Handläggare
Annett Laurin

Datum
2020-02-18

Vår beteckning
RS/192342

Ert Datum
2019-10-15

Er beteckning
Rev/19012

Region Värmlands revisorer

Svar på revisionsrapport om Granskning av regionens informationssäkerhet (inkl. IT-säkerhet)

Regionstyrelsen vill avge följande svar på rubricerad revisionsrapport.

Granskningen har, på revisorernas uppdrag, genomförts av PwC. I rapporten redovisar konsulterna bland annat följande sammanfattande iakttagelser.

Efter genomförd granskning bedömer vi att Regionstyrelsen till viss del har uppfyllt kontrollmålen. Sammantaget bedöms regionen arbeta med informationssäkerhet men det finns tydliga förbättringsmöjligheter för att fullt ut nå ett tillfredsställande och ändamålsenligt arbete. Vi lämnar ett antal rekommendationer för att säkerställa ett fortsatt effektivt arbete med informationssäkerhet inom regionen.

PwC:s bedömning som svar på revisionsfrågorna är att Regionstyrelsen inte helt har säkerställt en styrning och uppföljning som ger en ändamålsenlig informationssäkerhet. Grunden till denna bedömning är den nuvarande avsaknaden på regelbunden revision, granskning och uppdatering av styrande dokumentation, avsaknaden av dokumentation för vissa väsentliga informationssäkerhetsprocesser samt bristande systematisk uppföljning och rapportering kring informationssäkerhetshändelser och incidenter till Regionstyrelsen.

PwC bedömer även att Regionstyrelsen inte helt har vidtagit åtgärder med anledning av de brister och förbättringsförslag som framfördes i förstudien 2015. Denna bedömning bygger på den iakttagna avsaknaden på både systematisk informationsklassning av samtliga system samt regelbundet och dokumenterat utförande av riskanalyser, åtgärder som rekommenderades av förstudien. Den ovan nämnda punkten kring brister med styrningen och dokumentation påvisar även att det fortfarande finns ett förbättringsarbete som regionen bör utföra.

Utifrån våra iakttagelser bör nämnas att flertalet åtgärder identifierats av Region Värmland och eventuellt redan påbörjats avseende de förbättringsområden som uppmärksammats i granskningen.

Utifrån de iakttagelser och bedömningar som framkom i granskningen lämnade konsulterna ytterligare ett antal rekommendationer till Regionstyrelsen.

Regionens revisorer bedömer att Regionstyrelsen bör tillse att konsulternas rekommendationer beaktas i kvalitets- och utvecklingsarbetet inom berörda verksamheter.

Rekommendationer

Människor och processer:

Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.

Huvudsakliga informationssäkerhetsprocesser fastställs på en övre nivå i den säkerhetspolicy som beslutades av regionfullmäktige i november 2019 och i den riktlinje för informationssäkerhet som beslutades av regionstyrelsen i december 2019. I dessa styrande ledningsdokument tydliggörs roller, ansvar och mandat inom informationssäkerhetsområdet. Ytterligare förtydliganden av informationssäkerhetsprocesser finns i styrande verksamhetsdokument. Dessa kommer att kompletteras under 2020 och löpande när behov uppstår.

För att ett systematiskt och strukturerat informationssäkerhetsarbete ska kunna bedrivas i en stor och komplex organisation som Region Värmland så måste en väl definierad organisation finnas på plats. Begreppet informationssäkerhet måste etableras från ledningen nedåt för att ge tyngd åt arbetet.

Regionen har genomgått en större organisationsförändring som trädde i kraft vid årsskiftet 2018/19 som har inneburit att det görs en översyn av styrande dokument överlag.

Säkerställ att samtlig dokumentation är uppdaterad och giltig.

Inom Region Värmland finns sedan 2019-10-17, genom riktlinjen Styrande dokument – struktur, fastställande och hantering (RS/190178), en reglering av med vilka intervall styrande dokument ska revideras. Styrande

ledningsdokument gäller tillsvidare men ska aktualitetsprövas regelbundet, medan styrande verksamhetsdokument gäller som längst två år.

Dokumenthanteringssystemet Vida livscykelhanterar och versionshanterar dokumenten. Dokumentägare är utsedda för samtliga dokument vilka notifieras när dokument ska revideras.

Säkerställ att informationssäkerhetspolicyn 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.

Besvarat enligt rekommendationerna ovan. Uppföljning kommer att ske.

Identifiera och definiera mätbara mål för samtliga åtgärdsmål i syfte att följa upp dessa kontinuerligt. Därtill bör regionen slutföra omsättningen av principerna beskrivna i informationssäkerhetspolicyn till riktlinjer.

Under 2019 har en GAP-analys påbörjats för att visa på nuläget för informationssäkerhetsarbetet i regionen på ett tydligt sätt. Region Värmland kommer under 2020 att definiera mätbara mål för informationssäkerhetsarbetet utifrån denna för att möjliggöra uppföljning på ett effektivt och tydligt sätt och på ett sätt som går att följa över tid.

GAP-analysen innehåller beskrivning och förklaring av vårt ledningssystem för informationssäkerhet och i detta även en modell innehållande aktörer, resurser, lagkrav etc.

Principerna beskrivna i policyn är omsatta i en riktlinje för informationssäkerhet som beslutades av regionstyrelsen i december 2019.

Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Region Värmland. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.

Utbildning inom informationssäkerhet finns tillgänglig i it-stödet Kompetensverktyget och riktad information/utbildning erbjuds vid behov. Region Värmland använder sig i liten grad av obligatoriska utbildningar. Ett inriktningsbeslut om obligatoriska utbildningar skulle underlätta vid uppföljning och utvärdering. Det är istället personalens närmaste chef som är ansvarig för att personalen har den utbildning och kunskap den behöver.

Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Regionen bör även genomföra systematiska uppföljningar av utbildningsverksamheten.

I kommande nämndplan och förvaltningsplan avser regionstyrelsen och regiondirektören precisera aktiviteter som ska genomföras för att öka säkerhetskulturen inom organisationen.

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

Region Värmland har en riktlinje för avvikelsehantering och en beskriven avvikelsehanteringsprocess samt ett it-stöd för hantering av avvikelser, AHA. Här ska alla avvikelser, inklusive de som rör informationssäkerhet, rapporteras för att bedömas och hanteras utifrån nämnda riktlinje och process. För it - relaterade incidenter har region - IT en beskriven incidenthanteringsprocess och it-stöd för att anmäla incidenter, Nilex. Utifrån nämnda processer finns eskaleringsvägar och ansvar beskrivna liksom att organisationen ska lära sig utifrån inträffade incidenter. Arbetet med anmälan, dokumentation och uppföljning av incidenter kan dock förbättras vilket kommer tydliggöras i mätbara mål för informationssäkerhetsarbetet som Region Värmland under 2020 kommer att definiera.

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

I den säkerhetspolicy som beslutades av regionfullmäktige i november 2019 och den riktlinje för informationssäkerhet som beslutades av regionstyrelsen i december 2019 fastslås att informationssäkerhetsansvaret följer linjeansvaret och att informationsägare ska identifieras och utses. Som stöd för dessa ska det finnas två informationssäkerhetssamordnare, en it-säkerhetsansvarig och ett dataskyddsombud. I linjen behöver man mycket stöd då informationssäkerhetsarbetet ännu inte har blivit en naturlig del av t.ex. verksamhetsutveckling, inköp av it - stöd eller andra förändringar.

Med hänsyn till den nya lagstiftningen inom säkerhetsskydd från april 2019 bör Region Värmland genomföra en djupare analys av regionens kritiska informationstillgångar för Sveriges säkerhet.

Genom en tydlig beskrivning och process rörande incidenter så uppfyller Region Värmland kraven både i säkerhetsskyddslagen och NIS-direktivet.

Säkerhet- och beredskapsenheten tar fram rutiner och instruktioner runt denna hantering tillsammans med Region-IT. Samtliga inblandade i processen måste veta vad de ska göra och när.

Teknik:

Undersök möjligheten till att införskaffa en SIEM-lösning som aggregerar säkerhetsloggar från väsentliga nätverkspunkter och skapar relevanta alerter.

Region-IT anser att SIEM endast är en metod att lösa grundproblemet som är insyn och detektion, andra metoder finns också.

SIEM: Implementation finns redan. Region-IT har börjat med de system som bedöms ha högst riskvärde (AD och O365). Verktyget utvecklas löpande av AD-förvaltningen. Automatisering i olika nivåer är också påbörjad (från larm till åtgärder). Formell dokumentation av ramverk och rutiner saknas för närvarande.

Region-IT har också påbörjat ett projekt för att implementera Cisco StealthWatch som kommer att ge ytterligare verktyg för insyn och detektion. En första implementation ska vara färdig 2020.

Implementera behörighetstilldelning och behörighetsgrupper som baseras på i förväg bestämda roller.

Detta finns redan men styrning kan i vissa fall göras mer granulär.

En ny modell för detta är framtagen och ska implementeras steg för steg. Implementering påbörjad och testad under 2019 men aktiviteten behöver prioriteras för att kunna genomföras.

Automatisera sårbarhetsskanning så att det genomförs på regelbunden basis och dokumentera processen.

Detta görs delvis redan men formell dokumentation av processen saknas för närvarande. Region-IT kommer att prioritera etablering av förvaltning och utökning av användandet i nästa fas. Förvaltningen kan sedan dokumentera arbetssätt.

Utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans.

Region Värmland

Datum
2020-02-18

Diarienummer
RS/192342

Region-IT har utrett förutsättningar och tagit fram förslag till lösning för detta. Aktiviteten behöver prioriteras med resurser och budget för att kunna genomföras.

Regionstyrelsen

Fredrik Larsson
Ordförande

Peter Bäckstrand
T f Regiondirektör