Informationssäkerhetsberättelse 2021

Beslutad 2022-05-xx, av:

REGION JÄMTLAND HÄRJEDALEN

Sammanfattning/bakgrund

2021 har i mycket hög grad präglats av de restriktioner som fortsatt har behövt tillämpas till följd av corona-pandemin. Dessa förutsättningar har skapat ökade insikter inom flera områden som påverkar informationssäkerheten, exempelvis vikten av att kunna arbeta mer flexibelt både i tid och rum. Medarbetare har fått tillfälliga arbetsuppgifter då de bemannat roller som har behövt förstärkas för att klara nya åtaganden såsom covid-intensivvård och vaccinationer.

Grundförutsättningen för arbetet med informationssäkerhet är ett väl fungerande IT-säkerhetsarbete. Det försämrade säkerhetsläget med ökande cyberhot kräver att resurser kan arbeta med att införa aktiva skydd mot intrång, ransomware och stöld av information. Hoten går inte helt att skydda sig emot. Däremot går det i allt högre grad att minska tiden till upptäckt av ett inträffat intrång/angrepp och att kunna agera aktivt på händelsen för att minimera skador. De mycket stora konsekvenser som kan bli resultat av ett angrepp har kunnat ses på nära håll under året genom ett större IT-avbrott hos Kalix kommun. Kostnaderna för detta har varit omfattande och merarbete med att återställa kommunens IT-miljö har tagit mycket stor kraft.

Utökat fokus under 2021 har lagts av tillsynsmyndigheten för dataskydd/personuppgifts-hantering IMY (Integritetsskyddsmyndigheten) på att hitta brister och utfärda höga viten för överträdelser i personuppgiftshanteringen. Som en följd av detta har under 2021 flera större viten (storleksordning 3–4 MSEK) dömts ut till svenska organisationer. Bland dessa finns flera regioner som av tillsynsmyndigheten befunnits ha brister i behörighetstilldelning i vårdsystem samt i skyddet av känsliga personuppgifter som överförts till extern part.

Under 2021 har ett aktivt arbete med rollen informationsägare testats och utvärderats inom ramen för två pilotuppdrag. De verksamheter som deltagit i detta är läkemedelsenheten samt HR-avdelningen. Erfarenheter från pilotuppdragen visar bland annat att det är viktigt att tydligt avgränsa informationsägarens uppdrag/uppgifter.

Regionen har under 2021 besvarat den nationella mätningen/enkäten från MSB kallad ”Infosäkkollen” som för första gången använts för att kartlägga och förbättra informations-säkerheten inom offentlig sektor. Syftet med mätningen/enkäten är att stödja uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter. Regionens resultat visar på att det är mycket arbete som återstår för att kunna nå föreslagen målbild. Områden där extra stor förbättringspotential finns är:

- Riskhantering
- Säkerhet upphandlingskrav
- Inventeringar, undersökningar, omvärldsbevakning

INNEHÅLL

1 Informationssäkerhetsarbete 2021

1.1 Allmänt

Informationssäkerheten i Region Jämtland Härjedalen ska ytterst tillvarata medborgarnas krav på integritet, rättssäkerhet och god service. Regionens informationstillgångar är en vital resurs som avgör regionens förmåga att uppnå sina mål och behöver därför ett väl avvägt skydd.

IT-baserade processtöd har blivit en integrerad del av regionens dagliga verksamheter och är grundläggande för att upprätthålla, stödja och utveckla verksamheten. Därför blir det allt viktigare att förstå och hantera risker och begränsningarna vid användning av IT-stöden.

Under 2021 har corona-pandemin präglat prioriteringar inom hälso- och sjukvården samt i hög grad även hur den administrativa verksamheten har arbetat. Vikten av en god informationssäkerhet inklusive hög informationskvalitet (att informationen är relevant, aktuell och anpassad för sitt syfte) har synliggjorts ytterligare under denna pandemikris. För att uppnå en tillräckligt hög informationssäkerhet krävs ett utökat systematiskt informationssäkerhetsarbete som bedrivs så att det täcker informationens hela livscykel – från att informationen skapas till att den avvecklas/gallras.

Det har under 2021 kommit ytterligare indikatorer på att det krävs utökade resurser mot tidigare för att klara regionens uppdrag inom informationssäkerhet/IT-säkerhet. Inte minst har corona-pandemin visat att verksamheter under hög arbetsbelastning behöver stöttning med enklare och säkrare arbetssätt som minskar administrativa bördor och som kan underlätta genomförande av sina uppdrag. De primära områden som behöver utökade resurser är att ge verksamheterna metodstöd vid informationsklassningar och riskanalyser, att upptäcka och agera på cyberangrepp samt att kunna arbeta mer aktivt med dataskyddsåtgärder (såsom behovs- och konsekvensanalyser).

1.2 Uppföljning aktiviteter 2021

Från föregående års prioriterade arbete enligt övergripande handlingsplan informationssäkerhet 2020-21 finns följande aktiviteter.

Aktivitet	Status för genomförande 2021-12-31
Vidareutveckling hantering av NIS-direktivets krav och åtgärder med fokus på genomförande och uppföljning.	**Pågående.** Gap-analys mot NIS-direktivets krav framtagen. Ska följas upp under 2022.
Förbättrad behörighetshantering i regionens IT-system.	**Inlett.** Behov har identifierats av en central behörighetskälla som håller regionens IT-system/tjänster uppdaterade med korrekta behörigheter. Ännu har ingen behörighetskälla skapats.
Genomförande av åtgärder för höjd robusthet i nätverk, specifikt fastighets-system/styrsystem.	**Pågående.** Åtgärder vidtagna för ökad robusthet/driftsäkerhet.

Fortsätta utveckla arbetssätt och stöd för informationsklassning.	**Pågående.** Klassningsmodell och tillhörande stöd uppdaterade.
Stödja arbetet med att utse informations-ägare i verksamheterna.	**Pågående.** Pilotuppdrag för etablering av informationsägarskap genomfört. Stödmaterial för informationsägare identifierat.
Uppföljning av åtgärder/årshjul för dataskyddsarbetet.	**Kvarstår.**
Framtagning av e-utbildning i informationssäkerhet för chefer och registerkoordinatorer (lokala samordnare för skydd av personuppgifter)	**Kvarstår.**

1.3 Ökat beroende av molntjänster

Tydliga trender som förstärkts under 2021 är att allt fler av de IT-stöd som regionen använder driftas som molntjänster utanför regionens egen lokala IT-miljö.

Regionens lokala IT-driftpartner Atea (som ansvarar för driften av regionens lokala IT-miljö fr o m 2021-11-01) ansvarar för en allt mindre andel av de IT-tjänster som regionen använder. Dessa förutsättningar ändrar delvis förutsättningar för kravställning på IT-miljön inklusive kraven på hur säkerhet ska hanteras. Kraven behöver numera ställas mot allt fler IT-leverantörer av externa molntjänster. Regionens lokala IT-driftpartner (Atea) är alltså bara en av många IT-driftleverantörer för regionen.

Med allt fler IT-driftleverantörer blir det ännu viktigare än tidigare att arbeta strukturerat med kravställning och kravutvärdering mot de som ansvarar för IT-driften av tjänster/system i regionens hela IT-miljö. Större resurser och fokus än tidigare behövs för att kravställa på säkerhet i respektive IT-tjänst samt för att följa upp att kraven efterlevs. En relativ förflyttning behöver alltså stegvis göras inom regionen från leverans av IT-drift (från lokal IT-miljö) till mer kravställande och uppföljande resurser/roller.

1.4 Många beroenden för att nå en god informationssäkerhet

Informationssäkerhet är i grunden inget ”eget område” utan en produkt av att det finns genomtänkta och strukturerade arbetssätt med tydliga roller och ansvar. Bland de områden som i hög grad påverkar vilken informationssäkerhet som kan uppnås finns:

- Tydlig styrning och rollfördelning för hur IT-system kravställs, anskaffas och förvaltas.
- Att den information som används i verksamheterna kartläggs och beskrivs för att kunna upprätthålla tydliga arbetssätt för hur informationen ska hanteras/skyddas.
- Att manuella moment kan automatiseras/digitaliseras för att förenkla flöden, minska arbete som behöver utföras för att hantera informationen samt skapa ett sammanhängande skydd för informationen som används.

1.5 Riskanalyser – förebyggande arbete

Under 2021 har den övergripande riskanalysen för regionens informationssäkerhetsrisker uppdaterats och ett par nya risker som ökat i betydelse under covid 19-pandemin har tillkommit. Den största enskilda risken som identifierats på den övergripande nivån är fortsatt (kvarstår sedan år 2020):

1) bristande medvetenhet hos medarbetarna om hur informationen ska hanteras enligt gällande regelverk (s.k. ”oavsiktligt insiderhot”).

Tillkommande risker i topp under 2021 är:

2) cyberangrepp som kan leda till större IT-störningar/-avbrott. Sedan tidigare har ransomware (skadlig kod, utpressning/informationsstöld) funnits bland risker i topp.

3) felaktigt tilldelade behörigheter för medarbetare

På grund av pandemin har inte riskanalyser för verksamheten kunna genomföras i nödvändig omfattning. Fokus har under 2021 istället lagts på att uppdatera och förenkla regionens modell/regelverk för informationsklassning.

1.6 Cyberhoten ökar

Antagonistiska hot i form av cyberbrottslighet och aktörer som bedriver informations-inhämtning och IT-sabotage har under 2021 ökat ytterligare. Ransomware är fortsatt det största cyberhotet mot regionens IT-system och information. Även säkerhetspolisens utpekande av staters ökade aggressivitet i beaktande i regionens bedömning avseende cyberhot.

1.7 Dataskydd – personuppgiftshantering

Utökat fokus under 2021 har lagts av tillsynsmyndigheten för dataskydd/personuppgifts-hantering IMY (Integritetsskyddsmyndigheten, f.d. Datainspektionen) på att hitta brister och utfärda höga viten för överträdelser i personuppgiftshanteringen. Som en följd av detta har under 2021 flera större viten (storleksordning 3–4 MSEK) dömts ut till svenska organisationer, däribland regioner, baserat på överträdelser av dataskyddslagarna/GDPR. Bland dessa finns flera regioner som av tillsynsmyndigheten befunnits ha brister i behörighetstilldelning i vårdsystem samt i skyddet av känsliga personuppgifter som överförts till extern part.

Detta ger större incitament att fördjupa arbetet med dataskydd som syftar till att medborgarna ska känna sig trygga med att uppgifter om dem hanteras så att personlig integritet upprätthålls. Inte minst behöver behörighetshanteringen i vårdsystemen säkerställas.

1.8 Behörighetshantering

Området behörighetshantering innefattar delar från att behov av information för en medarbetare identifieras, beställning, godkännande, tilldelning, ändring samt borttag av behörigheter i IT-systemen. Under 2021 har inget aktivt arbete bedrivits från informationssäkerhetsfunktionen inom detta område. Orsaken är att andra delar såsom informationsklassning och skyddsåtgärder i stort har prioriterats i första hand baserat på de resurser som finns inom informationssäkerhet och dataskydd.

1.9 Informationsägarskap

För att tydliggöra hur regionens informationstillgångar kan kartläggas och hanteras på ett mer strukturerat sätt behöver rollen *informationsägare* definieras och etableras inom regionen.

Rollen finns med sedan tidigare i rollbeskrivningar kopplade till informationssäkerhet men har ännu inte aktivt lyfts fram i styrningen. Rollen är närmast kopplad till det överordnade området informationsförvaltning av vilket informationssäkerhet är en del. På motsvarande sätt som det finns ägarskap för personalresurser/roller och för ekonomiska tillgångar behövs ett ägarskap för den information som ska försörja regionens verksamheter. Utan tillgång till rätt information i rätt tid går det inte att genomföra verksamheten och uppnå målen på rätt sätt.

Under 2021 har ett aktivt arbete med rollen informationsägare testats och utvärderats inom ramen för två pilotuppdrag. De verksamheter som deltagit i detta är läkemedelsenheten samt HR-avdelningen. I uppdragen har ingått att;

- Tydliggöra vad informationstillgångar kan bestå av och hur de kan kopplas till arbetsflöden och funktioner,
- Identifiera informationstillgångar som används i några viktiga arbetsflöden inom respektive verksamhet,
- Identifiera vilka uppgifter rollen informationsägare ska ha och vilka stöd som rollen behöver för att kunna utföra dessa uppgifter,
- Utse informationsägare för de informationstillgångar som används i valda arbetsflöden,
- Ev. påbörja informationsklassning som en metod för att hitta säkerhetskraven på informationstillgångarna

Erfarenheter från pilotuppdragen visar bland annat att det är viktigt att tydligt avgränsa informationsägarens uppdrag/uppgifter. För att uppnå detta behöver det finnas ett tydligt ”språk” för hur informationsägaren ska kommunicera sina krav på informationen. En viktig del av detta ”språk” är informationsklassningen som ger informationstillgången en ”kravprofil” i form av klassningsnivåer som i sin tur avgör hur informationen behöver skyddas och hur den får hanteras.

1.10 Strategi för informationssäkerhet

Regionen saknar fortsatt en strategi för informationssäkerhet vid utgången av 2021. En strategi bidrar till att välja riktning för organisationen och belyser organisationens vision, mission samt kort- och långsiktiga mål inom ett område. Därmed ges en stöttning av hur arbetet ska bedrivas.

Det övergripande planeringsdokument som t o m 2021 har använts, Övergripande handlingsplan för informationssäkerhet och dataskydd (godkänd av regiondirektör), har fr o m 2022 avvecklats och överförts till lokalpolitiska mål/aktiviteter i Stratsys. Detta gör att behovet av en strategi nu blir ytterligare mer synligt.

2 Inträffade incidenter under året

Gällande större incidenter som har påverkat informationssäkerheten under 2021 finns följande händelse att uppmärksamma särskilt.

2.1 IT-störning

I början av september 2021 drabbades regionen av en större IT-störning/-avbrott i servermiljön. COSMIC journalsystem gick då inte att nå vilket påverkade såväl planerade operationer som telefonrådgivningen på hälsocentralerna. Detta innebar också störningar för distansarbete utanför den lokala IT-miljön. Regionen gick upp i stabsläge under incidenten.

Inledningsvis beslutades att alla planerade operationer skulle ställas in, men dessa kunde återupptas enligt plan. I övrigt togs reservrutiner i bruk för att klara avbrottet. Orsaken till avbrottet har identifierats och åtgärdats. Incidenten fick kvarstående effekter under ett par veckor innan en återgång till normaldrift kunde göras.

Incidenten visar på vikten av fungerande reservrutiner i verksamheten, något som också kräver att reservrutinerna övas regelbundet.

3 Uppföljningar av säkerhetsarbetet

3.1 Uppföljning – mätning ”MSB Infosäkkollen 2021”

Regionen har under 2021 besvarat den nationella mätningen/enkäten från MSB kallad ”Infosäkkollen” som för första gången använts för att kartlägga och förbättra informationssäkerheten inom offentlig sektor. Enkäten kommer att genomföras vartannat år med start 2021 och är en mätning i form av en egenkontroll/självskattning av arbetet de senaste två åren (2019-21). Mätningen är ett regeringsuppdrag till MSB som kommer att slutrapportera den framtagna lägesbilden till regeringen i mars 2022 baserat på de svarande som rapporterat in sin mätning till MSB. Mätningen baseras på en uppföljningsmodell som utgår från MSB:s föreskrifter och stöd, som i sin tur bygger på standardserien ISO/IEC 27000. Modellen ger stöd till uppföljning på en strategisk nivå och ska ge ledningsgrupper ett bättre underlag för uppföljning av det systematiska informationssäkerhetsarbetet. Modellen mäter inte om den enskilda organisationens skydd är tillräckligt.

Syftet med mätningen/enkäten är att stödja uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter. Enkäten besvarades av totalt ca 300 regioner, kommuner och statliga myndigheter. Mätningen behandlar inte enskilda säkerhetsåtgärder, utan fokuserar på de bakomliggande arbetssätten som leder till att organisationer väljer att vidta sådana säkerhetsåtgärder som de gör.

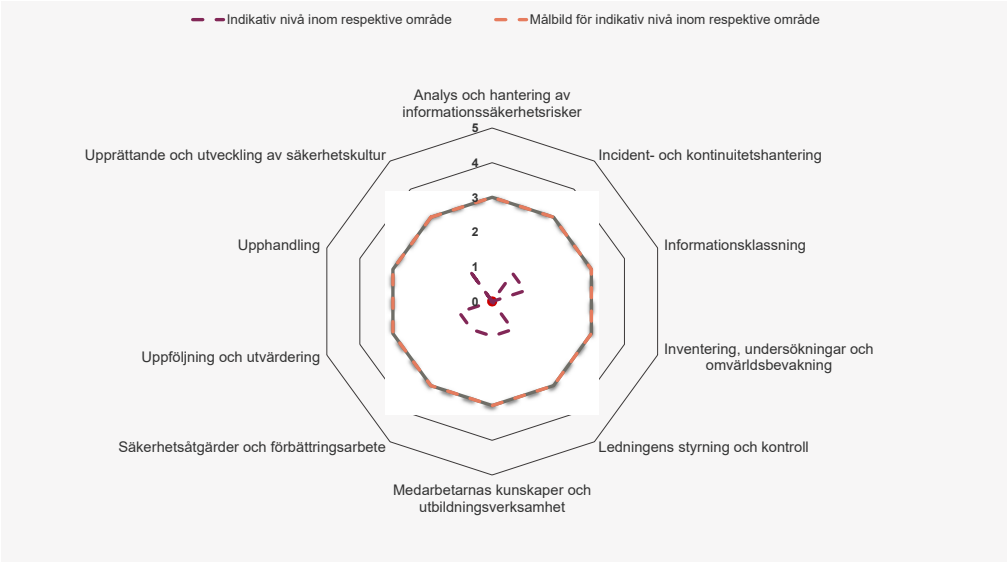
Mätningen har analyserats av MSB som förväntas återkoppla under januari 2022 till de svarande med hur resultatet kan tolkas och hur förbättringar i arbetssätt kan göras baserat på uppnått resultat. Resultatet ger underlag för planering och prioritering, och med regelbundna uppföljningar kan utvecklingen följas över tid. Genom att besvara frågorna ges organisationen också en möjlighet att följa om organisationen har resurssatt arbetet på ett systematiskt och tillräckligt sätt. Med mätningar över tid kommer MSB att kunna stödja organisationer med nyckeltal om hur mycket resurser som normalt sett behövs för att uppnå en viss nivå i Infosäkkollen - och därmed i organisationens eget systematiska informationssäkerhetsarbete.

De nivåer 0–5 som kan uppnås i mätningen definieras enligt:

Nivå 0: Inget eller litet systematiskt arbete enligt rekommenderade arbetssätt kan påvisas
Nivå 1: Organisation har grunderna i informationssäkerhetsarbetet

Nivå 2: Organisation som bedriver informationssäkerhetsarbetet med viss systematik
Nivå 3: Organisation som har ett kvalificerat innehåll i informationssäkerhetsarbetet
Nivå 4: Organisation som arbetar avancerat med ständiga förbättringar
Nivå 5: Organisation arbetar på ett fullt ut systematiskt sätt med förbättringar

Regionens mätresultat för ”Infosäkkollen 2021” visas i resultatdiagrammet nedan. Enkäten innehåller nivåfrågor för 10 st. områden, exempelvis ”Informationsklassning”, ”Medarbetarnas kunskaper” och ”Ledningens styrning och kontroll”. För varje område kan en poängnivå mellan 0–5 uppnås där 5 är högst (bäst resultat). Regionen uppnår i mätningen poängnivåer mellan 0–1 för de olika områdena.



Ovanstående resultatdiagram är hämtat från MBS:s Infosäkkollen. I diagrammet har en *målnivå* angivits vilken är poängnivå 3 (av max 5) för vart och ett av de 10 områdena. Denna målnivå har av informationssäkerhetssamordnare föreslagits för regionledningen att uppnå *inom två år*, vilket ska följas upp senast vid nästa omgång av ”Infosäkkollen” (höst 2023).

För 40 st. nivåfrågor i enkäten så samlades totalt 134 poäng in av totalt 348 (38%).

I mätningen går det att jämföra sig med andra regioner, kommuner och myndigheter. Genomsnittsresultatet för samtliga svarande *regioner* ser ut enligt nedan. Uppnådd nivå ligger i genomsnitt på nivå 1 (av 5) för samtliga områden förutom för ”Upphandling” där nivån är 2.

Analys av regionens resultat: Det är mycket arbete som återstår för att kunna nå föreslagen målbild (= nivå 3 för samtliga 10 områden). Områden där extra stor förbättringspotential finns är:

- Riskhantering
- Säkerhet upphandlingskrav
- Inventeringar, undersökningar, omvärldsbevakning

För att kunna nå högre resultat krävs att mer kraft kan läggas på det strategiska, långsiktiga arbetet, både då det gäller kravhantering och uppföljning/internkontroll.

3.2 Extern revision av informationssäkerhet/IT-säkerhet

Under våren 2021 genomfördes en extern revision av regionens informations- och IT-säkerhetsarbete. Revisionen initierades av regionens revisorer och utfördes av KPMG genom dokumentgranskning, intervjuer samt kartläggning av arbetsprocesser och rutiner. Se RS/338/2021. Bland de viktigaste resultaten från revisionen finns:

- Revisorerna rekommenderar Regionstyrelsen att säkerställa att informationsklassning och riskbedömning genomförs för samtliga verksamhetskritiska system och att kontinuitetsplaner upprättas.

Regionstyrelsens svar: Ansvaret för att informationsklassningar genomförs har placerats på nivån förvaltningsområdeschefer. Ansvaret för att kontinuitetsplaner (avbrottsplaner) har placerats på områdeschefsnivån. Vid utgången av året hade förvaltningsområdescheferna ännu inte påbörjat planeringen av informationsklassningar. Avbrottsplaner (reservrutiner) har utarbetats i viss omfattning för verksamhetskritiska system inom vårdverksamheterna.

- Revisorerna rekommenderar Regionstyrelsen att säkerställa att regionens behörighetshantering hanteras i enlighet med lagar och interna regler samt att en tillräcklig uppföljning sker för att kontrollera efterlevnaden.

Regionstyrelsens svar: Ambitionen är att successivt införa en enhetlig och styrd hantering av behörigheter där samhällsviktiga IT-system/resurser kommer att prioriteras. Det kommer

också att krävas att merparten av regionens behörigheter kan styras från en central behörighetskälla, något som ännu inte har införts. Denna centrala källa bedöms också kunna förenkla uppföljningen av behörigheter i hög grad. Vid årets slut hade arbetet med en central behörighetkälla har ännu inte planerats eller införts.

- Revisorerna rekommenderar Regionstyrelsen att riskanalyser upprättas regelbundet för IT-infrastruktur och drift.

Regionstyrelsens svar: IT-enheten har förstärkts med 1,0 tjänst som IT-säkerhetsspecialist, via statlig finansiering. Regionen har förstärkt med 2,0 Tjänsteansvariga för server och IT-arbetsplats samt för datornätverk. Ansvaret att genomföra riskanalyser ligger på Tjänste-ansvariga/systemansvariga. De båda tjänsterna som Tjänsteansvariga har tillsatts under 2021.

- Revisorerna rekommenderar att upprätta en riskanalys över att privata enheter kan ansluta via fjärraccess till regionens IT-miljö. Utifrån dessa risker fatta beslut om relevanta åtgärder för att möta dessa.

Kommentar dec 2021: Riskanalys har tagits fram.

- Revisorerna rekommenderar att uppdatera befintlig kontinuitetsplan för IT-driften.

Regionstyrelsens svar: Upphandling av nya leverantörer av IT-drift har avslutats under våren och nu pågår arbetet med övertagande och etablering. Revidering av kontinuitetsplaner startar i samverkan med de nya leverantörerna efter att övertagandeprojekten slutförts. Planen var inte uppdaterad vid årets slut.

- Revisorerna rekommenderar att besluta om en regionövergripande rutin för hantering av informationssäkerhetsincidenter.

Regionstyrelsens svar: Ett förtydligande ska tas fram gällande rutinen för hur uppföljning ska ske av rapporterade incidenter/avvikelser inom informations- och IT-säkerhet och vem som ansvarar för vad. Vid årets slut var rutin inte framtagen.

- Revisorerna rekommenderar Regionstyrelsen att säkerställa att den interna kontrollen inkluderar en riskbedömning kopplat till regionens informations- och IT-säkerhet utifrån gällande lagar och interna styrdokument.

Regionstyrelsens svar: Under 2021 införs internkontrollpunkter gällande riskarbetet inom informationssäkerhet och dataskydd. Dessa är riktade mot områdeschefer. För 2022 kommer ytterligare internkontrollpunkter att införas till förvaltningsområdeschefer samt divisionschefer. Internkontrollpunkter för informationssäkerhet riktat till verksamheterna är införda i styrningen fr o m 2022.

3.3 Uppföljning – utbildning medarbetare

Genomförandegraden för regionens e-utbildning i informationssäkerhet (som funnits sedan 2018) riktad till samtliga medarbetare är fortsatt låg, ca 40% av medarbetarna har genomfört denna utbildning med godkänt resultat vid 2021 års slut. Målvärdet för genomförande är 80%. Detta resultat är inte tillräckligt för att nå en gemensam kunskapsnivå om hur regionen ska arbeta med informationssäkerheten i det dagliga arbetsuppgifterna.

4 Genomförda förbättringar

4.1 Allmänt: Förbättringsåtgärder kopplade till informationssäkerheten

Under året har de förebyggande skydden att motstå phishingförsök, skadlig kod samt intrång i IT-miljön förbättrats ytterligare. Arbete har också påbörjats med att kartlägga förutsättningar för att kunna införa ett mer proaktivt, användarnära skydd mot att regionens information hanteras felaktigt. Exempel på denna typ av oavsiktliga fel i hanteringen är att känsliga uppgifter skickas i klartext i e-post eller att regionens information delas via ej godkända publika molntjänster. Målet är att denna typ av användarnära skydd ska göra det enklare att göra rätt samt i övrigt ge utökad vägledning i den praktiska informationshanteringen.

4.2 Utökade skydd mot intrång – cyberangrepp

Inga nya intrångsskydd har tillförts under året. Fokus har legat på att förbättra användandet av befintliga skydd samt det pågående arbetet med att vidareutveckla en försvarbar IT-arkitektur.

4.3 Utvärderingar av skydd mot olovlig åtkomst till datornätverk och informationssystem

Regionen arbetar löpande med att förbättra åtkomststyrningen till system och nätverk. Vilka utvärderingar som gjorts inom detta område faller utanför denna årliga redovisning av säkerhetsarbetet.

4.4 Hantering av privilegierade (höga) behörigheter i IT-miljön

Omfattande arbete har genomförts under se senaste åren med att reducera antalet systemadministrativa konton samt att upprätta en struktur där nödvändiga systemadministrativa behörigheter tilldelas restriktivt, och begränsat till de system som arbetsuppgiften kräver.

4.5 Uppdaterad modell för informationsklassning

En ny, förbättrad modell för regionens informationsklassning har tagits fram under året. Modellen förtydligar vilka klassningsnivåer som ska användas (baserade på en uppsättning konsekvenskategorier/-nivåer) och är anpassad till MSB:s nationella metodstöd för informationssäkerhet. Modellen ska kunna användas genomgående för samtliga informationsklassningar som genomförs inom regionen.

4.6 Genomförda informationsklassningar

Under 2021 har ytterligare grund lagts för att kunna arbeta effektivare med informations-klassningar av verksamhetens informationstillgångar. Så som konstaterats även föregående år 2020 innebär detta arbete stora utmaningar eftersom tillräcklig tillgång till metodstöd krävs för att planera och genomföra nödvändiga klassningar, något som dagens resurser inte räcker till.

Arbetet med kartläggning och klassning av informationen fortsätter under 2022 med ett till detta kopplat lokalpolitiskt mål i verksamhetsplaneringen. Arbetet kommer att kräva ett relativt

omfattande metodstöd för att kunna bedrivas i tillräcklig omfattning inom berörda *samhällsviktiga* verksamheter, vilka har prioriterats för kartläggning/klassning.

4.7 Införande av informationsskyddet MIP

Under 2021 har arbete skett inom Office365 förvaltning (e-post, Teams, Office-applikationer) med att införa informationsskyddet MIP (Microsoft Information Protection). Under året har en pilot genomförs inom HR-avdelningen som fått prova MIP. Skyddet i MIP bygger på att en känslighetsnivå (etikett för klassning) sätts på e-post, dokument och Teams baserat på vilket informationsinnehållet är. Genom att klassa innehållet via etiketter kan man medvetandegöra hur informationen ska hanteras och sätta automatiska regler som krypterar informationen, gör den tillgänglig bara för en viss grupp användare alternativt hindrar att en fil sparas i en molntjänst eller på en lagringsyta som inte är godkänd. Genom att använda MIP underlättas att kunna uppfylla exempelvis dataskyddslagarna/GDPR genom att kunna skydda känsliga personuppgifter. MIP planeras att införas löpande i verksamheterna med början under 2022.

4.8 Förbättringar i internkontrollen

För att förstärka regionens systematiska informationssäkerhetsarbete har ett litet antal interkontrollmoment tagits fram för att mäta och följa upp hur regelverket för informationssäkerhet och dataskydd efterlevs i verksamheterna. Kontrollmomenten ska införas i Stratsys internkontrollmodul under 2022 som ett led i den löpande uppföljningen/ egenkontrollen. Detta ska bidra till att uppfylla kraven på uppföljning/mätning av informationssäkerheten.

Kraven på dokumenterad uppföljning ställs från bland annat dataskyddslagstiftningen (SFS 2018:218), NIS-lagen (lag om informationssäkerhet för samhällsviktiga och digitala tjänster, SFS 2018:1174), ISO 27001-standarden liksom från Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Övergripande krav på mätning och uppföljning ställs också från Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete (SOSFS 2011:9), se 3 kap. 2 §: ”Vårdgivaren eller den som bedriver socialtjänst eller verksamhet enligt LSS ska med stöd av ledningssystemet planera, leda, kontrollera, följa upp, utvärdera och förbättra verksamheten”. Se även Systematiskt förbättringsarbete kap.5, 2 § egenkontroll: ”Vårdgivaren eller den som bedriver socialtjänst eller verksamhet enligt LSS ska utöva egenkontroll. I egenkontrollen ingår att kontrollera att verksamheten bedrivs enligt de processer och rutiner som ingår i ledningssystemet.”

4.9 Byte av driftleverantörer för regionens IT-miljö

Under hösten 2021 har regionen påbörjat nya driftavtal med nya IT-driftleverantörer för IT-arbetsplats och server samt nätverk. Samtidigt med övergången till de nya leverantörerna har regionens Helpdesk överförts från extern leverantör till intern regi inom regionen.

Ett nytt säkerhetsforum har skapats med representanter för leverantörerna i samband med övertagandet för de nya driftavtalen.

4.10 Ny enhet för informationsförvaltning skapas 2022

Under 2021 har beslut fattats av regionstabschef att tillskapa en ny enhet under Samordnings-kansliet, kallad Enheten för informationsförvaltning. Enheten kommer att överta uppgifter och

personella resurser som idag finns hos enheten för Krisberedskap, säkerhet och miljö respektive Sekretariatet. En ny enhetschef rekryteras. I enhetens uppdrag ingår bland annat att stödja en aktiv informationsförvaltning inom regionen, att införa och förvalta ett e-arkiv, att styra och samordna informationssäkerhet och dataskydd samt att förvalta ett antal av regionens administrativa system.

4.11 Nyckeltal för uppföljning

Under 2021 har ett antal nyckeltal (indikatorer) tagits fram för att kunna mäta och följa upp det systematiska informationssäkerhetsarbetet. Dessa nyckeltal ska spegla olika fokusområden såsom skydd mot skadlig kod, utbildning, informationsägarskap/-klassning och behörighetshantering. Mätningen av dessa nyckeltal påbörjas under 2022 som blir ett första år för att testa denna typ av uppföljning.

4.12 Avbrottshantering

Avbrottshantering för regionens kritiska informationstillgångar: Målstyrningen av arbetet med avbrottshantering överförs från informationssäkerhetsfunktionen till det förbättringsarbete som bedrivs inom ramen för utveckling av civilt försvar/ökad robusthet i försörjningsflöden (Enheten för Krisberedskap, säkerhet och miljö). Där ses verksamhetskritisk information/ kommunikation som ett av de viktiga försörjningsflödena vid sidan om exempelvis personal, el, vatten, läkemedel, livsmedel och värme.

5 Identifierade behov och förbättringar

5.1 Automatiserade arbetssätt ger högre säkerhet

Vid kartläggning av arbetssätt och informationsflöden inom regionen har i flera fall hög grad av manuella moment identifierats. Dessa består exempelvis av att information tas ut på papper eller läses från skärm för att sedan matas in manuellt på nytt i ett annat IT-system. Det kan också bestå i att hantera pappersutskrifter med känsliga uppgifter i skrivare istället för att överföra informationen elektroniskt. I detta fall är det lättare att styra vem som har åtkomst till uppgifterna.

För att undvika dubbelarbete och uppnå att informationen registreras på ett ställe och därifrån hämtas till övriga system från denna källa krävs systemintegrationer och tydligt utformade informationsflöden. Detta tillsammans med införande av automation/digitalisering av återkommande moment skapar bättre och billigare flöden med högre informationskvalitet. Att kunna lägga resurser på att uppnå detta blir viktigt för att kunna komma bort från dyra, osäkra och ineffektiva arbetssätt.

5.2 Ökad digitalisering kräver ett strukturerat säkerhetsarbete

Värdet av en ökad digitalisering för att klara nya utmaningar och för att kunna jobba smartare och mer flexibelt har blivit tydligare under pandemiperioden. Dessa förutsättningar har sammantaget ställt informationssäkerheten på nya prov, då de ändrade arbetssätten behöver kartläggas och säkras. Väsentligt är att medarbetarna får grundkunskaper för att kunna klara att arbeta på ett informationssäkert sätt utifrån de nya förutsättningarna. Konkreta resultat

gällande hur pandemin påverkat arbetssätt är delvis för tidigt att se, även om vissa trender, som kommit för att stanna, har börjat bli tydliga:

- Ökade behov av att kunna arbeta mobilt – medarbetarna behöver informationen för att kunna utföra sina arbetsuppgifter på den plats där de befinner sig.
- Behov av att kunna korta ledtider i exempelvis beställningar av nya behörigheter i IT-systemen, att snabbt kunna sätta upp nya tjänster som krävs för att stödja arbetssätt – såväl tillfälliga som mer varaktiga.
- Ökad förmåga att automatisera uppgifter som idag fortfarande utförs manuellt med stor resursåtgång både i tid och personalresurser, vilket innebär höga kostnader som skulle kunna undvikas.
- Behov att kunna arbeta säkert i nya arbetsprocesser med högre grad av digitalisering för att inte riskera informationsförluster, störningar i IT-miljön och höga viten orsakade av överträdelser av personuppgiftslagar/GDPR.

Sammantaget kommer ovanstående behov att behöva tillgodoses med investeringar i automation, digitalisering samt processer och utrustning som stödjer mobila arbetssätt. Dessa investeringar kommer att kunna betala sig på några års sikt men utan sådana satsningar kommer stora kostnader fortsatt att behöva läggas på att upprätthålla manuella arbetssätt.

Informationssäkerheten behöver ”hänga med” i utvecklingen och kommer att kräva utökade resurser för att kunna uppnå tillräcklig säkerhet i informationshanteringen.

6 Prioriterad inriktning för kommande arbete

Prioriterat arbete framåt inkluderar följande områden:

- Tillhandahålla metodstöd för informationskartläggning – informationsklassning till verksamheterna och ge tydliga underlag för att kunna utföra klassningen på ett enhetligt sätt för regionens samtliga verksamheter med fokus på samhällsviktiga verksamheter.
- Förbättra regionens behörighetshantering genom att förbereda för att införa en central behörighetsstyrande källa som förenklar styrningen av behörigheter och möjliggör automation av tilldelning/borttag för behörigheter i regionens IT-stöd.
- Göra det enklare för medarbetarna att göra rätt i den dagliga informationshanteringen – ökat fokus på det användarnära stödet att hantera informationen på rätt sätt inklusive hur informationsklassning ska ske.
- Följa upp tidigare genomförd säkerhetsanalys baserad på ett urval kontroller från ramverket ”CIS Controls” (som utgår från 20 st huvudområden benämnda ”Critical Security Controls”). Dessa kontroller är rekommenderade skyddsåtgärder som verksamheter bör implementera för att minimera risken för kända cyberangrepp.

- Utöka det systematiska dataskyddsarbetet för skydd av personuppgifter genom uppföljning av att obligatoriska, lagstyrda åtgärder enligt dataskyddslagstiftningen efterlevs.

- Vidareutveckla format på underlaget till ledningens genomgång samt tydliggörande av förväntat resultat som ska uppnås från ledningens genomgång för området informationssäkerhet.

- Införa systematisk incidenthantering med rapportering och uppföljning av inträffade säkerhetsincidenter och säkerställa att kännedom finns hos berörda om hur denna hantering ska ske.

- Säkerställa att kontinuitetsplan för IT-infrastrukturen tas fram och överlämnas till förvaltning.