Informationssäkerhetsberättelse 2018

Beslutad 2019-03-26, av: Regionstyrelsen

REGION JÄMTLAND HÄRJEDALEN

Sammanfattning/bakgrund

Informationssäkerhet handlar om att säkra att rätt information finns hos rätt person i rätt tid och om att regionen har ett väl avvägt skydd för sin information. Detta är en viktig del i Regionens totala förmåga att kunna leverera rätt nivå på sina tjänster till medborgare och övriga intressenter. Informationssäkerhetsarbetet har under 2018 intensifierats och uppbyggnaden av ett strukturerat arbetssätt har fortsatt från föregående år. Dominerande delar under året har varit förberedelsearbete inför den nya Dataskyddsförordningen med svensk dataskyddslag (för utökat skydd av personuppgifter inom hela EU) som trädde i kraft maj 2018 samt framtagning av regelverk för användning av Office 365. Införandet av Office 365 i Region Jämtland Härjedalen har också inneburit en hel del arbete inom informationssäkerhet bl.a. med utarbetande av nya regelverk och tillämpningsanvisningar.

Ny lagstiftning som påverkar arbetet är t ex NIS-direktivet med tillhörande svensk lagstiftning (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) som trädde i kraft i november 2018. En ny reviderad säkerhetsskyddslag träder i kraft i april 2019 och vikten av informationssäkerhetsarbete kopplat till säkerhetsskydd och civilt försvar/totalförsvar ökar i omfattning. Utvecklingen har således gått mot en hårdare kravbild och ett ökat behov av tydligare kontroll avseende att det finns rätt åtgärder på plats för att skydda vår information. Behovet av ett systematiskt informationssäkerhetsarbete och riskbaserade granskning- och uppföljningsverktyg har aldrig varit större.

Samtidigt som Regionens informationssäkerhetsarbete har tagit stora och viktiga steg framåt de senaste åren så går utvecklingen inom IT-området oerhört snabbt och de tekniska möjligheterna ökar för all verksamhet inom Regionen. Verksamheterna idag har ett högt IT-beroende och därmed ökar också våra risker och sårbarheter. Det finns ett växande behov av att Regionen har förmåga att arbeta med systemförvaltning på ett strukturerat och kvalitetssäkrat sätt. Detta är en grundförutsättning för att kunna nyttja digitaliseringens fördelar inom en allt större del av verksamheten. Ett flertal riskanalyser har genomförts och ett antal säkerhetshöjande åtgärder har vidtagits under året. Arbetet har i stort kunnat genomföras enligt plan, men då resurserna inom informationssäkerhets- och Dataskyddsarbetet fortsatt är mycket begränsade går arbetet långsamt i förhållande till behoven. Handlingsplan för informationssäkerhet reviderades under hösten 2018 och en viss ambitionssänkning genomfördes med hänsyn till resursläget. Bedömningen är att regionens organisation för personuppgiftshantering som byggts upp under 2018 behöver ses över kommande år.

Informationssäkerhet ska enligt föreskriften HSLF-FS 2016:40, Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, vara en del av den årliga patientsäkerhetsberättelsen. I Region Jämtland Härjedalen finns därför, förutom denna informationssäkerhetsberättelse, en kortare sammanfattning avseende informationssäkerhet i patientsäkerhetsberättelsen.

INNEHÅLLSFÖRTECKNING

1 Informationssäkerhetsarbete 2018

Informationssäkerhetsarbetet har under 2018 intensifierats och uppbyggnaden av ett strukturerat arbetssätt har fortsatt från föregående år. Dominerande delar under året har varit förberedelsearbete inför den nya Dataskyddsförordningen med svensk dataskyddslag (för utökat skydd av personuppgifter inom hela EU) som trädde i kraft maj 2018 samt framtagning av regelverk för användning av Office 365. Införandet av Office 365 i Region Jämtland Härjedalen har också inneburit en hel del arbete inom informationssäkerhet bl.a. med utarbetande av nya regelverk och tillämpningsanvisningar.

NIS-direktivet med tillhörande svensk lagstiftning (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) trädde i kraft i november 2018. En ny reviderad säkerhetsskyddslag träder i kraft i april 2019 och vikten av informationssäkerhetsarbete kopplat till säkerhetsskydd och civilt försvar/totalförsvar ökar i omfattning. Kopplingen mellan informationssäkerhet och områdena säkerhetsskydd och totalförsvarsplanering har under 2018 blivit ännu mer konkret och viktig, inte minst med tanke på de avslöjanden som förmedlats i media kring allvarliga säkerhetsincidenter hos flera myndigheter.

Utvecklingen har således gått mot en hårdare kravbild och ett ökat behov av tydligare kontroll avseende att det finns rätt åtgärder på plats för att skydda vår information. Behovet av ett systematiskt informationssäkerhetsarbete och riskbaserade granskning- och uppföljningsverktyg har aldrig varit större. Samtidigt som Regionens informationssäkerhetsarbete har tagit viktiga steg framåt de senaste åren så går utvecklingen inom IT-området oerhört snabbt och de tekniska möjligheterna ökar för all verksamhet inom Regionen. Verksamheterna idag har ett högt IT-beroende och därmed ökar också våra risker och sårbarheter. Det finns ett växande behov av att Regionen har förmåga att arbeta med systemförvaltning på ett strukturerat och kvalitetssäkrat sätt. Detta är en grundförutsättning för att kunna nyttja digitaliseringens fördelar inom en allt större del av sina verksamheter.

MSB och SKL presenterade i oktober 2018 en nationell rapport som baserades på en enkät om läget (mognadsgraden) för informationssäkerheten hos Sveriges regioner och landsting. Rapporten ger vägledning om förbättringsinsatser och pekar ut 8 st rekommendationer (fokusområden) som kan och bör användas som indikatorer på mognadsgrad och förmåga. Bland dessa områden finns vikten av att använda informationsklassning som en huvudmetodik för att arbeta systematiskt med informationssäkerhet. Ett extra tydligt förbättringsområde är enligt rapporten att verka för tydligare kravställning av säkerhet för nya IT-tjänster/system, något som hos de flesta granskade regionerna är eftersatt.

Informationssäkerhet ska enligt föreskriften HSLF-FS 2016:40, Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, vara en del av den årliga patientsäkerhetsberättelsen. I Region Jämtland Härjedalen finns därför, förutom denna informationssäkerhetsberättelse, en kortare sammanfattning avseende informationssäkerhet i patientsäkerhetsberättelsen.

1.1 Ledningssystem för informationssäkerhet (LIS)

Ett kontinuerligt arbete krävs för att utveckla och hålla ledningssystemet aktuellt. Nya områden tillkommer i takt med att arbetssätt förändras och vidareutvecklas. Under 2018 har ett regelverk byggts upp för personuppgiftshantering. Införandet av Microsoft Office 365 (O365) med nya

lagringsytor och kommunikationskanaler gör att ytterligare regler och rutiner behövs för att styra informationshanteringen via de tjänster som ingår i O365.

1.2 Ledningens genomgång och långsiktig handlingsplan

Vid ledningens genomgång (2 gånger per år) är informationssäkerhet en av de delar som följs upp avseende ledningssystemets verkan. Vid varje tillfälle finns ett antal beslutspunkter för informationssäkerhet. Detta är en viktig del för att uppnå ständiga förbättringar i ledningssystemet. Denna genomgång med dess beslut om åtgärder tillsammans med den långsiktiga tvååriga handlingsplanen (den nu aktuella gäller 2018-19) för informationssäkerhet skapar ett planerings- och uppföljningsunderlag som underlättar arbetet med att förbättra säkerheten.

I fokus vid ledningens genomgång för informationssäkerhet finns dessa huvudområden:

1. Utbildning i informationssäkerhet
2. Genomföra informationsklassningar av kritiska IT-system
3. Hantera personuppgifter i enlighet med gällande lagstiftning
4. Kontinuitetsplanera verksamhetens informationsförsörjning
5. Arbeta med strukturerad förvaltningsstyrning

Område 2 (klassningar) är ett mycket viktigt område för att kunna klargöra säkerhetskrav, något som kommer till användning i många sammanhang, inte minst vid upphandling av nya IT-system och IT-tjänster. Klassningen kommer också att styra vilka hanteringsregler som behöver följas av Regionens medarbetare.

Område 5 (förvaltningsstyrning) är fortsatt eftersatt inom Regionen vilket skapar svårigheter när organisationen vill digitalisera sina arbetssätt i allt högre grad. Att utveckla och införa en modernare förvaltningsmodell än den nuvarande bedöms som en kritisk framgångsfaktor för digitaliseringsarbetet och för hanteringen av IT-systemen inom Regionen i stort.

Bland de beslut som tagits på ledningens genomgång (regionledningen) under året finns att etablera kontinuitetshantering gällande informationen i kritiska IT-system för ett antal vårdverksamheter samt att säkerställa en budget för informationssäkerhetsarbetet.

1.3 Personuppgiftshantering – Dataskyddsförordningen

Ny lagstiftning som påverkar informationssäkerhetsarbetet är framförallt den nämnda Dataskyddsförordningen (GDPR). Denna lagstiftning ställer utökade krav gällande att kunna uppvisa att man efterföljer dataskyddslagarna, däribland att regionen kan tillgodose den registrerades rättigheter och har förmåga och rutiner för att incidentrapportera om det inträffar överträdelser. Det kan utdömas sanktionsavgifter från tillsynsmyndigheten (Datainspektionen) om regionen inte uppfyller kraven, med viten upp till 20 milj SEK. Utöver detta kan registrerade personer ställa skadeståndsanspråk mot ansvarig part om regelverket överträds.

Ett omfattande arbetet har gjorts under 2017–18 inom regionen med att etablera fungerande arbetssätt och skyddsåtgärder som gör att dataskyddslagstiftningen kan efterlevas. Merparten av detta grundarbete har gjorts inom projektet ”Garbo” som avslutades vid halvårsskiftet 2018. Ett flertal styrdokument har tagits fram i ledningssystemet gällande dataskydd, däribland rutiner för registerutdrag, hantering av vårdens kvalitetsregister.

En förvaltningsorganisation för personuppgiftshantering har etablerats i enlighet med Regionstyrelsens beslut. Organisationen ska bestå av ett centralt Dataskyddsombud (DSO), tre biträdande dataskyddsombud samt ”registerkoordinatorer” (som utses inom varje verksamhetsområde). Rollen som registerkoordinator har varit en framgångsfaktor i arbetet och finns utsedda i de flesta verksamheter. Det finns ett utsett centralt Dataskyddsombud, men i nuläget endast ett biträdande dataskyddsombud. Organisation för personuppgiftshantering har byggts upp inom befintliga resurser, det har visat sig vara svårt att bemanna alla roller och organisationen haltar. Bedömningen är att behovet av stöd till verksamheterna gällande dataskydd är relativt stort och att det krävs mer resurser för att stödja och samordna dataskyddsarbetet. En översyn avseende dataskyddsorganisationen behöver därför göras 2019.

Under 2018 har arbete med konsekvensbedömningar enligt GDPR påbörjats (s.k. DPIA – Data Protection Impact Analysis). Dessa behöver enligt lagen genomföras för alla personuppgiftsbehandlingar (PU) som innehåller känsliga/extra skyddsvärda personuppgifter. En central registerförteckning över pågående PU-behandlingar har införts inom Regionen under 2017 och byggts på under 2018. I detta arbete har också ansvar och roller tydliggjorts där ”registerägare” och ”informationsägare” är primära roller med ansvar för de PU som Regionen behandlar.

Regionen har under 2018 byggt upp rutiner för rapporteringen av PU-incidenter till Datainspektionen, som är tillsynsmyndighet för dataskyddsområdet. Regionen är skyldig att rapportera inträffade incidenter inom 72 timmar. Tre incidenter har rapporterats under året i enlighet med lagkraven.

Ett omfattande arbete inom dataskyddsarbetet är att etablera biträdesavtal för de PU-behandlingar som utförs för Regionens räkning av externa parter. Dessa avtal baseras på lagkraven och ska reglera såväl hur PU får hanteras som vilka kommersiella villkor som gäller vid eventuella överträdelser mot gällande dataskyddslagstiftning. Regionen arbetar löpande med att få dessa avtal på plats. Ett prioriterat område inom dataskydd under 2018 har varit hantering av personuppgifter inom personaladministration (HR).

Löpande utbildning genomförs av Regionens registerkoordinatorer samt uppföljningar av dataskyddsarbetet i verksamheterna.

1.4 Mobila arbetssätt

Ett område som fortsatt under snabb utbyggnad är mobila arbetssätt där informationshanteringen via mobila enheter ställer stora krav på att säkerheten följer med i utvecklingstakten. Här finns stora utmaningar. Det är viktigt att grundläggande säkerhetsprinciper såsom informationsklassning och riskanalys används för att styra användning och hantering av de mobila enheterna. Potentiellt finns stora risker i denna mobila användning. Under kommande år (2019) krävs större insatser inom det mobila området med utveckling av alltifrån användarinstruktioner till införandet av tekniska regelverk.

1.5 IT-stöd för informationsklassning

Under 2018 har en utvärdering av IT-stöd för att utföra informationsklassningar gjorts inom arbetsgrupp för informationssäkerhet. Bland de IT-stöd som utvärderats finns ”DIGFrame” som är en tilläggsfunktion till ledningsstödet ”Stratsys” som anskaffats av Regionen i slutet av 2018.

”DIGFrame” är ett stöd för förvaltningsstyrning, informationssäkerhet och styrning av digitaliseringsinsatser. Detta stöd är kandidat till att anskaffas under 2019 för att vara ett verktyg för informationsklassning och riskanalyser – vilket ska ses som en viktig kravdel i förvaltningsstyrningen. Därmed kan behoven av ett integrerat stöd för strukturerad förvaltning av Regionens IT-system/-tjänster mötas.

1.6 Andelen molntjänster växer stadigt

En allt större andel av de IT-system som används är molnbaserade och finns därmed utanför Regionens lokala IT-infrastruktur. Detta ger nya förutsättningar för Regionen, som stegvis ställer om för att i högre grad kunna arbeta med externa molnlösningar förutom hanteringen av den lokala IT-miljön som ägs av Regionen själv. Ett ökat fokus behöver därför riktas mot förvaltningsstyrning med tydlig kravställning och uppföljning mot såväl intern IT-hantering som mot externa molntjänster. Ett behov finns av att öka resurserna för Regionens införandestöd för nya IT-lösningar samt för det löpande arbetet med förvaltning och vidareutveckling av befintliga IT-lösningar.

1.7 Förstudie behörighetshantering

Ett eftersatt och prioriterat område inom Regionens IT-användning är förbättrad behörighetshantering. Ett flertal lagkrav, däribland Patientdatalagen, Socialstyrelsens föreskrifter HSLF-FS 2016:40 samt GDPR med den tillhörande nya svenska dataskyddslagen, anger att behörigheter ska styras och följas upp på ett strukturerat sätt så att åtkomst till skyddsvärda uppgifter kan minimeras.

Under 2018 påbörjades en förstudie för att utreda hur en förbättrad behörighetshantering ska kunna införas. Förstudien ska vara klar våren 2019 och har så här långt pekat ut att beställningar och godkännande av behörigheter i IT-systemen behöver centraliseras i högre grad via en gemensam beställningskanal för flertalet system. Dessutom behöver tilldelning och borttag av behörigheter automatiseras i så hög grad som möjligt.

1.8 Loggkontroller för vårdadministrativa system

Regionen har under 2018 samverkat inom området loggkontroll för vårdadministrativa system med några andra regioner. Dessa regioner använder också COSMIC-systemet och den valda loggplattformen för att lagra och analysera logginformationen. Syftet med detta är att etablera gemensamma arbetssätt och verktyg för att utföra loggkontroller där åtkomster till patientinformation följs upp mot gällande regelverk.

Under 2018 har det verktyg, ”LogPoint”, som används som plattform för loggkontroller, kravställts för att kunna införa en ny, förbättrad version av verkyget under 2019. Loggkontrollerna ska kunna förebygga obehörig åtkomst till patientuppgifter som lyder under hälso- och sjukvårdssekretessen. Kontrollerna består av såväl löpande stickprovskontroller som riktade kontroller vid misstanke om obehörig åtkomst.

Under 2018 har också en lösning utvecklats inom Regionen för att patienten själv ska kunna läsa loggarna för sin vårdinformation i COSMIC via den nationella Journal via Nätet-tjänsten/ 1177. Detta alternativ där patienten själv ges tillgång till logginformationen via direktåtkomst blir alltså ytterligare en granskningstyp för loggarna. Sedan tidigare har patienten vid behov fått begära ut loggutdrag på pappersutskrifter från Regionen, något som även fortsatt blir möjligt.

Loggkontroller genomförs löpande i vårdens verksamheter och uppföljning avseende att kontroller genomförs sker vid internrevisionen.

2 Riskanalyser och egenkontroll

2.1 Internrevision avseende informationssäkerhetsarbetet

Under året har två omgångar med internrevisioner med revisionspunkter för informationssäkerhet genomförts. Denna revision har skett hos utvalda verksamheter enligt löpande treårig revisionsplan.

2.2 Övergripande riskanalys avseende informationssäkerhet

Under 2017 gjordes en övergripande riskanalys avseende informationssäkerhet. Under 2018 har den uppdaterats. Analysen beaktar två områden; 1. De största riskerna i det systematiska arbetssättet för informationssäkerhet samt 2. De mest framträdande specifika operativa riskerna för Regionens informationshantering.

De två huvudsakliga riskerna som identifierats är:

1. Kritiska IT-system har inte informationsklassats (säkerhetanalyserats) och åtgärdsplanerats vilket medför ohanterade sårbarheter som riskerar stora störningar hos kritiska verksamheter – kan ge obehöriga åtkomst till känslig information och hindra åtkomst till IT-systemen
2. Dataintrång sker genom bristande säkert i behörighet/inloggning/kryptering – detta kan medföra spridning av känsliga uppgifter till obehöriga

2.3 Övriga riskanalyser och egenkontroll

Övriga riskanalyser som har genomförts under året är:

- Riskanalys för hantering av känsliga personuppgifter i Regionens beslutsstöd (datalager).
- Riskanalys för lagring av information i gemensam molntjänst Office 365.
- Riskanalys för läkemedelsbeställningar i Raindance beställningsportal.
- Riskanalys för hantering av central konfigurationsdatabas (CMDB).
- Riskanalys för IT-säkerhetsrisker i Office 365.
- LINK Samordnad vårdplanering region och kommun. Kundgemensam risk- och konsekvensanalys (RoK) kopplad till projektet, kommunerna har gjort RoK per kommun (blandning av projekt- och patientsäkerhetsperspektiv). Facklig RoK är gjord med risker för arbetsmiljö.
- NOVA Ward - RoK är gjord för projektet dock inte i avseende patientsäkerhet utan risker för hela projektet. Ett flertal frågeställningar kring informationssäkerhet hanterades i projektet utan att det gjordes en specifik RoK.
- eBesök - RoK gjord för projektet och det finns en RoK gjord för BUV Barn och unga vuxna (där ingår patient- och informationssäkerhetsaspekter).

- Ny rutin för smittspårning införd - script som körs i Cosmic för att fånga aktuella patienter - RoK utifrån nuläge och önskat läge och tar upp risker inom områdena patient- och informationssäkerhet.
- WebCert till Nationell Intygstjänst för läkarintyg - infördes under våren 2018. RoK gjordes gemensamt i kundgrupp Cosmic (främst för projektet, risk lyftes kring att signering måste göras via SITHS-kort).

Under 2018 har ett viktigt fokus gällande riskanalyser inom informationssäkerhet funnits på riskanalyser/konsekvensbedömningar vid behandlingar av känsliga/extra skyddsvärda personuppgifter. Detta område berör de övergripande GDPR-kraven på dataskydd.

2.4 Viktigare utvärderingar av säkerheten under 2018

Följande mer övergripande utvärderingar av säkerheten har genomförts under året:

- Utvärdering gällande efterlevnaden av rutin för säkerhetsuppdateringar genomförd.

- Utvärdering av brister och sårbarheter i system som exponeras mot Internet samt intern IT-infrastruktur genomförd.

2.5 Internkontroll för informationssäkerhet

Internkontrollen (riskbaserad), där egenkontrollen i respektive verksamhet är en del, är tillsammans med avvikelsehanteringen ”motorn” i förbättringsarbetet inom såväl informationssäkerheten som annan kvalitetsutveckling.

Förbättringar som initieras från dessa delar behöver effektueras i förbättringsuppdrag och projekt för att ”förbättringshjulet” ska rulla framåt. Fortsatt är internkontrollen avseende informationssäkerhet ett eftersatt område som inte fått tillräckligt fokus. En förklaring till detta är att det under de senaste 2–3 åren varit fokus på att etablera regelverk och övriga styrande dokument för att få till en grund för ett ledningssystem för informationssäkerhet. Ett naturligt kommande steg blir då att öka fokus på uppföljningsdelar i form av internkontroll och aktiv upptäckt av incidenter via avvikelserapportering och uppföljning.

2.6 Avvikelser och incidenter

Under 2018 har ett minskat antal avvikelser (jämfört med föregående år) rapporterats. Det finns stora brister i Regionens avvikelsesystem som gör att det är svårt att följa upp kvalitetssäkrad statistik. Det är också troligt att det finns en underrapportering och okunskap avseende avvikelser inom informationssäkerhet.

Under 2018 har 3 st incidenter gällande personuppgifter rapporterats till Datainspektionen enligt gällande dataskyddslagstiftning.

Under 2018 har sex polisanmälningar gjorts avseende dataintrång, d.v.s. fall där misstänkt dataintrång med obehörig läsning av patientjournal har rapporterats.

Under året har några oplanerade avbrott skett i Citrix och Cosmic, men inget har varat någon längre tid och eller gett några allvarliga konsekvenser för patientsäkerheten.

2.7 IT-säkerhet

Sårbarhetsscanning
Under 2018 har verktyg för sårbarhetsskanning och analys utvärderats och införskaffats. Breddinförande pågår och vi ser redan positiv effekt av investeringen baserat på att flertalet kritiska sårbarheter har kunnat identifierats och åtgärdats i både interna system såväl som system som exponeras mot Internet. Schemalagda sårbarhetsskanningar är upprättade.

Riskanalys för IT-säkerhetsrisker i Office 365
Riskanalys har genomförts tillsammans med externa säkerhetsexperter gällande den exponering för IT-säkerhetsrisker som Office 365 medför.

Egenkontroll av intern infrastruktur och IT-system
Stickprovskontroller utförs för att hitta eventuella säkerhetsbrister. Brister har identifierats och hanterats i bland annat Active Directory, Citrix-plattform och filservrar.

Egenkontroll av loggar i Office 365
Genomgångar av relevanta loggar i Office 365 samt konfigurationsmässigt hur Regionens Office 365 konfiguration står sig mot Microsofts säkerhetshöjande rekommendationer. Regionen når upp till en poäng av 257 där riktvärdet för en balanserad säkerhetsnivå är på 592 poäng. Jämfört med både organisationer inom samma bransch och organisationer i samma storlek håller Region Jämtland Härjedalen två till tre gånger högre nivå konfigurationsmässigt enligt Microsofts sammanställningar. Många kvarvarande rekommenderade säkerhetshöjande åtgärder har Regionen inte tillgång till då de ligger i dyrare licensformer.

Egenkontroll av infrastrukturella loggar
Central hantering av loggar möjliggör analys av loggar och trender för att identifiera allt från intrångsförsök till prestandarelaterade problem. Stickprov görs men i planen för 2019 ligger maskinell analys och larmsättning.

3 Genomförda förbättringar

Sammanfattningsvis har dessa huvudsakliga förbättringar genomförts under året:

- Utvärdering av AIP-skydd (Information Protection) för skydd/kryptering av dokument och e-post.
- Utvärdering och anskaffning av verktygsstöd för informationsklassning, riskanalyser samt systemförvaltning.
- Anskaffning och införande av verktyg för sårbarhetsscanning av både interna system och system som exponeras mot Internet.
- Införande av förbättrad kontroll av konton med höga behörigheter.
- Införande av förbättrad åtkomstlösning för extern åtkomst till lokal IT-miljö.
- Anskaffning och införande av funktion för centraliserad logginsamling och logganalys.
- Förbättring av verktyg för granskning av loggar från vårdinformationssystem.
- Införande av GDPR-anpassade personuppgiftsbiträdesavtal som täcker gällande dataskyddskrav.
- Förbättrad säkerhetskonfiguration i Citrix.

- Genomförd nätverkssegmentering av flera system, bland annat Citrix och vårdsystemet COSMIC.
- Krav på och införande av flerfaktorsautentisering för inloggning till Office 365.

Nedan beskrivs ytterligare några specifika områden där förbättringar genomförts.

3.1 E-utbildning för informationssäkerhet

En informationssäkerhetsutbildning för samtliga Regionens medarbetare (i Saba Cloud e-utbildningsplattform) har tagits fram under 2018. Utbildningen planerades först att införas under början på 2018. Eftersom dataskyddsförordningen trädde i kraft under 2018 beslutades dock att skjuta på införandet av utbildningen för att kunna få med de delar som rör denna nya lagstiftning eftersom den berör samtliga medarbetare. Utbildningen införs istället i början på 2019. Ett mål har satts om att 50% av Regionens medarbetare ska genomgå utbildningen under 2019.

3.2 Office 365-plattformens tjänster

Under året har Office 365 införts som grundplattform för Regionens kommunikations-, dokumentations- och samverkanstjänster. Införandet av dessa tjänster har i högsta grad påverkat Regionens informationssäkerhet. Det finns ett stort behov av att etablera fungerande och säkra arbetssätt i denna plattform som erbjuder mycket stora möjligheter att skapa, bearbeta och dela information. Inte minst krävs att informationen som hanteras i dessa tjänster kan informationsklassas för att kunna hanteras på rätt sätt och därmed få ett skydd som uppfyller ställda krav.

3.3 COSMIC

Under året har införandet av uppföljnings- och analysfunktionen ’COSMIC Insight’ påbörjats. Denna funktion ska användas för bland annat kvalitetsuppföljningar i vårdverksamheterna men även för viss produktionsuppföljning. För att klara att uppfylla kraven på dataskydd mm för patientrelaterade uppgifter som hanteras i funktionen behöver ett regelverk för behörighetsstyrning för Insight etableras under 2019.

Under 2018 har också funktionen ’COSMIC Nova Tablet’ införts i några vårdverksamheter. Detta är en lösning med mobila enheter/läsplattor som används av sjuksköterskor. Det pågår ett arbete med att få denna hantering informationssäker. Bland annat har säkrats att informationen på den mobila enheten där Nova Tablet används endast kan nås via en säker inloggning som baseras på användarens SITHS-kort.

3.1 IT-säkerhet

Sårbarhetsscanning
Under 2018 har verktyg för sårbarhetsskanning och analys utvärderats och införskaffats. Breddinförande pågår och redan inledningsvis ser vi positiva effekt av investeringen baserat på att flertalet kritiska sårbarheter har kunnat identifierats och åtgärdats i både interna system såväl som system som exponeras mot Internet. Schemalagda sårbarhetsskanningar har upprättats där samtliga system som exponeras mot Internet skannas varje dygn medan interna system skannas på veckobasis.

Hantering av höga behörigheter – nedlåsning och eskalerad behörighet
Den gallring av tjänstekonton och administratörskonton med för höga behörigheter i Region Jämtland Härjedalens domän som påbörjades under 2017 har under 2018 givit effekt, framför allt gällande tjänstekonton. Antalen har gått från:

- Tjänstekonton med hög behörighet 36 st (2017) till 3 st (2018)
- Administratörskonton med hög behörighet 153 st (2017) till 26 st (2018)

Att minska antalet höga behörigheter innebär att regionen minskar sin riskexponering avsevärt för både obehörigt intrång och angrepp av skadlig kod. Under 2019 är målsättningen att antalet administratörs- och tjänstekonton med hög behörighet skall minska med minst 60%.

Förbättringar i AD-struktur
Koncept som påbörjades 2017 för att säkerställa kontroll över hanteringen av höga behörigheter men som också minskar risken för att konton med höga behörigheter skall kunna nyttjas av angripare i Regionens IT-infrastruktur. Etableringsfas pågår där system börjar lyftas in i den uppsatta strukturen.

Säkrare serverkonfiguration
En säkrare serverkonfiguration har tagits fram utifrån internationella rekommendationer. Konfigurationen har under 2018 börjat användas i nya Citrix, Datalagrets nya servrar samt under året uppsatta servrar som är nåbara från Internet.

Segmentering av nät
Arbetet med nätverkssegmentering har fortgått under året med flertalet segmenterade system. Däribland Cosmic, Datalagret, Sonic, T4, Citrix.

Loggverktyg
För efterlevnad av bland annat Dataskyddsförordningen har spårbarhet och möjligheten att upptäcka intrång förbättrats genom att samla in och analysera relevanta infrastrukturella systemloggar från samtliga servrar och klienter. Regionen samlar idag in i snitt 180 GB loggdata per dygn vilket motsvarar ca 73 728 000 skriva A4-sidor/dygn.

3.2 Informationssäkerhetsrådet

Informationssäkerhetsrådet är ett nytt forum som startade 2018. Detta forum har haft fyra möten under året med företrädare för Cosmic, e-hälsotjänster, IT-säkerhet, informationssäkerhet, patientsäkerhet och dataskydd samt administrativa system. Rådets syfte är att;

- Skapa transparens i arbetet mellan olika funktionsområden och undvika stuprör
- Bidra till processorienterat arbetssätt
- Bidra till att göra ”rätt från början” och därmed effektivisera arbete
- Fokusera på säkerhetsaspekter
- Är inte ett ”arbetsmöte”, men ska bidra till att identifiera behov och former för gemensamt arbete
- Vara sakkunnigstöd inom verksamheter som är beroende av informationssäkerhet respektive relaterar till området.

Rådets arbete och samverkansformer fortsätter under 2019.

4 Prioriterade åtgärder för 2019

Följande prioriterade åtgärdsområden finns med i den övergripande handlingsplanen för informationssäkerhet 2018-19, i stabsarbetsplan för informationssäkerhetsfunktionen samt i förvaltningsplanen för IT-säkerhet (utan inbördes prioritet);

- Tillhandahålla utbildning och stöd i informationssäkerhet för medarbetare samt riktad utbildning till roller såsom chefer och systemförvaltningsansvariga roller
- Etablera systematisk kontinuitetshantering för verksamhetskritiska informationssystem i utpekade vårdverksamheter
- Införa skyddsfunktioner för att kunna överföra och lagra känsliga uppgifter på ett säkert sätt såväl internt som till externa parter (exempelvis skyddsvärda personaluppgifter och avvikelseärenden med patientinformation samt andra typer av meddelanden som hittills har gått via fax)
- Etablera en ändamålsenlig internkontroll med ett riskbaserat arbetssätt för informationssäkerhet (generellt)
- Tydliggöra och kravställa säkerhetsrelaterade uppgifter i arbetssätt och rutiner för Regionens systemförvaltning
- Vidareutveckla arbetssättet för informationsklassning med verktygsstöd via ’DIGFrame’
- Slutföra förstudie om förbättrad behörighetshantering
- Revidera Regionens informationssäkerhetspolicy
- Fortsatt införande av koncept för hantering av administrativa behörigheter
- Fortsatt införande av system för sårbarhetsskanningar och logganalys
- Utveckla användning och nytta av insamlade infrastrukturella loggar
- Etablera vitlistningsskydd i Citrix motsvarande det vi har i eKlient
- Riskanlays gällande de risker som Regionen exponeras för från leverantörer
- Analys gällande hur Regionen svarar upp mot IT-säkerhetskrav i NIS-direktivet