Koncernkontoret
Enheten för säkerhet och intern miljöledning

Johan Reuterhäll
Infromationssäkerhetschef

RAPPORT

Datum: 2021-04-05
Dnr:

Rapport till Regionstyrelsen om informationssäkerhetsarbetet

Denna rapport utgör den information som enligt Socialstyrelsens föreskrifter[1] och enligt Region Skånes riktlinjer för informationssäkerhet en gång om året ska lämnas till Regionstyrelsen. Rapporten utgör underlag till ledningen med information om status på informationssäkerhetsarbetet och om effektiviteten i ledningssystemet för informationssäkerhet[2].

Regionstyrelsen beslutar om handlingsplan som följer med denna rapport.

Mats E Persson
Informationssäkerhetschef

[1] 1 kap. 3§ Socialstyrelsens föreskrifter (HSLFS-FS 2016:40) om informationshantering och journalföring i hälso- och sjukvård
[2] Enligt kapitel 5.3 punkt b, ISO 27001:2017

Innehåll

Sammanfattning

Informationssäkerhetsarbetet har bedrivits i positiv riktning de senaste åren. Organisation, roller och ansvar är definierat och centralt har grundläggande styrande dokument tagits fram för hantering av incidenter, klassificering av information och genomförande av riskanalyser. Arbetet bedrivs i vissa delar systematiskt och ändamålsenligt men det finns potential till förbättringar.

Antalet medarbetare har under året inte förändrats i det regionala informationssäkerhetsarbetet. Samtidigt fortsätter digitaliseringsarbetet på bred front med en stor mängd projekt varav ett flertal är relativt stora som ställer mycket höga krav på avancerad kompetens inom informations-hantering. Regionala resurser bedöms i allt större utsträckning behövas för att stödja projekten då informationssäkerhetsarbetet blir allt mer omfattande och komplext.

Fokus på god informationssäkerhet blir allt större i samhället och hos lagstiftaren. Kraven på att skydda personuppgifter och information som omfattas av sekretess blir allt högre. Utvecklingen går i en riktning där kraven och kontrollen ökar. En dom från EU-domstolen i somras upphävde den mekanism som hittills använts vid överföring av personuppgifter till tredjeland. Det får påverkan på Region Skåne då regionen använder ett flertal tjänster där den här mekanismen använts.

Regeringen har utrett möjligheterna att låta privata företag som hanterar sekretessbelagd information omfattas av straffsanktionerad tystnadsplikt. En ny lag börjar gälla från årsskiftet som innebär att privata företags anställda kommer omfattas. Bedömningen är att det här i låg grad påverkar möjligheterna för utnyttjande av molntjänster då de flesta molntjänster har utländskt ägande och den nya lagstiftningen kommer då inte ha någon verkan.

Arbetet med säkerhetsskydd har intensifierats under året. Genomförande av säkerhetsskyddsanalyser pågår i förvaltningarna. Analyserna ligger till grund för säkerhetsskyddsåtgärder som exempelvis säkerhetsprövning av medarbetare i tjänster. Syftet med säkerhetsskyddet är bland annat att skydda säkerhetskänslig verksamhet och information. Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för Sveriges säkerhet.

Granskningar och revisioner av större betydelse

Externa granskningar

Granskning av IT- och informationssäkerhet (genomförd av EY)

EY granskade[3] på uppdrag av Region Skånes revisorer om Region Skånes arbete med informationssäkerhet och IT-säkerhet sker på ett systematiskt och ändamålsenligt sätt inom regionstyrelsen och kollektivtrafiknämnden. Bedömningen var att IT- och informationssäkerhetsarbetet inom granskade nämnder till stora delar bedrivs systematiskt och ändamålsenligt men i vissa delar är otillräckligt.
Granskningen påvisar en positiv utveckling de senaste åren, framförallt inom styrning och ledning. Man konstaterar också att Region Skåne utformat en organisation för regionalt dataskyddsarbete som möjliggör ett strukturerat och målinriktat arbete för uppfyllande av kraven enligt GDPR. De brister som identifierats rör systematiskt uppföljning, kontroll och utvärdering. Även utbildning bedöms vara ett område som kan utvecklas. Revisionen tar även upp patientintegriteten i journalsystem och att den inte fullt ut kan säkerställas.

Granskning av IVO

Inspektionen för vård- och omsorg (IVO) öppnade ett tillsynsärende[4] den 10:e mars 2020 för att granska Region Skånes systematiska informationssäkerhetsarbete i egenskap av leverantör av samhällsviktiga tjänster inom hälso- och sjukvården. Syftet med granskningen var att i första hand bedöma om regionen uppfyller kraven enligt lagen om informationssäkerhet (2018:1174) för leverantörer av samhällsviktiga och digitala tjänster samt Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.
Granskningen avslutades 24:e augusti 2020. IVO:s granskning kunde inte påvisa några avsteg från kraven på systematiskt informationssäkerhetsarbete inom de granskade områdena.

Status på informationssäkerhetsarbetet

Region Skånes informationssäkerhetsarbete har sin grund i ledningssystemet för informationssäkerhet som är en allmänt erkänd standard för hur en organisation ska organisera och leda sitt informationssäkerhetsarbete.
Region Skåne har en central organisation med utsedda roller som ska verka regionalt i att leda och samordna informationssäkerhetsarbetet. I förvaltningarna finns samordnare utsedda som i sin tur har kontaktpersoner.
Region Skåne har utsett informationsägare som ansvarar för information och fattar beslut om vilka risker Region Skåne kan acceptera och det finns även

[3] Region Skåne, Revisionskontoret, Granskning av IT- och informationssäkerhet (rapport nr 6 - 2020)
[4] Tillsyn av IVO, 2020-08-25, dnr 2020-o000590

utsedda systemägare som ansvarar för att våra system uppfyller verksamhetens krav och lagkrav.

Statusen på informationssäkerhetsarbetet är relativt gott och grundläggande styrande dokument är beslutade. Efterlevnaden brister dock i vissa avseenden. Framförallt finns brister i samband med upphandling och vidareutveckling av IT-system där krav på informationssäkerhet inte alltid analyseras i ett tidigt skede vilket påverkar säkerhet och kvalitet. En avgörande faktor för god effektivitet är att informationssäkerhetsaktiviteter implementeras i verksamhetens normala processer. Det är först då som informationssäkerhetsarbetet kommer igång i rätt skede och det är då problem eller brister kan fångas upp i tid. Därför är utbildningsinsatserna prioriterade på alla nivåer.

Förändringar i externa eller interna frågor som är relevanta för ledningssystemet för informationssäkerhet

Beslut om informationsstyrningsrådet

Informationsstyrningsrådet inrättades ursprungligen inom Koncernkontoret för att samla kompetens i informationsstyrningsfrågor. Rådets funktion var att fungera som samarbetsorgan och beredningsforum i frågor och ärenden för beslut hos regionstyrelsen eller regiondirektören.
Efterhand har frågorna som rådet behandlar kommit att bli alltmer centrala och behovet av en bredare regional förankring har aktualiserats. Regiondirektören fattade därför beslut under året om att informationsstyrningsrådet blir ett regionalt organ där representationen breddats till att omfatta förvaltningarna. Utgångspunkten är en tydligare samordning av Region Skånes centrala funktioner inom informationsstyrning och att det bidrar till ökad effektivitet och en rättssäker hantering. Dataskydd, informationssäkerhet, arkiv- och bevarandekrav, dokumentationsplikt, registreringsskyldighet och andra legala eller funktionella krav på informationen omfattas.
Sammantaget är informationsstyrningsrådet ur ett informationssäkerhetsperspektiv ett bra tillskott som omedelbart bidrar till en högre informationssäkerhet.

Kommande uppdatering av NIS-direktivet

Nuvarande NIS-direktiv har varit gällande under en tid nu och har utvärderats. Ett nytt lagstiftningsförslag presenterades den 16 december 2020. Detta förslag är en del av ett åtgärdspaket för att ytterligare förbättra motståndskraft och incidenthantering hos offentliga och privata organisationer inom cybersäkerhet och skydd av kritisk infrastruktur.
Det nya NIS-direktivet tar hänsyn till den ökade digitaliseringen de senaste åren och ett växande cybersäkerhetslandskap och kommer, när det börjar gälla, att ersätta det nuvarande NIS-direktiv.

Förslag syftar till att åtgärda bristerna i det nuvarande NIS-direktivet, att anpassa det till de nuvarande behoven och göra det framtidssäkert.
Det som kan komma att påverka Region Skåne är följande tillägg som finns i förslaget.

- Högre krav på säkerhet och rapportering, där en lista med minimumkrav måste uppfyllas
- Säkerhet för leverantörskedjor och leverantörer
- Striktare tillsynsåtgärder för nationella myndigheter

Lagen om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter
Lagen syftar till att uppgifter från en myndighet som hanteras av en tjänsteleverantör ska få ett sekretesskydd som är likvärdigt med det som gäller när en annan myndighet tillhandahåller en motsvarande tjänst.
Lagen bedöms framförallt ha betydelse för möjligheterna för svenska företag. Lagen förväntas få en begränsad praktisk betydelse med hänsyn till det stora antalet utländska tillhandahållare av it-driftstjänster.
Tystnadsplikten kommer dock bara omfatta vissa tjänsteleverantörers personal. Det är endast dessa leverantörer som det kan bli tillåtet att röja sekretesskyddade uppgifter till. Förklaringen är att brott mot tystnadsplikt utanför Sveriges gränser har svensk domstol domsrätt endast om: 1) den som begått brottet är svensk medborgare eller en utlänning med hemvist i Sverige; och 2) gärningen är straffbar även på gärningsorten.
Tystnadsplikten kan därmed endast åberopas som grund för att röja sekretesskyddade uppgifter till tjänsteleverantörer som kan garantera att den egna (och ev. underleverantörers) personalstyrka är bosatt i Sverige.
Den nya lagen bedöms därför inte ha någon påverkan på Region Skånes möjligheter att utnyttja utländska tjänsteleverantörer för behandling av information som omfattas av sekretess.
Lagen träder i kraft den 1 januari 2021.

Större riskanalyser

SDV
I SDV-programmet har riskanalyser genomförts avseende överföring av information till leverantören Cerner. Analyserna var omfattande och avgränsats till den första fasen, den s.k. migreringen till M1912 och ”onboardingen” till HealtheIntent. Analyserna genomfördes av regionala dataskyddsfunktionen, enheten för juridik, samt förvaltningen digitalisering IT och MT. Syftet med analyserna var att skapa så goda förutsättningar som möjligt inför beslut om överföring av information till leverantören.

Säkerhetsskyddsanalyser
Den 1 april 2019 fick Sverige en ny säkerhetsskyddslag.
Med säkerhetsskydd avses skyddet av säkerhetskänsliga verksamheter mot antagonistiska aktiviteter såsom spionerі, sabotage, terroristbrott och andra

brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

För att veta vilka av våra verksamheter som omfattas av säkerhetsskyddslagen och dess krav ska Regionen enligt lagen genomföra säkerhetsskyddsanalys. Säkerhetsskyddsanalysen är grunden i säkerhetsskyddsarbetet och syftet är att i första steget identifiera de verksamheter som Regionen bedriver och som omfattas av säkerhetsskyddslagen, så kallade säkerhetskänsliga verksamheter. Säkerhetskänsliga verksamheter är verksamheter som uppfyller åtminstone ett av följande tre krav:

- Verksamheten är av betydelse för Sveriges säkerhet
- Verksamheten hanterar Säkerhetsskyddsklassificerade uppgifter
- Verksamheten omfattas av ett internationellt åtagande om säkerhetsskydd.

Efter identifieringen kan berörda verksamheter gå vidare med analysen och bedöma konsekvenser för Sverige, vad som kan hota, vilka sårbarheter som kan utnyttjas av en angripare samt ta fram förslag på Säkerhetsskyddsåtgärder.

I februari 2020 startade Region Skåne upp arbetet med att genomföra säkerhetsskyddsanalyser på samtliga förvaltningar inom Regionen. Arbetet har inledningsvis varit fokuserat på att ta fram styrning kring arbetssätt och metodik samt höjning av säkerhetsskyddskompetens hos berörd personal.
Arbetet med analysen avsågs till en början vara färdig under året men har för flera förvaltningar dessvärre blivit försenat på grund av omprioriteringar till följd av hanteringen av Covid-19.

Även om förseningar i analysen föreligger på en övergripande nivå har flera verksamheter som hittills identifierats kunnat fullfölja sin analys och arbetar för närvarande med de säkerhetsskyddsåtgärder som bedöms behövas för att uppfylla lagkraven. Parallellt med denna hantering arbetar Regionen även med att ta fram förslag på instruktioner för hur arbetet kan bedrivas framöver. Syftet är att bygga upp en säkerhetsskyddsorganisation och regelverk som möjliggör ett systematiskt och kontrollerat säkerhetsskyddsarbete som bedrivs samordnat, kan utvecklas löpande och utvärderas regelbundet.

Åtgärder mot specifika hot

Säkerhetsåtgärder för att stärka skyddet av användarnas datorer

Nedan redovisas generella åtgärder mot specifika hot som är allmänt förekommande mot företag och offentlig sektor i dagsläget.

Under 2020 så stärktes skyddet av användarnas datorer med program mot skadlig kod.

När vi nu valt att använda Microsoft Endpoint Protection så har vi följande funktioner:

- Identifiering av skadlig kod och spionprogram med åtgärder
- Identifiering av spökprogram med åtgärder
- Utvärdering av kritiska säkerhetsrisker och automatisk uppdatering
- Funktioner för upptäckt av säkerhetsproblem i nätverket

Skydd mot elaka länkar i exempelvis e-post har stärkts genom att aktivera en brandväggstjänst som kontrollerar alla länkar och öppnar länkarna i en skyddad miljö som inte utsätter datorn för risk. Denna tjänst blir det viktigaste skyddet mot ransomeware och identitetsstöld.

Förbättringsåtgärder

Informationssäkerhetsaktiviteter i verksamheternas processer

Regionstyrelsen har tidigare beslutat om mål för informationssäkerhetsarbetet. Ett av målen är att *processer där information hanteras ska utformas på ett sätt som innebär att informationstillgångar hanteras säkert. Processer inför beslut om nya verksamhetsstöd, arbetssätt m.m. ska innehålla aktiviteter för att analysera vilka krav som ska ställas på informationssäkerhet.*
Arbetet med detta pågår alltjämt. Både den regionala dataskyddsfunktionen såväl som den regionala informationssäkerhetsfunktionen prioriterar insatser inom detta område eftersom det har stor betydelse för effektiviteten i informationssäkerhetsarbetet.

Inom dataskyddsområdet har en arbetsgrupp för inbyggt dataskydd med representanter från de regionala funktionerna för dataskydd och informationssäkerhet, riskanalysledare från Digitalisering IT och MT samt dataskyddssamordnare från Digitalisering IT och MT, Koncernkontoret och Primärvården har tillsatts. Se bilaga 1 för mer information.

Ny utbildning i informationssäkerhet

En ny e-utbildning med namnet ”Säker informationshantering” introducerades under 2020. Den ersätter tills vidare den tidigare e-utbildningen i informationssäkerhet som funnits några år. Den nya utbildningen ger en grundläggande förståelse för vad det innebär att arbeta i offentlig verksamhet. Den berör lagstiftning, regelverk kring hantering av allmänna handlingar och olika skyddsåtgärder för personuppgifter och annan information som hanteras i vår vardag.
Utbildningen finns i Utbildningsportalen och är inkluderad i introduktionen för nya medarbetare.
Utbildningen bidrar till informationssäkerhetsarbetet då medarbetarnas kunskap om hur olika typer av information är grundläggande.
E-utbildningen kommer under 2021 kompletteras med fler utbildningar för olika målgrupper.

Skyddade personuppgifter
Under året har man från Region Skånes sida tagit initiativ till ett nationellt arbete för att få till en enad hantering av patienter med skyddade personuppgifter. Skyddade personuppgifter är en möjlighet för Skatteverket att markera att en folkbokförd person har en hotbild eller riskerar att utsättas för hot. Varje vårdgivare/myndighet ansvarar för att ta fram rutiner för hantering i sin organisation vilket medför att det ser olika ut. Skatteverket har tagit fram en vägledning som bygger på att uppgifterna är offentliga, men inom hälso- och sjukvården omfattas patientuppgifter alltid av stark sekretess. På Ineras juridik och informationssäkerhetsråd har punkten varit på agendan sedan förra hösten. Den har även lyfts till SKR:s nätverk för hälso- och sjukvårdsdirektörer som ansåg att frågan är angelägen och säger sig vara beredda att godkänna en nationell vägledning. På uppdrag av Ineras juridik- och informationssäkerhetsråds har Region Skånes representant lett en nationell arbetsgrupp med representanter från 12 regioner för att ta fram ett utkast. Det riskanalys som gjordes visar att det med reservnummerhantering uppstår nya risker, främst rörande patientsäkerhet, men även risker i kontakter/kommunikation med andra myndigheter och vårdgivare.
Enligt Region Skånes nu gällande instruktion ska patienter med skyddad folkbokföring rutinmässigt registreras på reservnummer, vilket ställer till med en del bekymmer både för vården, exempelvis bristfällig kunskap om gällande instruktion, flera reservnummer upprättade på en patient, svårigheter vid kommunikation med andra myndigheter/vårdgivare/apotek. Den enskilde patienten kan inte använda 1177 Vårdguidens e-tjänster, högkostnadskort för läkemedel med mera. Det finns ännu ingen nationell rekommendation men resultatet av riskanalysen och problemen påvisar behovet av att se över och uppdatera Region Skånes instruktion så att även patienter med skyddad folkbokföring ska registreras med personnummer, ett arbete som nu pågår. Det kan finnas fall då dokumentation på personnummer inte är tillräckligt säkert, varför instruktionen måste hantera avsteg, då verksamhetschef kan fatta beslut om reservnummerhantering. Arbetet omfattar även att stödja verksamheterna genom att ta fram övergångsrutiner, utbildnings- och informationsmaterial.

Expertgrupp under Covid-19
Under våren 2020 bildades en stab för hantering av krisen. Krisen satte sjukvården på hårt prov såväl som IT och våra expertfunktioner inom juridik, dataskydd, informationssäkerhet och IT-säkerhet.
Under krisen ökade behovet av att kunna möta patienter på distans. Även internt ökade kraven på distansarbete för att inte behöva träffas fysiskt och riskera sprida smitta. Kraven på skyndsamhet mellan idé och realisering för att underlätta under krisen var höga. Etablerade rutiner för hantering av ärenden behövdes optimeras och skyndas på varför den regionala krisledningsstaben fattade beslut om att inrätta en expertgrupp för granskning av tjänster och förändringar som påverkade eller kunde påverka informationssäkerheten. En av utgångspunkterna var att kravet på skyndsamhet inte skulle resultera i undermåliga lösningar utan varje lösning

skulle bedömas både juridiskt och tekniskt innan informationsägaren kunde driftgodkänna utifrån identifierade och värderade risker.
Expertgruppens arbete var en framgång. Expertgruppen granskade under mars – juni 29 ärenden varav 23 avslutats och 6 fortfarande var pågående. Ett flertal ärenden har, efter granskning, krävt förändringar för att möta lagkrav eller verksamhetskrav. Arbetet har därmed haft positiv effekt på kvalitet.
Det arbetssätt som tillämpades var framgångsrikt och bidrog även till spridning av kunskap och insikt i ärendena vilket minskade personberoendet.
En utredning genomfördes efter att Covid-staben avvecklades och behovet av expertgruppen upphörde i det akuta skedet. Utredningens resultat ingår i diskussioner om förändrat arbetssätt.

Övning i Helsingborg

Regionstyrelsen gav Regiondirektören i uppdrag att under 2018/2019 genomföra minst en övning där Region Skånes IT-infrastruktur är otillgänglig för hälso- och sjukvården.
Övningens syfte var att undersöka vårdens beroende av IT-system och i förlängningen vikten av robusta system samt genomtänkt och välkänd planering för avbrott. Övningen fungerade som ett test av den utvalda avdelningens kontinuitetsplanering för IT-avbrott och gav deltagarna ökad medvetenhet och förståelse för Region Skånes krisorganisation och behov av aktuella larmrutiner.
Övningen genomfördes som en seminarieövning där deltagarna under övningsledningens guidning tillsammans diskuterade sina förutsättningar att hantera olika problem. Övningen delades upp i flera etapper där de övade fick beskriva läget på avdelningen och ta fram lägesbilder till möten för delad lägesbild.
IT-beroendet inom vården är stort och möjligheten att bedriva god vård påverkas avsevärt när åtkomst till nätverk upphör. Redan efter två timmar har såväl patientsäkerhet, arbetsmiljö, personalplanering och patientupplevelse påverkats negativt.
Övningen visar på stor komplexitet i vad som påverkar en avdelnings förutsättningar att bedriva vård. Samverkan med andra enheter och hur de påverkas är utmanande att kartlägga. Det pågår dock flera initiativ som kan ge positiva effekter. Delar av verksamheten har påbörjat arbetet med att se över sina arbetsprocesser för att kartlägga informationshanteringen i verksamheten. I arbetet med kontinuitetsplanering kartläggs också verksamheternas beroenden. Viktigt är att IT-beroendet inte glöms bort i detta sammanhang utan undersöks och tas hänsyn till i arbetet med åtgärder.
Andra exempel är utredningen om resursförstärkt läkemedelsförsörjning inför kris, höjd beredskap och krig som ger insikt i en del av utmaningarna kopplat till läkemedelsförsörjning.
Tydligt är att vidare undersökningar krävs för att angripa många av utmaningarna med att bedriva vård utan nätverksuppkoppling. Andra mycket avgörande resursberoenden kan åtgärdas med små medel och ändå förbättra förutsättningarna avsevärt.

Handlingsplan (förslag till beslut i Regionstyrelsen)

I samband med ledningens genomgång ska förslag till handlingsplan lämnas.

1. Medarbetare och chefers kunskap utgör den enskilt viktigaste faktorn för en god informationssäkerhet. Samtliga anställda ska därför under 2021 ha genomgått den grundläggande e-utbildningen i säker informationshantering.

2. Region Skåne upphandlar för stora summar varje år. Det är av stor vikt att egenskaperna hos de varor och tjänster som upphandlas uppfyller säkerhetskrav. Processerna i samband med upphandling och utveckling av nya tjänster ska därför revideras och korrigeras i den utsträckning som behövs för att rätt säkerhetskrav ska ställas.

Uppföljning av tidigare beslut

Underlag till besluten återfinns i föregående års rapporter. Nedan återges besluten i korthet med tillhörande uppföljning.

Översyn av utlämningar till kvalitetsregister och forskning

Regionstyrelsens beslut (§ 278, dnr 1604263, 2018-12-18)

Regionstyrelsen ger Regiondirektören i uppdrag att snarast möjligt, dock senaste 30:e juni 2019:

- genomföra översyn av samtliga pågående utlämningar till kvalitetsregister och forskning för att kontrollera att utlämnandet sker på laglig grund och att beslut om utlämnande har fattats av behörig
- vidta åtgärder för att förhindra att patientuppgifter lämnas ut innan beslut fattats av S-KVB
- lämna förslag till Regionstyrelsen med underlag till beslut om vem eller vilka som ska besluta om tillfälligt utlämnande av hälsodata.

Uppföljning:
Beslutet har inte genomförts.

Riskbedömningar med informationsklassning

Regionstyrelsens beslut (§ 189, dnr 1502668, 2015-11-05)

Regionstyrelsen uppdrar åt regiondirektören att definiera processerna för riskbedömningar och informationsklassning och besluta om vilket eller vilka verktyg som ska användas inom hela Region Skåne för inventering, informationsklassificering, uppföljning och dokumentation av informationssystem och tillhörande skyddsåtgärder.

Uppföljning:
Upphandling har genomförts och ett projekt för införande pågår. Regionstyrelsens beslut har genomförts.

Fördjupade riskanalyser inom SDV

Regionstyrelsens beslut (§ 278, dnr 1604263, 2018-12-18)

Med anledning av det ökande beroendet till externa leverantörer ges Regiondirektören i uppdrag att inom ramen för SDV genomföra fördjupade riskanalyser avseende krav på tillgänglighet till system som stödjer samhällsviktig verksamhet med målet att identifiera åtgärder som behöver vidtas för att säkerställa tillgängligheten såväl under normala omständigheter, som under höjd beredskap och krig.

Uppföljning:
Området för strategisk krisberedskap, säkerhet och miljö (KSM) stödjer och följer SDV:s arbete inom området kontinuitetspanering.

Övning vid otillgänglig IT-infrastruktur
Regionstyrelsens beslut (§ 278, dnr 1604263, 2018-12-18)
Regionstyrelsen ger Regiondirektören i uppdrag att under 2018/2019 genomföra minst en övning där Region Skånes IT-infrastruktur är otillgänglig för hälso- och sjukvården.

Uppföljning:
Regionstyrelsens beslut har genomförts och redovisas i rapporten under rubriken ”Övning i Helsingborg”.