställa att den uppföljning som sker av informationssäkerhetsarbetet även inkluderar it-säkerhet. - Stärka den interna kontrollen avseende efterlevnad av styrdokument för informationssäkerhet. - Säkerställa att nämnden erhåller återrapportering i tillräcklig utsträckning i syfte att kunna fatta beslut om erforderliga åtgärder för att stärka it-säkerheten.

Utöver ovan rekommendationer i förhållande till revisionsfrågorna rekommenderar vi även regionstyrelsen i dess övergripande ledningsansvar för informationssäkerhet att:

- Utvärdera om organisation och funktioner inom koncernkontoret är anpassade i förhållande till ledningssystemets omfattning och krav på hur informationssäkerhetsarbetet ska bedrivas.
- Säkerställa att regionstyrelsen i sin uppsiktsplikt stärker den interna kontrollen avseende efterlevnad av styrande dokument i samtliga nämnder och styrelser.

2 Bakgrund

KPMG har av revisionskontoret och de förtroendevalda revisorerna i Region Skåne fått i uppdrag att granska it-säkerheten inom kollektivtrafiken.

Skånetrafiken och dess resenärer är beroende av att digitala tjänster fungerar för köp av biljetter och för information om restider och avgångar. Avbrott och störningar är en risk för Skånetrafiken då det kan leda till missnöjda resenärer och intäktsbortfall.

Tidigare granskningar har visat på brister inom granskningsområdet och revisorerna har därför bedömt att det finns behov av att granska it-säkerheten inom kollektivtrafiken.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen har varit att bedöma om Region Skåne har säkerställt en tillräcklig it-säkerhet inom Skånetrafikens it-system.

För att uppnå ovanstående syfte har följande revisionsfrågor besvarats:

- Finns det ändamålsenliga styrdokument för it-säkerheten inklusive kontinuitetsplaner för störningar och avbrott, och säkerställer ansvarig nämnd att dessa efterlevs?
- Har övningar genomförts för att säkerställa att kontinuitetsplaneringen är tillräcklig?
- Är ansvarsfördelning och roller tydligt definierade gällande it-säkerheten för de digitala system som används inom Skånetrafiken?
- Finns ett systematiskt arbete med informationsklassning och riskanalyser?
- Har vidtagna tekniska skyddsåtgärder utvärderats genom tekniska test eller it-säkerhetsanalyser?
- Hanteras och dokumenteras it-säkerhetshot och incidenter på ett ändamålsenligt sätt?
- Har nämnden säkerställ en tillräcklig uppföljning och återrapportering av it-säkerhetsarbetet och vidtas åtgärder vid behov?

Granskningen avgränsas till kollektivtrafiknämnden, regionstyrelsen och nämnden för operativ regiongemensam verksamhet.

I granskningen har framkommit att nämnden för operativ regiongemensam verksamhet inte har något ansvar eller uppgifter gällande it-säkerheten inom Skånetrafiken, varför denna nämnd inte nämns ytterligare i rapporten.

2.2 Revisionskriterier

I granskningen utgörs revisionskriterierna av:

- Kommunallagen (2017:725) -kap 6:6
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Säkerhetsskyddslag (2018:585)
- Offentlighets- och sekretesslag (2009:400)
- MSB FS 2021:9 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (NIS-direktivet)
- Säkerhetspolicy (RF 2017-06-20)
- Säkerhetsstrategi (regionstyrelsen 2017-12-07)
- Riktlinjer för informationssäkerhet (regionstyrelsen 2017-12-07)
- Instruktioner och anvisningar för informationssäkerhet

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med verksamhetsföreträdare inom Skånetrafiken, Koncernkontoret och Avdelningen Digitalisering IT och MT.

Dokumentanalysen har bland annat omfattat övergripande styrdokument fastställda av regionfullmäktige, regionstyrelsen och regiondirektör i Region Skåne i form av:

Reglemente för styrelser och nämnder i Region Skåne, Säkerhetspolicy, Säkerhetsstrategi, Riktlinjer för informationssäkerhet, Instruktioner och anvisningar för informationssäkerhet i Region Skåne.

Styrdokument och underlag fastställda av kollektivtrafiknämnden eller ansvariga tjänstepersoner inom Skånetrafiken i form av:

Instruktion för informationssäkerhet 2.0, Instruktion Informationssäkerhetsincident, Mallar för incidenthantering och incidentrapport för it, Internkontrollplan 2023 för Kollektivtrafiknämnden samt deluppföljning 1 samt urval av protokoll från kollektivtrafiknämndens sammanträden 2023.

Rapporten är faktakontrollerad av de intervjupersoner som ingått i granskningen.

3 Resultat av granskningen

3.1 Styrdokument och kontinuitetsplanering

3.1.1 Styrdokument

Region Skåne har ett ledningssystem för informationssäkerhet som utgör ramverk för hur informationssäkerhetsarbetet i regionens samtliga verksamheter ska bedrivas och hur ansvaret är fördelat. Regionfullmäktige har beslutat om säkerhetspolicy och regionstyrelsen har etablerat styrande dokument i form av riktlinjer för informationssäkerhet. Till denna har en instruktion för tillämpning upprättats som stöd i arbetet. Dessa ingår i ledningssystem för informationssäkerhet och ska efterlevas av samtliga förvaltningar i Region Skåne. Skånetrafiken har som komplement till de regionövergripande styrdokumenten fastställt dokumentet Instruktion för informationssäkerhet.

Intervjuade uppger att ledningssystemet haft ett bristande underhåll och uppdatering där de styrande dokumenten är i behov av revidering. Vi konstaterar att majoriteten av dokumenten beslutats 2017. Därtill uppges att ledningssystemet inte är etablerat i regionens verksamheter så att aktiviteter genomförs i enlighet med beslut.

Riktlinjerna anger att arbetet ska följa standarden ISO/IEC 27001 och ISO/IEC 27002. ISO 27001 reglerar krav på ledningssystem för informationssäkerhet medan 27002 reglerar säkerhetsåtgärder som kan vara organisatoriska eller tekniska (it-säkerhet).

Regionens riktlinje för informationssäkerhet reglerar att uppföljning för att säkerställa att styrande dokument efterlevs ska genomföras årligen samt när det inträffar väsentliga händelser som påverkar informationssäkerheten.

Enligt uppgift har ingen uppföljning av efterlevnad av styrdokument genomförts inom Skånetrafiken. Genom våra samlade iakttagelser från intervjuer kan vi konstatera att det inom Skånetrafiken saknas kännedom om både regionövergripande och förvaltningsspecifika styrdokument. Exempelvis saknas kännedom om de standarder (ISO 27001 och ISO 27002) som it-säkerhetsarbetet ska genomföras utifrån.

3.1.2 Kontinuitetsplanering

I riktlinjer och instruktioner för informationssäkerhet beskrivs krav på kontinuitetsplanering. Kontinuitetsplaner ska finnas för all information och alla system som klassas i tillgänglighetsklass T2 eller högre enligt Region Skånes informationsklassificeringsmodell. Kontinuitetsplanerna ska testas regelbundet genom granskningar och övningar för att säkerställa aktualitet och ändamålsenlighet.

Dokumenterade kontinuitetsplaner saknas inom Skånetrafiken och följaktligen har inte några övningar eller granskningar genomförts i enlighet med riktlinjens krav.

3.1.3 Bedömning

Vår bedömning är att regionstyrelsen har fastställt riktlinjer och instruktioner för it-säkerhetsarbetet och att dessa i allt väsentligt är ändamålsenliga.

De styrande dokumenten är dock i behov av att aktualiseras. Myndigheten för samhällsskydd och beredskaps rekommendation är att styrdokument inom informationssäkerhet inte ska vara äldre än tre till fem år och nuvarande policy och riktlinjer är över sex år gamla.

Vi bedömer att kollektivtrafiknämnden inte har tillsett en tillräcklig efterlevnad av styrande dokument för informationssäkerhet.

Uppföljning har inte genomförts i enlighet med krav i styrdokumenten och vi kan konstatera att kännedom om dokumenten och de krav som ställs är bristfällig. Det saknas därigenom etablerade processer och aktiviteter för it-säkerhetsarbetet. Till exempel genomförs inte arbetet med den systematik och enligt den struktur som beslutats.

Vi bedömer att kontinuitetsplaner för störningar och avbrott saknas inom Skånetrafiken.

I avsaknad av kontinuitetsplaner har övningar och granskning som ska säkerställa att kontinuitetsplaneringen är aktuell och ändamålsenlig inte genomförts.

3.2 Ansvar för it-säkerhet

Skånetrafiken har en egen it-miljö och avseende it-säkerhetsarbetet bedrivs inte något gemensamt arbete med Region Skånes avdelning Digitalisering IT och MT.

Inom Skånetrafiken finns avdelningen Digitalisering och IT som består av ett antal enheter. Intervjuade beskriver att it-säkerhetsarbetet i huvudsak genomförs inom Enhet IT som ansvarar för it-infrastruktur i form av servar, nätverk, plattform mm. Inom Enhet Tjänsteutveckling sker utveckling och förvaltning av system, däribland betal- och biljettsystemets delar. Arbetet inom båda dessa enheter leds av enhetschefer där Enhet IT har ett antal systemansvariga som ansvarar för olika it-komponenter medan det inom Enhet Tjänsteutveckling finns ett antal produktägare med systemansvar.

Ansvarsfördelning i informationssäkerhetsarbetet regleras i de styrande dokumenten för säkerhet och informationssäkerhet. Enligt instruktion för tillämpning av riktlinjer för informationssäkerhet har systemägaren det övergripande ansvaret för systemet och ansvarar för att dessa uppfyller lagkrav och verksamhetskrav som fastställts av informationsägaren.

Region Skåne har en beslutad förvaltningsmodell, *Verksamhetsstyrd styr- och förvaltningsmodell för IT- och MT-system*. Regelverket beskriver samarbetsformerna för styrning och förvaltning av it- och medicintekniska system. Modellen beskrivs i ett antal instruktioner och bilagor där ansvarsfördelning och uppgifter framgår. Av

dokumentationen framgår ”Trafik” som ett styr- och ansvarsområde (SAO) för kärnverksamhet.

Genom intervjuer kan vi konstatera att modellen inte är etablerad för de system som nyttjas inom Skånetrafiken. Det innebär att den samverkan som regionens verksamhetsstyrda styr- och förvaltningsmodell syftar till att etablera saknas. De uppgifter som ingår för rollerna verksamhetsansvarig och systemansvarig genomförs inte av produktägare och objektledare inom Skånetrafiken i enlighet med beskrivning i instruktioner.

Det pågår ett arbete på uppdrag av trafikdirektören för att etablera en system-förvaltningsmodell. Utifrån den beskrivning som vi fått uppfattar vi att det inte är den styr- och förvaltningsmodell som övriga verksamheter inom Region Skåne har etablerat för sina system. Etablering av modellen uppges vara en prioriterad aktivitet för att Skånetrafiken ska få en bättre struktur och systematik i arbetet med informations- och it-säkerhet.

I intervjuer framkommer ett flertal upplevda brister generellt utifrån roller och ansvar. Vi uppfattar bland annat ett glapp mellan verksamhetsansvaret för informationssäkerhet och arbetet med att etablera tekniska säkerhetsåtgärder. Det saknas även en funktion med övergripande ansvar för it-säkerhet, i nuläget både på strategisk och operativ nivå. Ansvaret är spritt på olika enheter och roller vilket innebär att risker och åtgärder hanteras inom respektive enhet och roll och inte på ett samlat sätt.

Skånetrafikens it-säkerhetskoordinator innehar enligt intervjuade uppdrag att koordinera säkerhetsarbetet, genomföra omvärldsbevakning, beställa säkerhetslösningar och vid behov olika typer av penetrationstest. Funktionen involveras även vid vissa incidenter. Vi uppfattar dock att rollen inte omfattar ansvar för det samlade it-säkerhetsarbetet.

3.2.1 Bedömning

Vi bedömer att ansvarsfördelning och roller gällande it-säkerheten för de digitala system som används inom Skånetrafiken inte är tydligt definierade.

Ansvar för system är dokumenterat i styrande dokument men mot bakgrund av den låga kännedomen om styrande dokument genomförs inte de uppgifter som hör till de olika rollernas ansvar.

3.3 It-säkerhet för system

Som del i metoden för granskningen ingick att genomföra en systemgranskning av de system som utgör betal- och biljettsystemet inom Skånetrafiken. Granskningen skulle utgå från processer och aktiviteter som ingår i ett systematiskt informationssäkerhetsarbete. Detta då verksamhetens analys och bedömningar av skyddsvärde är utgångspunkten för att etablera anpassade it-säkerhetsåtgärder.

För att genomföra systemgranskningen har vi efterfrågat dokumentation för nedanstående aktiviteter

- Informationsklassning
- Riskbedömning
- Handlingsplan för säkerhetsåtgärder
- Uppföljning av handlingsplan
- Riskhanteringsplan eller beslut om riskacceptans
- Utvärdering av etablerade säkerhetsåtgärder

Inget av ovanstående dokument har kunnat presenterats i granskningen. Enligt uppgift saknas underlagen på grund av att aktiviteter inte har genomförts. Detta trots att det finns krav i styrande dokument för informationssäkerhet samt i beskrivningar av det arbete som ska genomföras inom ramen för Verksamhetsstyrd styr- och förvaltningsmodell. Det saknas därigenom kännedom om vilka it-säkerhetsåtgärder som det finns behov av att etablera för system som nyttjas inom Skånetrafiken.

Intervjuade anger att det saknas kunskap för hur informationsklassning och riskbedömning ska genomföras. Samtidigt upplevs det finnas en otydlighet vem som ansvarar för att göra klassning samt utifrån det etablera identifierade behov av säkerhetsåtgärder.

Det saknas enligt uppgift rutiner för uppföljning av säkerhetsåtgärder. Utvärdering av säkerhetsåtgärder har gjorts för valda komponenter i it-miljön där delar av betal- och biljettsystemet ingått. Utvärdering har genomförts genom att anlita en hackare som fått i uppdrag att penetrationstesta nätverk och system. Utifrån resultatet av tester har sårbarheter identifierats och åtgärdats. Arbetet har till största delen utförts efter initiativ från en enhet på Digitalisering och IT inom Skånetrafiken (i fortsättningen benämnd Enhet IT) och har gjorts i den omfattning som tid och finansiella resurser medgett.

3.3.1 Bedömning

Vår bedömning är att det saknas ett systematiskt arbete med informationsklassning och riskanalyser.

I nuläget saknas därigenom bedömningar för att anpassa säkerhetsåtgärder i relation till det skyddsvärde som informationstillgångarna har. Vår bedömning är att utvärdering av tekniska skyddsåtgärder endast gjorts i begränsad omfattning genom de penetrationstest som omfattat delar av system och it-miljö. Det finns därigenom risk att sårbarheter inte har identifierats så att dessa har minimerats eller eliminerats.

3.4 It-säkerhetshot och incidenthantering

3.4.1 Förmåga att upptäcka och hantera it-säkerhetshot

Riktlinjer och instruktioner innehåller beskrivning av driftsäkerhet och kommunikationssäkerhet där krav på säkerhetsåtgärder för att skydda information och anslutna tjänster mot obehörig åtkomst ingår. Därtill framgår av dokumenten att loggning och övervakning ska finnas för att registrera och upptäcka åtgärder som kan påverka informationssäkerheten.

Utöver systemgranskningen har en översiktlig granskning gjorts av tekniska säkerhetsåtgärder för it-infrastruktur och förmåga att identifiera och hantera säkerhetshot mot Skånetrafikens digitala miljö. Denna har till största delen utgått från intervjuuppgifter.

Enhet IT har ett antal systemansvariga som har it-säkerhetsansvar för olika delar av it-miljön, exempelvis nätverk och servrar. It-säkerhetsåtgärder har etablerats för de it-komponenter som enheten ansvarar för. Intervjuade beskriver dock att det i nuläget saknas en överblick över den sammantagna säkerheten. För att få den bilden behöver samtliga systemansvariga involveras och delge uppgifter om säkerhetsåtgärder för respektive funktion.

Intervjuuppgifter beskriver att implementering av it-säkerhetsåtgärder inom Skånetrafiken utgår från enskilda funktioners kompetens, omvärldsbevakning samt ”best practice”. Det saknas dokumentation som ger spårbarhet till om etablerade it-säkerhetsåtgärder inom Skånetrafiken motsvarar de krav som ställs i interna styrdokument. Som vi beskrivit tidigare så är kännedom låg om styrande dokument och arbetet genomförs därigenom inte med grund i ISO 27001 och 27002.

Enligt uppgift skulle utvecklarna av system som är organiserade på Enhet Tjänsteutveckling på Skånetrafiken själva ta ansvar för it-säkerheten i systemen. Enhet IT har därigenom inte varit involverad i arbetet. Utifrån det ansvar som Enhet IT har för nätverk och servrar samt övervakning av hot och risker, har de dock upptäckt sårbarheter i betal- och biljettsystemet och genom det initierat och vidtagit säkerhetsåtgärder för att stärka it-säkerheten.

Intervjuade bedömer att incidenter som inträffat hade kunnat undvikas om informationssäkerhetsarbetet genomförts mer systematiskt och med förebyggande säkerhetsåtgärder utifrån aktuella hot och risker. Enhet IT har etablerat tekniska funktioner i syfte att kunna upptäcka säkerhetshot. Intervjuade uppger dock att nuvarande lösningar inte gör det möjligt att arbeta proaktivt utan enbart reaktivt när säkerhetshändelser eller incidenter sker.

3.4.2 Incidenthantering

Skånetrafiken har upprättat en instruktion för informationssäkerhetsincidenter[1]. Av instruktionerna framgår hur en incident ska anmälas både internt och till externa parter när så krävs. Vi har även tagit del av en mall för utredning av en informationssäkerhetsincident[2], en mall för utredning av it-incident[3] samt en mall för upprättande av it-incidentrapport[4].

Intervjuade anger att de dokumenterade rutinerna inte fullt ut är etablerade och att alternativa tillvägagångssätt förekommer. Det upplevs finnas en otydlig ansvarsfördelning och bristande kommunikation när incidenter inträffar.

I praktiken beskrivs att upptäckta incidenter anmäls till Enhet IT via ett ärendehanteringssystem för it-frågor inom kollektivtrafiken. Enhet IT har etablerat en beredskapskedja bestående av tekniker som ansvarar för hantering av it-säkerhetshot. Det är den som innehar beredskapsfunktionen vid det enskilda tillfället som gör bedömningen av hur allvarlig incidenten är.

Inom Enhet IT dokumenteras inträffade incidenter och det sker en genomgång dagligen av händelser. Utöver den genomgång som sker inom Enhet IT saknas hos Skånetrafiken ett övergripande analysarbete av de incidenter som inträffat inom förvaltningen.

3.4.3 Bedömning

Vi bedömer att kollektivtrafiknämnden delvis hanterar och dokumenterar it-säkerhetshot och incidenter men att förbättringsbehov finns för att hanteringen ska vara ändamålsenlig.

Incidenthanteringsrutinerna behöver etableras ytterligare i syfte att säkerställa att incidenter hanteras i enlighet med dessa. På förvaltningsövergripande nivå behöver erfarenheter från inträffade incidenter utgöra del i uppföljning och förbättringsarbete så att väsentliga brister kan identifieras och åtgärdas.

Enhet IT har etablerat ett antal säkerhetsåtgärder för övervakning som delvis säkerställt att it-säkerhetshot kan hanteras. Det har dock skett ett antal incidenter med påverkan på verksamheten vilket leder till att vi inte kan utesluta att vissa säkerhetsåtgärder saknas i syfte att hantera it-säkerhetshot och incidenter på ett ändamålsenligt sätt i förhållande till aktuella hot och risker.

Vi ser därtill att analys av inträffade incidenter kan stärkas på övergripande nivå och inkluderas i förvaltningens arbete med förbättringsåtgärder i syfte att stärka informationssäkerheten inom Skånetrafiken.

[1] Instruktion för informationssäkerhetsincident, Skånetrafiken, 2019-10-03
[2] Mall utreda informationssäkerhetsincident, Skånetrafiken, 2019-10-01
[3] Mall för incidentrapport, Skånetrafiken, 2019-11-26
[4] Mall incidentrapport, saknar datum samt vem som antagit.

3.5 Uppföljning

I instruktion för tillämpning av riktlinjer för informationssäkerhet regleras att förvaltningar löpande ska följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

En uppföljning av informationssäkerhetsarbetet görs årligen som rapporteras av förvaltningens informationssäkerhetsamordnare till förvaltningschef och sedan vidare till informationssäkerhetschef inom koncernkontoret. Uppföljningen genomförs med stöd i en lathund där respektive förvaltning beskriver hur arbetet bedrivits utifrån beslutade informationssäkerhetsmål. Enligt uppgift rapporteras inte denna till kollektivtrafiknämnden. Vi har tagit del av rapport för det samlade informationssäkerhetsarbetet inom Skånetrafiken för 2023 och kan konstatera att it-säkerheten inte ingår i denna uppföljning.

Intervjuade beskriver att Enhet IT halvårsvis rapporterar om it-säkerhetsarbetet till kollektivtrafiknämnden. Vi uppfattar att det genomförs som del i uppföljning av intern kontroll där informationssäkerhet och it-säkerhet ingår som riskområden i internkontrollplan för 2023. Risker har nått ett totalt riskvärde om sex (3 x 2) vilket innebär att det är risker som nämnden bevakar under 2023.

Den ena risken som identifierats är bristande följsamhet till riktlinjer för informationssäkerhet. Den andra risken avser it-incidenter och större IT-störningar på grund av cyberattacker, DDoS (överbelastningsattack), ransomeware (skadlig kod som krypterar och låser filer där krav om ekonomisk ersättning eller utpressning följer) etcetera.

Deluppföljning 1 per augusti har rapporterats till kollektivtrafiknämnden vid sammanträde 3 oktober 2023. Risktrenden bedöms vid uppföljningen vara konstant. Den åtgärd som genomförts för att möta risk inom it-säkerhet beskrivs i den dokumenterade uppföljningen vara att avdelning Digitalisering och IT inom Skånetrafiken under 2023 implementerat ytterligare säkerhetslösningar. Planer finns att under kvartal tre implementera ytterligare säkerhetslösning.

3.5.1 Bedömning

Vi bedömer att kollektivtrafiknämnden inte har säkerställt en tillräcklig uppföljning och återrapportering av it-säkerhetsarbetet.

I den samlade uppföljningen av informationssäkerhetsarbetet som görs årligen saknas uppföljning av it-säkerhet. Den rapportering som sker till nämnden utifrån identifierade risker i internkontrollplanen bedömer vi inte vara tillräcklig som uppföljning. Nämnden har inte beslutat om uppdrag eller åtgärd för att stärka it-säkerheten. Åtgärder har dock vidtagits inom it-enheten i syfte att stärka it-säkerheten och förmåga att motstå säkerhetshot och incidenter.

Mot bakgrund av de faktiska bristerna i efterlevnad och avsaknaden av uppföljning och åtgärder bedömer vi att kollektivtrafiknämnden inte har säkerställt att it-säkerhetsarbetet är ändamålsenligt inom Skånetrafiken.

4 Samlad bedömning och rekommendationer

Syftet med granskningen har varit att bedöma om Region Skåne har säkerställt en tillräcklig it-säkerhet inom Skånetrafikens it-system.

Vår samlade bedömning utifrån granskningens syfte är att Region Skåne inte har säkerställt en tillräcklig it-säkerhet inom Skånetrafikens it-system.

Ledningssystemet för informationssäkerhet är inte etablerat i tillräcklig utsträckning vilket har genererat en bristfällig kännedom om gällande styrdokument och krav. Ansvarsfördelning och roller avseende it-säkerheten för system framgår av styrdokument men är inte etablerad så att arbetet genomförs i enlighet med de uppgifter som roller och ansvar tilldelats.

Arbetet med it-säkerhetshot och incidenter har förbättringsbehov i syfte att hanteras på ett ändamålsenligt sätt. Då flertal incidenter har genererat konsekvens och påverkan på verksamheten kan vi inte utesluta att Skånetrafiken saknar erforderliga säkerhetsåtgärder i förhållande till aktuella hot och risker.

Mot bakgrund av de faktiska bristerna i efterlevnad och avsaknaden av uppföljning och åtgärder bedömer vi att kollektivtrafiknämnden inte har säkerställt att it-säkerhetsarbetet är ändamålsenligt inom Skånetrafiken.

Utifrån vår bedömning och slutsats rekommenderar vi regionstyrelsen att:

- Revidera styrdokument så att dessa är aktuella och utgör en ändamålsenlig styrning av informationssäkerhetsarbetet i Region Skåne.
- Säkerställa att ledningssystemet för informationssäkerhet etableras i samtliga verksamheter och att aktiviteter genomförs i enlighet med den systematik som beslutats.
- Utvärdera om organisation och funktioner är anpassade i förhållande till ledningssystemets omfattning och krav på hur informationssäkerhetsarbetet ska bedrivas.
- Säkerställa att regionstyrelsen i sin uppsiktsplikt stärker den interna kontrollen över efterlevnad av styrande dokument.

Utifrån vår bedömning och slutsats rekommenderar vi kollektivtrafiknämnden att:

- Säkerställa att informationssäkerhetsarbetet genomförs i enlighet med beslutade krav och systematik.
- Säkerställa att roll- och ansvarsfördelning tydliggörs och etableras inom kollektivtrafiknämndens verksamheter.
- Säkerställa att kontinuitetsplaner för störning och avbrott upprättas för it-system inom kollektivtrafiknämnden samt att övning och granskning genomförs i syfte att säkerställa ändamålsenlighet, aktualitet och kunskap.

- Säkerställa att informationsklassning och riskanalyser genomförs systematiskt på de informationstillgångar som hanteras i verksamheten samt att åtgärdsplaner upprättas utifrån erhållet resultat.
- Säkerställa att säkerhetsåtgärder vidtas i syfte att skydda informationstillgångar och för att minimera eller eliminera risker som identifierats samt att dessa utvärderas regelbundet.
- Säkerställa att gällande incidenthanteringsrutiner etableras samt att inträffade incidenter utgör del i uppföljning och förbättringsarbete så att väsentliga brister kan identifieras och åtgärdas.
- Säkerställa att den uppföljning som sker av informationssäkerhetsarbetet även inkluderar it-säkerhet.
- Stärka den interna kontrollen avseende efterlevnad av styrdokument för informationssäkerhet.
- Säkerställa att nämnden erhåller återrapportering i tillräcklig utsträckning i syfte att kunna fatta beslut om erforderliga åtgärder för att stärka it-säkerheten.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Ida Larsson
Verksamhetsrevisor

Simon Homander
Verksamhetsrevisor

Veronica Hedlund Lundgren
Certifierad kommunal yrkesrevisor