Informationssäkerhetsberättelse 2020

REGION JÄMTLAND HÄRJEDALEN

Sammanfattning

Under året har regionens behov av informationssäkerhetsarbete ökat alltmer i takt med de ökade kraven på tillförlitlig informationshantering. De främsta skälen till detta har varit det ökade säkerhetsmedvetandet i samhället med anledning av covid-pandemin samt de ökande hoten mot vår information. Dessutom har den ökade digitaliseringen skapat allt större behov av säkerhetsåtgärder och systematiska arbetssätt. En ökad prioritering av säkerhetsarbetet medger att takten i digitaliseringen kan öka. Därmed blir det också allt tydligare varför säkerhetsarbetet behöver prioriteras högre än tidigare.

Ett flertal förbättringsarbeten inom informationssäkerhet och dataskydd (säker personuppgiftshantering) har genomförts under året. Insatserna har dock behövt minskas jämfört med planerat på grund av Coronapandemin och den stora arbetsbörda denna inneburit och fortsatt innebär för vårdverksamheterna, men också för regionen i stort. Informationsklassning har varit ett prioriterat område i flera år, det är ett omfattande arbete som kommit ytterligare en bit framåt, men det är av största vikt att Regionen kan öka takten i det arbetet. Det saknas också fortfarande en långsiktig strategi för informationssäkerhetsarbetet.

Insikten har under året ökat hos regionens medarbetare och ledning om att ett aktivt säkerhetsarbete i hög grad kan bidra till att effektivisera och förenkla regionens uppdrag och arbetssätt. Det är fortsatt mycket utmanande att kunna hålla jämna steg mellan säkerhetsinsatser och den allt snabbare utvecklingen i informationshanteringen, inte minst genom ökad digitalisering. Regionens verksamheter har idag ett ännu högre IT-beroende än för ett år sedan, vilket bidrar till ytterligare större risker och potentiella sårbarheter.

NIS-direktivet (lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) trädde i kraft under 2018 och får en allt tydligare innebörd då det gäller skydd av informationen som hanteras i samhällsviktig verksamhet. Detta direktiv sätter ytterligare fokus på vikten av att kritiska uppdrag och verksamheter har tillgång till rätt information i rätt tid. Kunskapen om krav som behöver uppnås för att efterleva dataskyddslagarna (GDPR) har ökat i organisationen. Resurser har tillförts under året och arbetssätt har utifrån detta kunnat etableras på ett mer systematiskt sätt än tidigare.

I enlighet med prioriteringar i flera andra regioner är bedömningen att Region Jämtland Härjedalen också behöver tillföra säkerhetsområdet mer resurser för att kunna hantera utmaningarna. I slutänden kommer ökade resurser kunna bidra till att minska kostnaderna från säkerhetsbrister. Detta är kostnader som har varit och fortsatt är svåra att identifiera och prioritera utifrån. Ökade insikter om säkerhetsrisker och deras konsekvenser har uppnåtts genom en rad allvarliga händelser i omvärlden, inte minst kopplade till cyberattacker mot redan mycket ansträngda hälso- och sjukvårdsverksamheter som är under extrem press från den allvarliga Coronapandemin.

Informationssäkerhetsberättelse 2020
Dnr RS/45/2021
2021-02-25

Fastställd av:
Regionstyrelsen 2021-03-23--24, § 37

Region Jämtland Härjedalen
Box 654, 831 27 Östersund
www.regionjh.se

INNEHÅLL

Informationssäkerhetsberättelse 2020
Dnr RS/45/2021
2021-02-25

Fastställd av:
Regionstyrelsen 2021-03-23--24, § 37

Region Jämtland Härjedalen
Box 654, 831 27 Östersund
www.regionjh.se

Informationssäkerhetsberättelse 2020
Dnr RS/45/2021
2021-02-25

Fastställd av:
Regionstyrelsen 2021-03-23--24, § 37

Region Jämtland Härjedalen
Box 654, 831 27 Östersund
www.regionjh.se

1 Informationssäkerhetsarbete 2020

1.1 Allmänt

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

Coronapandemin har ökat exponeringen mot olika säkerhetshot och gjort att antalet risker har utökats avsevärt, något som fått till följd av att riktade och utökade säkerhetsåtgärder krävts. Parallellt har också pandemin inneburit ökad användning av digitala verktyg och tjänster, vilket är positivt på många sätt, men det innebär nya risker för en säker informationshantering. Behovet av att öka takten för såväl teknisk som organisatorisk säkerhet har blivit tydligt.

Säkerhet för regionens information ses alltmer som en möjliggörare och inte längre som ett ”nödvändigt ont” vilket i hög grad var synsättet tidigare på säkerhetsområdet. Genom att säkerhetsfrågorna blivit mer centrala och fått genomslag går det också att öka takten i digitaliseringen. På så sätt kan regionen förbättra verksamhetsprocesser som tidigare i högre grad fick hanteras med manuella rutiner som kan utföras enklare och snabbare med hjälp av digitala stöd.

Ett flertal förbättringar har genomförts under året. Samtidigt har pandemin försvårat förutsättningarna för att arbeta systematiskt med informationssäkerhet. De mål och aktiviteter som fanns i handlingsplan för informationssäkerhet 2020 har endast delvis kunnat genomföras. Det har varit svårt för verksamheter att kunna prioritera det arbetet. Området upplevs också som svårt av många chefer och det finns ett stort behov av stöd till verksamheterna i frågorna. Samtidigt har pandemin gjort behovet av ett mer aktivt säkerhetsarbete tydligare utifrån behoven av tillgång till kritisk information. Rätt information med rätt kvalitet i rätt tid till rätt person har blivit ännu mer avgörande än tidigare för att lyckas med verksamheternas uppdrag.

1.2 Uppföljning aktiviteter 2020

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

Aktivitet	**Status för genomförande 2020-12-31**
Ta fram och etablera utbildning/stöd i informationssäkerhet till chefer och systemförvaltningsansvariga roller	**Ej genomfört.** Arbetet har inte hunnits med under 2020 utan är framflyttat till 2021.
Etablera systematisk kontinuitetshantering för verksamhetskritiska informationssystem i utpekade vårdverksamheter	**Delvis genomfört.** Arbetet har försenats och försvårats med anledning av pandemin. Under hösten återupptogs dock arbetet, riktlinjer och rutiner som stöd finns

Aktivitet	Status för genomförande 2020-12-31
	utarbetade. Arbetet med avbrottsplanering specialistvården har fortsatt.
Etablera en ändamålsenlig internkontroll med ett riskbaserat arbetssätt för informationssäkerhet (generellt)	**Ej genomfört.** Arbetet har inte hunnits med. Planeras till 2021.
Identifiera, planera och genomför skyddsåtgärder för att efterleva NIS-direktivets krav enligt Cyber Assessment Framework	**Ej genomfört.** Arbetet har fått pausats med anledning av pandemin och pågående IT-driftsupphandlingar som behövt prioriteras.
Revidera regionens informations-klassningsmodell inklusive hanterings-regler genom att arbeta enligt MSB:s metodstöd för informationssäkerhet	**Delvis genomfört.** Arbetet har påbörjats, men inte hunnit göras klart. Området är högt prioriterat kommande år.
Etablera arbetssättet med informations-klassning och hanteringsregler i verksamheterna genom utbildning	**Delvis genomfört.** Arbetet påbörjat i ett fåtal verksamheter i Regionstaben. Mycket arbete återstår.
Fortsätta arbetet och slutföra de uppdrag som delats ut utifrån förstudie behörighetshantering	**Delvis genomfört.** IT-avdelningen har givits uppdrag om att utreda behörighetsstyrande källa och påbörja förbättringar inom behörighetshantering. Mycket arbete kvarstår och alla delar i tidigare förstudie 2019 är inte omhändertagna.
Fortsatta förbättringar av system för sårbarhetsskanningar och logganalys	**Genomfört.** Arbetet är till stor del genomfört.
Vidareutveckla användning och nytta av insamlade infrastrukturella loggar	**Genomfört.** Arbetet är påbörjat och vidareutvecklas kommande år.
Utarbeta processtöd avseende informationssäkerhet och dataskydd för anskaffning och införande av nya IT-tjänster	**Delvis genomfört.** Påbörjat i samverkan med Utvecklings- och digitaliserings-enheten. Processtöd saknas ännu och arbetet behöver fortsätta kommande år.

1.3 Informationsklassning – ett prioriterat område

En viktig del av regionens systematiska arbete med informationssäkerhet är att genomföra informationsklassningar av informationstillgångar i verksamheten. Det har varit ett prioriterat område i flera år, det är ett omfattande arbete och har varit svårt att komma framåt i önskvärd takt. Det är av största vikt att Regionen kan öka takten i arbetet med informationsklassning, vilket bl.a. innebär att:

- Informationsklassa verksamhetskritiska informationstillgångar för gemensamma administrativa stödprocesser
- Öka medvetenhet om vilka skyddsbehov som finns för kritiska informationstillgångar inom administrativa stödprocesser
- Förbättra skydd/säkerhet för kritiska informationstillgångar som ingår i denna klassning
- Säkerställa funktion för kritiska verksamheter och identifiera behov av reservrutiner

Sammantaget ska genomförda informationsklassningar bidra till ökad robusthet i informationsförsörjningen samt att minska de kvalitetsbristkostnader som uppkommer genom bristande säkerhet i informationshanteringen.

Som ett stöd i det systematiska arbetet med informationsklassning har regionen under 2020 påbörjat utvärdering av ett klassningsverktyg för att praktiskt kunna utföra klassningen av informationstillgångar. Verktyget innehåller funktioner för identifiering och registrering av tillgångar, genomförande av klassning utifrån en konsekvensbedömning, riskbedömning samt åtgärdsplanering och uppföljning.

Under året har också ett uppdrag genomförts med externt konsultstöd avseende informationskartläggning och inledande klassning av informationstillgångar. Detta avser områdena HR/personal, ekonomi samt ledningssystem/Centuri dokument. Arbetet lägger en grund för kommande informationskartläggningar och ger stöd då informationsägare ska utses i verksamheterna.

1.4 Uppföljning av åtgärder för NIS-direktivet

Under 2020 har Regionen i arbetet med Cyber Assessment Framework besvarat samtliga påståenden och värderat dessa utifrån Regionens nuläge. Arbetet med att ta fram åtgärdsförslag har påbörjats inom samtliga delområden men av resursskäl inte kunnat slutföras under året. Hittills har ca 100 åtgärder identifierats varav har 20 ansetts röra grundläggande behov och har därför redan påbörjats eller slutförts.

1.5 Förvaltningsstyrning och digitalisering

Arbetet med att förbättra regionen förvaltningsstyrning inleddes under 2019, inte minst genom en övergripande behovsanalys inom ramen för en genomlysning av regionens IT-verksamhet. Under 2019 påbörjades också inom Samordningskansliet framtagningen av en ny förvaltningsmodell, vilken har förtydligats ytterligare under 2020. En mindre pilotutvärdering påbörjades också under 2020 av ett verktygsstöd för förvaltningsstyrning (DIGframe/Stratsys).

Under 2020 har ytterligare steg tagits för att uppnå en förbättrad och mer strukturerad styrning av regionens förvaltning av IT-tjänster/-system. Detta har gjorts via ett uppdrag, beställt av regiondirektören. Uppdraget syftar till att inventera samtliga IT-stöd/system inom regionen och utifrån dessa skapa en förvaltningsbar ”objektstruktur” (FOA objektkarta). Detta ska bidra till en mer strukturerad förvaltningsstyrning med tydligare uppdrag, roller och ansvar.

Hur denna förvaltningsstyrning utformas och införs kommer att få stor inverkan på möjligheterna att kunna bedriva ett ändamålsenligt säkerhetsarbete. Det kommer också att påverka möjligheterna att bedriva en adekvat arkivverksamhet för att på bästa sätt ta om hand regionens informationstillgångar under hela deras livscykel.

Hur säkerhetsarbetet kan bedrivas är också i hög grad beroende av ett strukturerat arbete med regionens digitaliseringssatsningar. Inom detta område är det strukturerade, långsiktiga arbetet endast i sin linda, och många delar återstår för att kunna bedriva ett strategiskt digitaliseringsarbete inom regionen. Exempelvis saknar regionen ännu en strategi för

digitalisering, något som gör att digitaliseringsmål och styrning ännu förblir oklar. Därmed blir det än mer oklart hur säkerhetsfrågorna ska hanteras inom ramen för digitaliseringsarbetet.

1.6 Informationsägarskap

Ett tydliggjort ägarskap för regionens informationstillgångar är fortsatt en primär framgångsfaktor för en effektiv och säker informationsförsörjning. Genom att informationsägare utses inom organisationen ökar förutsättningarna att steg för steg kunna öka informationens kvalitet (riktig, aktuell och begriplig) samt säkerhet (tillgänglig och endast åtkomlig för behöriga).

Mycket arbete återstår inom detta område. Under hösten 2020 har ett inledande uppdrag kring informationskartläggning bedrivits, där informationsklassning är en del. Uppdraget ska lägga en grund för kommande arbete och har omfattat workshops med företrädare för ledningssystem/dokumenthantering, HR-området samt ekonomiområdet. En viktig del i uppdraget har varit att få en ökad förståelse för rollen som informationsägare och vad som ligger inom ansvaret för denna roll.

Ett beslut har fattats av regionledningen att påbörja utseendet av informationsägare i verksamheterna. Detta ska ge ett tydligare mandat och ansvar i arbetet med att säkra informationens kvalitet och skydd. När informationsägare finns utsedda, kommer det att ge bättre förutsättningar för att arbeta med säkerheten kring informationshanteringen.

1.7 Behörighetshantering

Arbetet med förbättrad behörighetshantering i regionens IT-system innebär mycket stora utmaningar. Under slutet på 2020 har Datainspektionen (numera Integritetsskydds-myndigheten fr o m 2021-01-01) utdelat höga viten till regioner och privata vårdgivare för överträdelser mot dataskyddslagstiftningen. Överträdelserna som avses gäller hantering av behörigheter i det centrala vårdadministrativa systemet, motsvarande regionens system COSMIC.

Behörighetshantering är ett viktigt grundläggande område för att få kontroll över vem som har tillgång till vilken information. Detta påverkar i slutänden möjligheterna att kunna bedriva ett effektivt arbete i samtliga verksamheter. Under 2020 har ett uppdrag påbörjats inom IT-avdelningen i syfte att förenkla tilldelning av behörigheter till en central behörighetskälla (AD-katalogen). Detta är en del av processen för att säkerställa att medarbetarna har aktuella och tillräckliga men inte för omfattande behörigheter. Under 2021 behöver detta arbete utökas för att också kunna komplettera med delar för förenklade beställningar, uppföljningar samt automatiserade tilldelningar/borttag av behörigheter i regionens allt fler IT-system/-tjänster. I dagsläget hanterar regionen mellan 400–700 st IT-system (beroende på hur definitionen av ”IT-system” görs), vilket innebär en allt större administrativ börda att upprätthålla och förvalta. Merparten av behörighetshanteringen i Regionens verksamhetssystem sker fortfarande manuellt.

1.8 Ökande cyberhot mot vårdens journalsystem och patientuppgifter

Bland de som varnar för ökade hot från hackerattacker med utpressningsprogram mot sjukvårdens journalsystem finns MSB. Attackerna kan ske bland annat via s.k. ransomware, vilket innebär att hackare gör intrång och kapar hela eller delar av en verksamhets IT-system. Informationen i systemet krypteras och blir därmed omöjlig att komma åt för medarbetarna. Därefter hotar angriparen med att publicera den känsliga informationen om inte en lösensumma betalas ut. Den svenska säkerhetsmyndigheten CERT.SE gör bedömningen att utpressnings-attacker mest troligt kan slå hårdare mot vården än andra sektorer i samhället.

Under året har också amerikanska myndigheter, bland andra FBI, varnat sjukvårdssektorn i USA för ökat hot från ransomware-attacker. Det som är delvis nytt i dessa attacker mot tidigare är att angriparen först etablerar sig i nätverket innan man slår till och låser eller stjäl informationen. Detta gör det svårare att upptäcka intrången och att man är utsatt för attacken. Angriparen hotar i flera fall även med att publicera exempelvis stulet innehåll i patientjournaler öppet på Internet och kan på så sätt även utöva utpressning mot enskilda personer (medborgare/patienter).

Regionen har under året ökat förmågan att skydda sin information och datanätverk mot denna typ av attacker, något som påverkar prioriteringar i allt högre grad.

1.9 Strategi för informationssäkerhet

Regionen saknar fortsatt en uttalad strategi för informationssäkerhet, något som försvårar genomförande och uppföljning av arbetssätt inom säkerhetsområdet. Detta har lyfts fram som en brist vid ledningens genomgång. En strategi ger en viljeinriktning från ledningen och blir ett naturligt nästa steg för att peka ut en tydligare riktning och kunna få med säkerhetsfrågorna i regionens digitaliseringsarbete. Säkerheten skulle med en strategi som hjälpmedel för styrning också få en närmare koppling till det övergripande arbetet med informationsförsörjning av regionens verksamheter. Detta kan också bidra till en mer integrerad och fördjupad samverkan mellan funktionsområden och aktörer inom regionen. Inte minst skulle också en strategi bidra till ett uttalat stöd för säkerhetsfrågorna och ge en mer naturlig koppling mellan ledningsnivå och hur informationsskyddet kan stärkas i verksamhetens processer. Detta stärker i slutänden informationsförsörjningen och ger högre kvalitet på informationen samtidigt som det bidrar till hållbar utveckling med hanterbara kostnader.

2 Riskanalyser och egenkontroll

2.1 Riskanalyser – förebyggande arbete

Under 2020 har den övergripande riskanalysen för regionens informationssäkerhetsrisker uppdaterats vår och höst. Denna övergripande riskanalys syftar till att få en aggregerad bild av de allvarligaste riskerna mot regionens informationstillgångar. Den övergripande riskanalysen presenteras vid ledningens genomgång följd av en diskussion med ledningen om lämpliga riskreducerande åtgärder.

Den största enskilda risken som identifierats på den övergripande nivån är bristande medvetenhet hos medarbetarna om hur informationen ska hanteras enligt gällande regelverk. Den typ av åtgärd som kopplar mot denna risk är utbildning och informationsspridning till medarbetarna. Inför 2021 behöver också andra åtgärder än regelrätt utbildning genomföras för att höja medvetenheten, exempelvis övningar i form av diskussionsexempel rörande säkerhet i den egna verksamheten - att ta upp på arbetsplatsträffar - samt kontrollfrågor som får besvaras av slumpvisa medarbetare i ”minienkäter”. Regionen har också utsedda ”registerkoordinatorer” för varje område, med roll att stödja sin verksamhet i dataskyddsarbetet (skydd av personuppgifter), en roll som med tiden fått en ökad betydelse i säkerhetsarbetet.

Följande är de största övergripande riskerna enligt den senaste övergripande riskanalysen:

1. Medarbetare hanterar känslig information felaktigt genom att exempelvis spara den på en lagringsyta med bristande skyddsnivå eller överföra den via e-post – ”passiv delning på felaktigt sätt”.

2. Medarbetare delar (omedvetet) känslig information till obehörig i tro att informationen får delas – ”aktiv delning i god tro”.

3. Internkontroll/egenkontroll för informationssäkerhetsåtgärder genomförs inte i verksamheten vilket leder till att arbetssätt inte följs och att risker inte hanteras.

4. Informationsklassning genomförs inte av verksamhetens information vilket gör att behov av skyddsnivå för informationen inte är tydliggjord.

5. Teknisk sårbarhet möjliggör intrång med läckage av känslig information som följd.

Flera av ovanstående övergripande risker ökar som en följd av den allt snabbare digitaliseringen. Utvecklingen gör att alltmer information hanteras digitalt och kan delas till en stor mängd användare på enkelt sätt. Digitaliseringen ökar alltså den totala sårbarheten i informationshanteringen samtidigt som den bidrar med stora effektiviserings- och kvalitetsvinster.

Riskanalyser genomförs i samband med vissa informationsklassningar vid anskaffning (inköp) och införande av nya IT-system. Innan ett nytt IT-system kan införas behöver anskaffningen göras enligt en standardiserad anskaffningsprocess där informationsklassning är en del. Om informationsklassningen visar att informationen som ska hanteras i IT-systemet får en hög/mycket hög klassningsnivå ska klassningen kompletteras med en riskanalys för att kunna hitta de största riskerna och arbeta förebyggande med dessa. Detta spar/undviker i slutänden oönskade kvalitetsbristkostnader som annars kan uppstå då IT-systemet ska tas i bruk.

2.2 Internkontroll

Regionens internkontroll, där egenkontrollen i respektive verksamhet är en del, är tillsammans med avvikelsehanteringen ”motorn” i förbättringsarbetet inom såväl informationssäkerheten som annan kvalitetsutveckling.

Under 2020 har Stratsys-modulen för internkontroll börjat införas i regionens verksamheter. Genom att nyttja Stratsys för att mäta och följa upp internkontrollpunkter för informationssäkerhet och dataskydd kan förbättringar göras mer strukturerat, vilket bidrar till att en högre säkerhetsnivå kan uppnås jämfört med tidigare. Informationssäkerhet som uppföljningsområde har ännu inte hunnit införas i Stratsys.

För kommande år 2021 finns en inriktning att förbättra internkontrollen, något som diskuterats vid ledningens genomgång hösten 2020. Detta avser regionledningens och linjechefernas uppföljning och rapportering av utvalda internkontrollpunkter inom informationssäkerhet och dataskydd.

2.3 Resultat från internrevisioner

Regionens internrevisorer genomför, på uppdrag av regiondirektören, internrevisioner av utpekade verksamheter i två revisionsomgångar (vår och höst). Kontrollpunkterna avseende informationssäkerhet i 2020 års internrevisionsplan omfattade dataskydd (skydd av personuppgifter) samt kontroll av om områdeschefer och enhetschefer följer upp att medarbetarna genomgår den obligatoriska e-utbildningen för medarbetare i informationssäkerhet (i lärplattformen Saba Cloud). I kontrollpunkterna ingick också en granskning av om linjecheferna känner till vad som ingår i deras eget utpekade ansvar som chefer rörande informationssäkerhet (enligt regelverk i ledningssystemet).

Resultaten visar generellt på mycket stora brister i medvetenhet och kunskap, särskilt från chefer och vad de behöver kunna i sin roll. E-utbildningen har endast genomgåtts av ca 40% av medarbetarna, något som ligger långt från målet på 80%. Detta behöver hanteras på ett betydligt tydligare sätt av ledning och cheferna men också av varje medarbetare.

2.4 Dataskydd – uppföljningar

För att dataskyddslagstiftningen ska kunna efterlevas krävs etablerade arbetssätt, skyddsåtgärder och en fungerande förvaltningsorganisation. Under 2020 rekryterades en dataskyddshandläggare och under 2020 har ett nytt verksamhetsstöd, DIGFrame, införts för registrering av personuppgiftsbehandlingar. Både Dataskyddsombud och dataskyddshandläggare är organisatoriskt placerade i Samordningskansliet.

Regionen har rutiner för rapporteringen av PU-incidenter till Integritetsskyddsmyndigheten (f.d. Datainspektionen), som är tillsynsmyndighet för dataskydd. Regionen är skyldig att rapportera inträffade incidenter inom 72 timmar. Under 2020 har 10 incidenter rapporterats av Region Jämtland Härjedalen i enlighet med dataskyddsförordningen. Den mänskliga faktorn visar sig vara grundorsaken till alla dessa 10 incidenter. Därför är det viktigt att ha regelbundna utbildningar där vi belyser och lyfter de incidenter som skett. Det är en del av det systematiska utvecklingsarbete som dataskyddsfunktionen bedriver.

Dataskyddsförordningen ställer krav på medvetenhet, att göra verksamheten medveten om regelverket och lyfta vilka risker som finns med behandling av personuppgifter. Dataskyddsarbetet har under 2020 bedrivits genom bland annat utbildningsinsatser av regionens nya verksamhetsstöd för behandling av personuppgifter. Det arbetet kommer att fortlöpa under hela år 2021. Regelbundna utbildningar har genomförts under året för regionens

registerkoordinatorer och nya utsedda registerkoordinatorer har fått specifik utbildning. Dessa tillfällen är viktiga för informationsutbyte, medvetenhet och samarbete kring dataskyddsarbetet i verksamheterna.

Ett omfattande arbete inom dataskydd under året har varit att se över regionens personuppgiftsbiträdesavtal och uppdatera kraven i enlighet med lagkrav. Regionen arbetar löpande med att få dessa avtal på plats. Ett annat prioriterat område inom dataskydd har varit att arbeta med rollen informationsägare och kopplingen till registerkoordinatorer.

3 Genomförda förbättringar

De förbättringar som genomförts under året redovisas inte i detalj utan sammanfattas kort nedan.

3.1 Ökad robusthet i fastighetssystem

Arbete har under året bedrivits för att höja säkerheten i styrsystem för fastighetsdrift och andra försörjningstjänster vilket brukar benämnas SCADA. En analys har genomförts under året och ett antal åtgärder har identifierats för att höja säkerheten. Det finns nu en handlingsplan för det fortsatta arbetet med att prioritera och genomföra dessa åtgärder, vilket kommer att påbörjas under 2021. SCADA-systemen är en mycket kritisk stödfunktion för hälso- och sjukvårdens drift.

3.2 Utökad sårbarhetsscanning av IT-miljön

Förmågan att upptäcka tekniska sårbarheter i IT-miljön har stärkts såväl som möjligheterna att kunna se och följa upp säkerhetskritiska händelser i IT-infrastrukturen.

3.3 Säkerheten i Office 365-tjänsterna

Regionen använder sedan ett par år tjänsterna i Microsoft Office 365 (nedan benämnd ’O365’) som centrala plattformar för informationshantering. Där ingår bland annat e-post, grupparbetsytor, dokumentlagring och distansmötestjänster. I syfte att vidareutveckla säkerheten i dessa tjänster har en översyn genomförts under året utifrån perspektivet att informationen i tjänsterna till stor del lagras i extern molntjänst med Microsoft som leverantör. Arbetet har också omfattat identifiering av nödvändiga hanteringsregler för O365-användningen. Det är högt prioriterat att tillämpa informationsklassning även i O365 och tydliggöra vilka uppgifter som får och kan hanteras i O365-tjänsterna. Personuppgifter behöver också ges ett adekvat skydd.

Analysen har givit förslag på kompletterande säkerhetsåtgärder som rekommenderas att införas utöver de åtgärder som redan vidtagits. Nationell praxis och lagtillämpning för molntjänsters användning är fortsatt en utmaning, inte minst då det gäller amerikanska molntjänster. Statliga utredningar på området väntas bli klara under 2021, något som kan bidra till tydligare regler för lagtillämpning och praxis. Tillsvidare finns ett antal föreslagna åtgärder som kan genomföras gällande O365 oavsett hur den framtida regleringen kommer att se ut.

3.4 Hantering av molntjänster

Molntjänster är den leveransform som alltmer tar överhanden för drift av IT-tjänster. Detta innebär att kunder i allt mindre grad kommer att ansvara för sin egen IT-drift i en lokal IT-miljö och istället använda ett IT-system som en tjänst via en extern leverantörs IT-driftmiljö ”i molnet” (extern driftmiljö). Det innebär stora skillnader i hur IT-verksamheten bedrivs men ställer också förändrade krav på hur avtal ingås med leverantörerna av de externa (moln-) tjänsterna. Regionen har under året genomfört ett antal workshops för att bygga upp kunskap om molntjänster, hur de kan användas samt vilka risker som finns med användningen. Arbetet kommer att ligga till grund för ett tydligare regelverk för hur molntjänster anskaffas och förvaltas inom regionen.

3.5 MIP informationsskydd i Office 365

Under året har ett uppdrag startats avseende pilotanvändning av informationsskyddet ”MIP” (Microsoft Information Protection) i Office 365. Detta skydd innebär att ett krypterings- och behörighetsskydd kan läggas på dokument, Teams-ytor samt e-post. Detta säkrar att endast behöriga läsare/mottagare har åtkomst till informationen i dessa dokument/Teams/e-post. HR-avdelningen kommer att inleda användningen för att bygga upp kunskap om hur skyddet kan används för att efterleva bland annat dataskyddslagstiftningen (GDPR).

3.6 Cyberhot: skydd mot phishing, skadlig kod mm

Med cyberhot menar vi här antagonistiska hot såsom intrång/angrepp, sabotage, utpressning via ransomware, bedrägeri, id-stöld och informationsläckage/stöld. Under året har förbättrade tekniska skydd införts för att öka förmågan att motstå phishingförsök, skadlig kod samt intrång i IT-miljön. Under året har phishing-hotet (skadliga länkar via e-post) ökat ytterligare från en redan hög nivå tidigare.

Detta hot är numera i högsta grad en fråga för organisationers ledningsgrupper, en dignitet denna fråga knappast hade för 4-5 år sedan. Möjliga konsekvenser av angrepp via phishing kan numera blir extremt långtgående och skadliga för organisationens information och de kostnader och merarbete som skador från dessa hot kan innebära.

3.7 Skydd mot obehörig åtkomst till patientuppgifter

Förbättringar har under året gjorts av loggkontrollen för åtkomst till patientuppgifter i vårdstödet COSMIC. Detta avser vidareutveckling av verktygsstödet LogPoint som analys- och uppföljningsstöd vid granskning av åtkomstloggar i COSMIC. En enklare och mer träffsäker granskning kan nu göras genom att hitta ”mönster” på obehörig åtkomst i loggarna.

Det tidigare använda vårdadministrativa systemet VAS övergick i ”läsläge” i samband med att systemet COSMIC infördes inom regionen 2015. VAS behöver fortsatt finnas kvar och vara tillgängligt för läsning av journalinformation och övrig historik för patienter även om nya journalanteckningar förs i COSMIC. Skyddet för informationen i VAS mot obehörigt intrång och informationsstöld har stärkts genom förbättrat logiskt skydd i nätverket.

En skiktad logisk modell för behörigheter i regionens nätverk har införts under året. Detta minskar också exponering för obehörig åtkomst via höga behörigheter hos administrativa konton som används av IT-driftpersonalen.

3.8 Samverkan i centralt informationsförvaltningsråd påbörjad

Regionen ser ett stort behov av att kunna förbättra sin informationsförvaltning. Detta innebär att kunna tillämpa tydligare regler för hur verksamhetens information ska hanteras (lagras, sökas, följas upp/analyseras och återanvändas). Insikten har under året fördjupats av att den information som används har ett mycket stort värde och att den, rätt använd, kan tillföra en mycket stor nytta för organisationen. Detta ställer krav på att informationen värderas som den tillgång det utgör och att den kan styras och skyddas på motsvarande sätt som andra tillgångar såsom ekonomiska tillgångar och personella tillgångar. Ett informationsförvaltningsråd (”IF-rådet”) har inrättats som en start på arbetet att identifiera och styra informationstillgångarna. Rådet ska bidra till att föreslå förbättringsarbete och underlätta att arbeten/uppdrag initieras och genomförs.

3.9 Tydliggörande av rollen informationsägare

Ett tydliggörande har under året gjorts i regionens styrande regelverk avseende rollen informationsägare. Mandatet för denna roll har förtydligats. Rollen har mandat att ställa krav på skyddet av informationstillgångar och besluta om tillhörande skyddsåtgärder. Införande av rollen innebär en tydlig markering från regionledningen av det värde i verksamheten som regionens informationstillgångar representerar och att de ska skyddas i likhet med andra viktiga skyddsvärda tillgångar såsom ekonomiska tillgångar, patienter och personal.

3.10 Informationsklassningar

Under året har arbetet med informationsklassningar fortsatt avseende informationen i regionens IT-system som stödjer samhällsviktiga tjänster. Arbetet innebär utmaningar eftersom tillgång till metodstöd krävs, något som i många fall inte kan tillgodoses med nuvarande resurser inom informationssäkerhetsfunktionen.

Inriktningen på arbetet har varit att underlätta att verksamhetens företrädare i allt högre grad själva ska kunna genomföra och dokumentera informationsklassningar för att bygga upp kunskap om informationen som verksamheten hanterar och hur den behöver skyddas.

3.11 Kontinuitetshantering – avbrottsplanering

Arbetet med avbrottsplanering för vårdverksamheterna gällande avbrott i kritiska IT-system för vården inleddes 2019 och har fortsatt under året men med lägre prioritet på grund av corona-pandemin. Avbrottsplaneringen för IT-system ingår nu i övergripande avbrottsplanering ihop med andra kritiska beroenden såsom el- och vattenförsörjning.

3.12 Förbättrat stöd för hantering av personuppgifter

Under året har ett förbättrat stöd för hantering och styrning av personuppgiftsbehandlingar införts inom regionen (DIGframe, en modul i Stratsys-plattformen). Detta stöd ska underlätta

efterlevnad av dataskyddslagstiftningen/ GDPR och minska riskerna att regionen genom brister i skyddet av personuppgifter drabbas av sanktionsavgifter och skadestånd.

3.13 Förbättrad central logghantering och analys

För att uppfylla spårbarhetskrav i Dataskyddsförordningen har Regionen under året driftsatt ett nytt system för central långtidslagring och analys av loggar. Systemet möjliggör för Regionen att uppnå nödvändig förmåga att upptäcka pågående intrång.

4 Prioriterad inriktning för fortsatt arbete

För kommande år finns följande prioriterade insatsområden för informationssäkerhet och dataskydd:

- Fortsatt arbete med hantering av NIS-direktivets krav och åtgärder med fokus på genomförande och uppföljning.
- Förbättrad behörighetshantering i regionens IT-system.
- Genomförande av åtgärder för höjd robusthet i nätverk, specifikt fastighetssystem.
- Fortsätta utveckla arbetssätt och stöd för informationsklassning.
- Stödja arbetet med att utse informationsägare i verksamheterna.
- Uppföljning av åtgärder/årshjul för dataskyddsarbetet.
- Framtagning av e-utbildning i informationssäkerhet för chefer och registerkoordinatorer (lokala samordnare för skydd av personuppgifter).