Region Örebro län

Rapport
Datum: 2024–03–21
Författare: Anneli Björkholm

Årsrapport informationssäkerhet 2023

Version 1

Version: 1

Årsrapport informationssäkerhet 2023

Version 1

Anneli Björkholm och Sofia Öhrman

2024-03-21

Innehåll

1. Sammanfattning 5
2. Bakgrund 6
   2.1 Informationssäkerhetspolicy 7
3. Informationssäkerhetsarbetet i regionen 8
   3.1 Bemanning och organisation 8
   3.2 Informationssäkerhetsarbetet under 2023 8
   3.3 Dataskydd 9
   3.3.1 Överföring av personuppgifter till tredjeland 9
   3.4 Microsoft Office 365 10
   3.5 Nytt Vårdinformationsstöd, Cosmic 11
   3.6 Externa och interna samarbeten 11
   3.6.1 Informationssäkerhetsgruppen i Sjukvårdsregion Mellansverige 11
   3.6.2 Hälso- och sjukvårdens informationssäkerhetsnätverk, HoSiS 12
   3.6.3 Regionservice IT-SIRT 12
   3.6.4 Regionservice IT-Säkerhetsgruppen 12
   3.6.5 Regionövergripande kunskapsutbyte inom it- och cybersäkerhet 12
   3.6.6 Övriga samarbeten 13
4. Granskningar och skyddsåtgärder 13
   4.1 Informationsklassning och riskanalys 13
   4.2 Granskningar 13
   4.3 Skyddsåtgärder 13
   4.3.1 Loggning och logguppföljning 13
5. Uppföljningar 14
   5.1 Uppföljning av informationssäkerhetsarbetet i regionen Intern styrning och kontroll (ISK) 14
   5.2 MSB:s Infosäkkoll– i syfte att mäta kunskap och informationssäkerhetskultur i regionen 16
6. Förbättringsåtgärder 18

6.1 Genomförda aktiviteter 2023 18
6.1.1 Hälso- och sjukvårdsförvaltningen 18
6.1.2 Folktandvården 18
6.1.3 Regionalutveckling 19
6.1.4 Företagshälsa och Tolkförmedling 19
6.1.5 Regionkansliet Staben Digitalisering 20
6.1.6 Regionkansliet Staben Administration juridik och säkerhet 20
6.1.7 Regionservice Stab 21
6.1.8 Regionservice IT 21
6.1.9 Regionservice MedicinskTeknik 21
6.1.10 Regionservice Avdelning Upphandling 22
6.1.11 Regionservice Regionarkiv och registratur 22
6.1.12 Regionservice Shared Service Center 22
6.1.13 Regionservice Område Fastigheter 23
6.1.14 Genomförda förbättringar kopplat till IT 23
6.2 Rapporterade planerade aktiviteter för 2024 23
6.2.1 Teknisk säkerhet 23
6.2.2 Administrativ säkerhet 24
6.3 Ett verktyg för informationsklassning och riskanalys ..24
6.4 Utbildningsinsatser 25
7. Incidenter/avvikelser 25
7.1 IT incidenter, ransomware och phising mm 25
7.1.1 Granskade och stoppade intrång via internet 25
7.1.2 E-post filter 27
7.2 Världsomfattande hotbild 29
7.3 Driftavbrott it-system 29
8. Fokusområden 2024 30
8.1 Det systematiska informationssäkerhetsarbetet 30
8.2 NIS-direktivet och NIS- lagstiftningen 31
8.3 Lämplighetsbedömning vid utkontraktering av it-drift..31
8.4 Nytt vårdinformationsstöd, Cosmic 32
8.5 Upphandling och kravställning 32

1. Sammanfattning

Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt. Information är en av Region Örebro läns (nedan regionen) viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt en förutsättning för en säker och bra digitalisering. Dataskydd, cybersäkerhet och IT-säkerhet är del av informationssäkerheten. Det handlar om att skydda information men utifrån olika perspektiv.

Regionen ska bedriva ett systematiskt informationssäkerhetsarbete. Det systematiska arbetet med informationssäkerhet och utveckling av regionens säkerhetskultur blir allt viktigare då alltmer information finns tillgänglig digitalt och hanteras/behandlas av olika leverantörer. Detta medför också risker, genom it-attacker kan information göras otillgänglig eller gå förlorad. Riskerna måste därför fångas upp och hanteras, rätt säkerhetskrav måste ställas på leverantörer i rätt tid.

Samhället står inför nya utmaningar i takt med att vår omvärld ständigt förändras. Efter att kriget i Ukraina inleddes har det världspolitiska säkerhetsläget snabbt förändrats. En del av kriget, som pågår genom riktade it-attacker, så kallat cyberkrigs-föring, inom Europa har medfört att även hotläget har ökat inom hela Europa. Det pågående cyberkriget som nu sker resulterar i en ökad mängd cyberattacker för att skada myndigheter samt andra offentliga verksamheter, där vissa aktörer inriktar sig specifikt på hälso- och sjukvård.

I detta nya läge blir informationssäkerhetsarbetet inklusive säkerhetskulturen ännu viktigare samtidigt som ny lagstiftning kommer att ställa ännu högre krav på det systematiska informationssäkerhetsarbetet.

Informationsklassningar och riskanalyser behöver ske i verksamheter som hanterar information. Det är grunden i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som ska finnas i alla regioner och kommuner. Således är det här ett ständigt återkommande arbete för regionen såsom för alla andra organisationer som hanterar information.

De uppföljningar som skett av informationssäkerhetsarbetet och säkerhetskultur i regionen visar på ett fortsatt behov av att öka kunskapen kring informationssäkerhet i

stort, i synnerhet kunskapen om ansvar och roller, vem som är informationsägare och vad det innebär att vara informationsägare etcetera. Områdena uppföljning och utvärdering, upphandling och utveckling av säkerhetskultur är viktiga områden som fortsatt behöver utvecklas.

Uppföljningarna visar vidare att informationsklassningar och riskanalyser till viss del genomförs i organisationen. För att förbättra arbetet i regionen behöver kunskapen stärkas. Vidare finns det ett kvarstående behov av att förbättra verktyget för informationsklassning och riskanalys.

2. Bakgrund

Information är en av regionens viktigaste tillgångar. Det är även en förutsättning för en säker och effektiv verksamhet samt för digitaliseringen. Informationssäkerhet handlar om att skydda information på ett säkert sätt. Det gäller all slags information oavsett var den finns lagrad, exempelvis på papper, digitalt eller muntligt.

Regionen ska utöva ett systematiskt informationssäkerhetsarbete med stöd av den svenska och internationella standarden ISO 27000 för informationssäkerhet och cybersäkerhet samt dataskydd.

Ledningssystem för informationssäkerhet (LIS) ska i tillämpliga delar baseras på SS-ISO/IEC 27001:2022 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet, innefattande att samtliga säkerhetskritiska administrativa och tekniska processer ska vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

I det systematiska informationssäkerhetsarbetet ska hot, sårbarheter och risker identifieras samt säkerhetsåtgärder införas som reducerar dessa till en för regionen acceptabel nivå med hänsyn till konfidentialitet, riktighet och tillgänglighet. Medborgarna ska kunna lita på den information regionen hanterar och att den skyddas på ett bra vis.

Ett systematiskt informationssäkerhetsarbete innebär att strukturerat planera, avsätta resurser, fatta medvetna beslut för att skydda rätt information på rätt sätt. Det systematiska informationssäkerhetsarbetet ska bedrivas för att stärka förmågan att undvika negativa händelser som påverkar regionens verksamheter. Inträffar en negativ händelse ska denna kunna hanteras på en godtagbar nivå med bibehållet förtroende från regionens intressenter.

Bedrivs inte informationssäkerhetsarbetet enligt de lagkrav som ställs kan det innebära konsekvenser som att informationssäkerhetsarbetet inte kan bedrivas med den kvalitet som förväntas vilket kan resultera i att regionens informationstillgångar inte hanteras på ett korrekt sätt. Detta kan vidare leda till sanktionsavgifter.

Ledningens genomgång är en viktig del enligt standarden för informationssäkerhet (SS-ISO/IEC 270001:2022) och ett krav enligt Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter inom hälso- och sjukvården (HSLF-FS 2016:40). Syftet med genomgången är att tillsammans med ledningen gå igenom och se över det systematiska informationssäkerhetsarbetet och dess styrning. Årsrapporten för informationssäkerhet är en del av denna genomgång för att säkerställa informationssäkerhetsarbetet och styrningens fortsatta lämplighet, tillräcklighet och verkan.

Denna rapport är framtagen av enheten för juridik och informationssäkerhet. Informationssäkerhetssamordnaren har samlat in material och information genom Myndigheten för samhällsskydd och beredskaps (MSB) verktyg Infosäkkollen samt genom representanter från alla regionens förvaltningar. Utifrån detta har rapporten sammanställts av informationssäkerhetsamordnaren och enhetschef för juridik och informationssäkerhet. Avsnitt 7.1.1 och 7.1.2 har skrivits av medarbetare på Regionservice IT.

2.1 Informationssäkerhetspolicy

Regionen ska utöva ett systematiskt informationssäkerhetsarbete med stöd av den svenska och internationella standarden ISO 27000 för informationssäkerhet och cybersäkerhet samt dataskydd. Ledningssystem för informationssäkerhet (LIS) ska i tillämpliga delar baseras på SS-ISO/IEC 27001:2022 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet, innefattande att samtliga säkerhetskritiska administrativa och tekniska processer ska vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

Enligt Socialstyrelsens föreskrifter HSLF-FS 2016:40 ska varje vårdgivares ledningssystem innehålla en informationssäkerhetspolicy. I informations-säkerhetspolicyn beskrivs regionens mål och principer för informationssäkerhet för alla verksamheter. Policyn ska bidra till ett professionellt förhållningssätt där informationssäkerhetsaspekter ska vägas in i beslut som rör hantering av information. Policyn omfattar all information oavsett i vilken form den lagras eller hanteras. Nuvarande informationssäkerhetspolicy fastställdes år 2015 och har uppdaterats två gånger, senast under år 2022. Syftet med uppdateringen var att förtydliga roller och ansvar samt förbättra informationssäkerhetsarbetet.

3. Informationssäkerhetsarbetet i regionen

3.1 Bemanning och organisation

Informationssäkerhetsarbetet i regionen utgår från Enheten för juridik och informationssäkerhet. Där är även informationssäkerhetssamordnaren samt dataskyddsombudet placerade.

Informationssäkerhetssamordnaren arbetar strategiskt med informationssäkerhet. Detta genom att exempelvis säkerställa att styrande och stödjande dokument finns på plats, genomföra utbildningar och informationsinsatser, ge råd och stöd. Arbetet är även av operativ karaktär. Dataskyddsombudets roll är till stor del reglerad genom EU:s dataskyddsförordning, GDPR. Exempelvis ska dataskyddsombudet ge råd och stöd, erbjuda utbildningar men även genomföra tillsyn samt anmäla brister i verksamheterna till Integritetsskyddsmyndigheten, IMY. Enhetschefen för juridik och informationssäkerhet arbetar till övervägande del med informationssäkerhet- och dataskyddsfrågor tillsammans med informationssäkerhetssamordnaren och dataskyddsombudet.

Regionen har ett informationssäkerhetsråd med representanter från samtliga förvaltningar. Informationssäkerhetsrådets uppdrag är att stödja och utveckla regionens systematiska informationssäkerhetsarbete på en övergripande nivå. Rådet och rådets medlemmar utgör en kanal för informationssäkerhetsfrågor mellan Regionkansliet och övriga förvaltningar inom regionen. Rådet rapporterar till regionens ledningsgrupp. Informationssäkerhetsrådet har fyra planerade möten per år. Vid behov kan fler möten hållas. Rådet är vidare en remissinstans för exempelvis styrande dokument.

Rådet består av följande medlemmar: enhetschef för juridik och informationssäkerhet (ordförande), informationssäkerhetssamordnare, dataskyddsombud, chef säkerhets- och beredskapsenheten, representant från staben digitalisering, it-säkerhetsansvarig, it-chef, representant från upphandling samt Medicinsk Teknik, förvaltningsövergripande chefläkare, beredskapsläkare samt en representant från övriga regionens förvaltningar.

3.2 Informationssäkerhetsarbetet under 2023

Regionens informationssäkerhetsarbete ska bedrivas systematiskt och riskbaserat. För att hitta rätt nivå av skydd för den information som regionen hanterar är det viktigt att utgå från värdet av informationen och de risker som finns. Det ska göras genom informationsklassning och riskanalys av regionens informationstillgångar. Att regelbundet följa upp informationsklassningar och riskanalyser är av största vikt då regionen måste anpassa sig till en ständigt förändrad och alltmer komplex hotbild.

All information ska ha en identifierad ägare. Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvar som informationsägare följer det delegerade verksamhetsansvaret. I de fall där det finns ett flertal informationsägare likställs rollen objektägare med informationsägare enligt regionens förvaltningsmodell för it-stöd.

Under år 2023 har it-attackerna fortsatt varit på en hög nivå mot myndigheter och företag både i Sverige och i andra länder. MSB tillhandahåller löpande information och omvärldsbevakning inom it-säkerhetsområdet som regionen tar del av.

Det finns ett behov av att öka kunskapen kring informationssäkerhet i stort, i synnerhet kunskapen om ansvar, vem som är informationsägare och vad innebär det att vara informationsägare. Informationsklassningar och riskanalyser genomförs till viss del i organisationen med varierande kvalité. Det finns fortsatt ett stort behov av att öka kunskapen i verksamheterna om hur informationsklassningar och riskanalyser sker. Fler personer i verksamheterna behöver utbildas för att kunna genomföra både klassningar och riskanalyser av regionens informationstillgångar.

Under 2023 har enheten för juridik och informationssäkerhet erbjudit flera informationstillfällen och utbildningsinsatser för olika grupperingar i syfte att öka kunskapen. Styrande och stödjande dokument tillkommer och uppdateras regelbundet för att höja kunskapen. Det är dock av stor vikt att fortsätta öka medvetenheten och höja kunskapsnivån generellt. Digitaliseringen går fortsatt väldigt snabbt och här måste informationssäkerheten fångas in i ett tidigt skede.

3.3 Dataskydd

Dataskydd utgör en del av informationssäkerheten. Det är exempelvis genom klassningar och riskanalyser kravställning på dataskydd och säkerhetsåtgärder kan ske. Informationssäkerhet och dataskydd hänger således nära ihop.

Arbetet med att säkerställa att regionens personuppgifter hanteras utifrån GDPR är ett ständigt pågående arbete. För att säkerställa att riktlinjer och rutiner följs kan interna kontroller, utifrån en tillsynsplan, ske årligen av regionens dataskyddsombud. Även oplanerade granskningar kan komma att ske, utifrån händelser i omvärlden eller inom regionen.

3.3.1 Överföring av personuppgifter till tredjeland

En stor del av dataskyddsarbetet handlar om överföring av personuppgifter till tredjeland (det vill säga länder utan för EU/EES). Detta mot bakgrund av den så kallade Schrems II domen som meddelades i juni 2020 av EU domstolen. I domen

underkände EU domstolen överföringsmekanismen Privacy Shield. Privacy Shield kunde tidigare användas som lagligt stöd för att överföra uppgifter till USA. I och med att denna överföringsmekanism underkändes så har möjligheten att överföra personuppgifter till USA starkt begränsats vilket skapat stora utmaningar för regionen liksom andra personuppgiftsansvariga i Sverige och Europa.

Genom ett nytt beslut från EU-kommissionen juli 2023, är det återigen möjligt att överföra personuppgifter till USA. Möjligheten gäller enbart de företag som har certifierat sig, det vill säga anslutit sig till dataskyddsreglerna hos det amerikanska Handelsdepartementet.
Saknar företag certifiering gäller inte lättnaden utan avrådan att använda sig av amerikanska leverantörer består. I vissa fall kan rekommenderade säkerhetsåtgärder tillämpas tillsammans med standardavtalsklausuler.

Vid nyttjande av tjänster som innebär överföring till tredjeland är det viktigt att vara uppmärksam då det nya beslutet närsomhelst kan stoppas, till följd av en trolig överklagandeprocess.
Personuppgifterna behöver fortsättningsvis pseudonymiseras och/eller krypteras i och med överföring till USA så långt det är möjligt utifrån den tänkta lösningen. Kortare uppsägningstider i avtalen är viktiga då det gör det möjligt att dra sig ur avtal om överföringen återigen skulle bli olaglig. Kraven gällande det systematiska informationssäkerhetsarbetet gäller som tidigare.

Under 2023 har en ny mall om konsekvensbedömning enligt GDPR tagits fram. I vissa fall ska en konsekvensbedömning ske enligt GDPR, det vill säga gällande personuppgiftsbehandlingen. Det är av stor vikt att arbetet med just konsekvens-bedömningarna i regionen kommer igång.

3.4 Microsoft Office 365

Teams infördes stegvis i två faser där fas ett innebär tillgång till chatt och mötesbokningar samt möten i Teams. Fas två innebär tillgång till att skapa team för grupper eller projekt, samarbeta, dela filer och använda verktyg som Planner, Forms och OneNote.
En konsekvensbedömning i samband med införandet av Teams startades under 2022 och slutfördes i början av 2023.

Under 2023 beslutades att regionen skulle införa Microsoft Office 365. En lösning som innebär att verksamheterna avgör vilken information som ska lagras lokalt och vad som ska lagras i molnet. (OneDrive).

Det har tagits fram nya riktlinjer, rutiner och utbildningsmaterial när det gäller informationssäkerhet kopplat till bland annat Teams.

3.5 Nytt vårdinformationsstöd, Cosmic

Under större delen av 2023 har ett stort fokus varit på informationssäkerhetsarbetet kopplat till det nya vårdinformationssystemet Cosmic. Regionens informationssäkerhetssamordnare har deltagit i en Sussa gemensam informationssäkerhetsgrupp (de nio regioner som ingår i den så kallade Sussa samverkan) men även i arbetet med informationssäkerhetsfrågor internt kopplat till införandet av Cosmic.

Det Sussa-gemensamma arbetet har exempelvis inneburit att på Sussa-nivå hantera gemensamma informationssäkerhetsfrågor samt ta fram gemensamma mallar och underlag för det systematiska informationssäkerhetsarbetet. Exempelvis har mallar för riskanalyser och konsekvensbedömning baserat på rättsliga krav tagits fram. Det interna informationssäkerhetsarbetet har inneburit att mallar och andra underlag som tagits fram på Sussa-nivå förankrats internt. Vidare har det interna informationssäkerhetsarbetet inneburit att ge råd och stöd i informationssäkerhetsfrågor inom regionen.

Ett omfattande arbete lades ner på acceptanstester under oktober månad 2022. Acceptantesterna byggde på att verifiera dokumentation ur perspektivet information- och it-säkerhet. Gruppen har fortsatt arbetat aktivt under 2023 med informations- och it-säkerhetsfrågor. Under perioden Q4 2023 har ett omfattande arbete genomförts för att genomföra användartester kopplat till lagar och förordningar samt it-säkerhet. Ett arbete inom regionen har initierats för att på regional nivå under 2023 genomföra informationsklassning, riskanalyser, Konsekvensbedömning (DPIA) samt kontinuitetsplanering kopplat till det nya vårdinformationssystemet.

3.6 Externa och interna samarbeten

3.6.1 Informationssäkerhetsgruppen i Sjukvårdsregion Mellansverige

I takt med digitaliseringen har samarbetet mellan regionerna stärks, främst inom Sjukvårdsregionen Mellansverige och genom informationssäkerhetsgruppen.

Informationssäkerhetsgruppen är underställd samverkansnämndens ledningsgrupp. Informationssäkerhetsgruppen består av medlemmar från sjukvårdsregionens sju regioner. Gruppens huvuduppgift är att utveckla samarbetet inom informationssäkerhetsområdet inklusive dataskydd och cyberssäkerhet, öka kompetensen inom området och synliggöra det samarbete som sker.

I arbetsgruppen ingår regionernas informationssäkerhetssamordnare/chefer, dataskyddsombud, jurister samt resurser med it-säkerhetskompetens. Under 2023 har fyra digitala möten genomförts. I augusti 2023 tog Region Örebro län över rollen som ordförande i informationssäkerhetsgruppen.

3.6.2 Hälso- och sjukvårdens informationssäkerhetsnätverk, HoSiS

HoSiS är främst ett nätverk för de som arbetar med eller har ett ansvar för arbetet med informationssäkerhet inom regionernas hälso- och sjukvård i Sverige.
Syftet med nätverket är att ge de personer som har ett uppdrag att samordna och stödja arbetet med hälso- och sjukvårdens informationssäkerhet i regionerna möjlighet att utbyta kunskap och information med varandra.

Målet är att genom att delta i nätverksträffar erbjuda medlemmar ett stöd för sitt arbete inom informationssäkerhetsområdet i den egna organisationen samt att tillhandahålla ett forum för utbyte och omvärldsbevakning. Ambitionsnivån med nätverket är att stödja och styra aktiviteter utifrån gemensamt framtagna fokusområden samt att informera om SKR:s och MSB:s kommande aktiviteter.

3.6.3 Regionservice IT-SIRT

IT-SIRT (IT Security Incident Response Team) är en operativ funktion med deltagare från samtliga teknikområden inom Regionservice IT, Regionservice Fastigheter och Regionservice Shared Service Center.

Syftet är att teamet ska hålla sig välinformerad om aktuella hot och inträffade säkerhetsincidenter inom regionen samt i omvärlden för att säkerställa att olika hotbildscenarier och säkerhetsincidenter kan hanteras och proaktivt verka för ökad säkerhet. Informationssäkerhetssamordnare deltar i IT- SIRT gruppens regelbundna avstämningar.

3.6.4 Regionservice IT-Säkerhetsgruppen

IT-säkerhetsgruppen har deltagare från samtliga avdelningar inom Regionservice IT, och även från Regionservice Medicinsk Teknik MT, Regionservice Fastigheter och Regionservice Shared Service Center samt regionens informationssäkerhets-samordnare. Syftet är att informera och diskutera aktuella informations- och IT-säkerhetsrisker samt vara ett stöd för de olika deltagande verksamheterna.

3.6.5 Regionövergripande kunskapsutbyte inom it- och cybersäkerhet

Syftet med gruppen, där alla regioner ingår, är att dela kompetens och erfarenheter gällande verktyg och arbetssätt med mera inom it- och cybersäkerhetsområdet. Gruppen träffas cirka 4-5 gånger per år.

3.6.6 Övriga samarbeten

Förutom ovan nämnda samarbeten sker regelbunden avstämning mellan informationssäkerhetssamordnare och it-säkerhetsansvarig för informationsutbyte och diskussion avseende aktuella frågeställningar inom informationssäkerhetsområdet.

4. Granskningar och skyddsåtgärder

4.1 Informationsklassning och riskanalys

Risker som påverkar regionens informationssäkerhet ska identifieras, analyseras och behandlas samt återföljas av kontinuerlig uppföljning. Beslut om olika lösningar ska baseras på bedömd risk och informationstillgångarnas klassificeringsvärde. Informationsklassning är grunden för att genomföra en riskanalys då riskanalysen baseras på informationens värde.

Informationsägare är den som äger och ansvarar för den information som skapas och används inom verksamheten. Ansvar som informationsägare följer det delegerade verksamhetsansvaret.

Det finns fortsatt ett behov av att öka kunskapen i verksamheterna när det gäller det systematiska informationssäkerhetsarbetet. Trots att det skett en ökning av arbetet så behöver fler personer i verksamheterna kunna genomföra riskanalyser och informationsklassningar av regionens informationstillgångar. Informationsklassningar och riskanalyser är grunden i det systematiska informationssäkerhetsarbetet. Detta är således något som måste bli en naturlig del av all informationshantering, exempelvis vid upphandlingar, inköp, drift och förvaltning av it-stöd samt för hantering av information i verksamheternas processer.

4.2 Granskningar

Ingen extern granskning eller tillsyn har utförts eller ägt rum under 2023.

4.3 Skyddsåtgärder

4.3.1 Loggning och logguppföljning

Loggning och logguppföljning är en viktig del i regionens arbete med patientsäkerhet. Framför allt för att kunna visa att regionens hantering av personuppgifter sker på ett legalt och riktigt sätt men också för att kunna utreda misstankar om otillåten hantering av personuppgifter. Regionen är enligt lag skyldig att föra logg över elektronisk åtkomst inom vårdgivarens verksamhet och dokumentera regelbunden och systematisk loggkontroll.

Loggsystemet var länge ett så kallat oförvaltat system men under 2022 kom loggsystemet in i den ordinarie systemförvaltningen och tillhör nu Vårdsystem. Logghanteringen sköts av Administrativ service, Hälso- och sjukvårdsförvaltningen.

Under 2023 har 277 patienter begärt ut loggar över vilka anställda som tagit del av deras journaluppgifter. Därutöver uppkommer olika situationer som gör att verksamhetschefer efterfrågar loggar på medarbetare, det kan till exempel vara kompletterande uppgifter till de slumpvisa loggarna eller att verksamhetschefen fått till sig uppgifter som rör misstanke om otillåten/obehörig åtkomst som måste granskas och kontrolleras vidare.

5. Uppföljningar

5.1 Uppföljning av informationssäkerhetsarbetet i regionen Intern styrning och kontroll (ISK)

Intern styrning och kontroll (ISK) är en process där regionstyrelsen, nämnderna och verksamhetsledningar har för att tillsammans upprätthålla en effektiv ledning och styrning av verksamheten. Processen ska säkerställa en ändamålsenlig och lagenlig verksamhet, det vill säga att verksamheten bedrivs i enlighet med de krav som ställs på verksamheten. För att säkerställa att kraven är uppfyllda finns i uppföljningen av ISK-processen beskrivningar av risken samt vad som förväntas av förvaltningarna när det gäller rapportering av informationssäkerhetsarbetet. När det gäller informations-säkerhetskraven ska dessa vara tillgodosedda utifrån kraven på konfidentialitet, riktighet, tillgänglighet samt spårbarhet.

För att säkerställa att kraven var uppfyllda under 2023 fanns i uppföljningen av ISK-processen beskrivningar av risken samt vad som förväntades av förvaltningarna när det gäller rapportering av informationssäkerhetsarbetet.

Risk:
Risken att verksamheten inte efterlever tillämplig dataskyddslagstiftning (GDPR och patientdatalagen) samt NIS-direktivet som implementerats genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Regionövergripande åtgärder inför 2023:

- Säkerställ ett systematiskt och riskbaserat informationssäkerhetsarbete med användande av de resurser som i prioritering i förhållande till andra angelägna verksamheter, kan anslås. All berörd personal ska ha god kunskap om och medverka till att följa regelverk för informationssäkerhet, att informationsklassa och riskbedöma vid inköp, upphandling och förändring som kan påverka informationssäkerheten.
- Säkerställ att informationsklassning av IT-stöd som innehåller personuppgifter har genomförts i enlighet med riktlinje för informationsklassning.
- Informationsägare/objektägare ska säkerställa att identifierade informationssäkerhetsbrister åtgärdas.

  Regionkansliet har rapporterat följande: Arbetet med informationssäkerhet pågår kontinuerligt. Staben administration, juridik och säkerhet har uppdraget att verka för att arbete görs i de olika delar av organisationen som berörs.

  Inom kommunikationsområdet har en genomlysning gjorts och vid förändringar ses informationssäkerheten över. Avseende digitalisering, när nya system implementeras som Regionkansliet ansvarar för, sker ett systematiskt informationssäkerhetsarbete i dialog med enheten för juridik och säkerhet. Arbete genomförs också i samarbete med andra verksamheter inom regionen men också nationellt gällande de nationella tjänsterna som regionen ansluter underliggande systemstöd till. Varje nytt it-system som implementeras analyseras utifrån informationssäkerhetsaspekten. Det är ett pågående arbete och Regionkansliet är även resurs i vissa avseenden i verksamheterna. De nationella systemen som regionen ansluter till informationsklassas via Inera respektive e-hälsomyndigheten.

  Regionkansliet arbetar löpande med informationssäkerhetsfrågor i samarbete med förvaltningarna. Regionkansliet arbetar med att dels verka för att brister som upptäcks åtgärdas, dels med att övergripande arbeta med att försöka upptäcka brister. Arbete fortgår även inom regionens verksamheter. För det nya vårdinformationsstödet sker arbetet tillsammans med åtta andra regioner

på en övergripande nivå, för att sedan tas hem till regionen och arbeta utifrån den regionala nivån utifrån dess förutsättningar. Arbete sker även på nationell nivå när det gäller vård och e-tjänster via bolaget Inera.

5.2 MSB:s Infosäkkoll– i syfte att mäta kunskap och informationssäkerhetskultur i regionen

Ett regeringsuppdrag ställdes till MSB (Myndigheten för samhällsskydd och beredskap) 2021 för att mäta framför allt förutsättningen för det systematiska informationssäkerhetsarbetet och i vilken utsträckning som det systematiska arbetet bedrivs i regioner och kommuner. De angivna svaren genererades in enligt en uppföljningsmodell som delade in det systematiska informationssäkerhetsabetet i fyra nivåer:

- Nivå 1: organisationer som har grunderna i informationssäkerhetsarbetet
- Nivå 2: organisationer som bedriver informationssäkerhetsarbetet med viss systematik och är bättre på grunderna
- Nivå 3: organisationer som har ett kvalificerat innehåll i informations-säkerhetsarbetet samt är bättre på både grunderna och systematiken
- Nivå 4: organisationer som arbetar avancerat med ständiga förbättringar samt är bättre på grunderna, systematiken och innehållet

IT-säkkollen

It-säkkollen är framtagen i enlighet med regeringsuppdraget Fö2023/00697 som uppdrogs MSB 23 mars 2023 och ingick som en del av infosäkkollen. It-säkkollen består av en enkät med 41 frågor baserade på MSB:s föreskrifter där svaren baseras på självskattande utifrån fyra svarsalternativ: stämmer inte, stämmer knappt, stämmer väl och stämmer helt. Resultatet från it-säkkollen som baseras på uppskattade svar från respondenterna lämnar ett stort tolkningsutrymme vilket påverkar trovärdigheten av insamlade data. It-säkkollen ska vidareutvecklas fram till 2025. Undersökningen ska ges samma metodologiska robusthet som Infosäkkollen. Inget resultat är därför redovisat i denna årsrapport.

Resultat 2021

Resultat 2023

Målet för regionen var att uppnå alla delar i nivå 1 fram till den mätning som genomfördes september 2023. Den nya mätningen visar ett positivt resultat där regionen uppnår alla delar i nivå 1 samt ett större ökat resultat inom incident- och kontinuitetshantering samt upphandling.
MSB har nu fått uppdrag från Regeringskansliet att genomföra mätningar årligen.

6. Förbättringsåtgärder

Här nedan följer en kort sammanställd redovisning av de förbättringsåtgärder som rapporterats av förvaltningarna för 2023.

- Stödja medarbetare i informationssäkerhetsarbetet genom att delta i grupperingar kopplade till informationssäkerhet i regionen.
- Lyfta behovet av dialoger inom informationssäkerhetsområdet.
- Genomgång av rutiner och var information finns på intranätet för nya medarbetare.
- Nya medarbetare ska genomgå e- learningutbildning för informationssäkerhet i PingPong.
- Arbeta aktivt med ansvar och säkerhet vid digitala möten.
- Säkra autentiseringen genom att ″authenticator″ installeras för samtliga datoranvändare.

6.1 Genomförda aktiviteter 2023

6.1.1 Hälso- och sjukvårdsförvaltningen

Flertalet verksamheter inom Hälso- och sjukvården har informationssäkerhet som en del av sitt årshjul där dialog samt genomgång av rutiner sker regelbundet på arbetsplatsträffar. Vid introduktion av nya medarbetare sker en genomgång av rutiner och vat information finns att tillgå på intranätet. E-learningutbildning för informationssäkerhet i regionens utbildningsportal PingPong ingår i flertalet av verksamheterna som en del i introduktionsprogrammet. Vissa verksamheter arbetar aktivt med att uppdatera kunskapen hos medarbetare genom att uppmana att gå utbildningen vartannat år.

Kunskapen gällande ansvar och säkerhet vid digitala möten är hög då medarbetare generellt har hög kunskap för sekretessfrågor. Verksamheterna väljer de säkra mötesalternativen utifrån regionens rutiner. Det är tydligt att riktlinjer och rutiner för hur digitala möten ska genomföras har fått ett stort genomslag och att medvetenheten för säkra digitala möten generellt är hög i samtliga verksamheter. Resultatet av genomförda aktiviteter är en ökad medvetenhet, säkerhet och kunskap för frågor som rör informationssäkerhet.

6.1.2 Folktandvården

En säkerhets- och beredskapshandbok har skrivits under 2023 där alla riktlinjer och rutiner finns för bland annat IT-säkerhet och informationssäkerhet. Syftet med handboken är att all säkerhets- och beredskapsinformation ska vara samlad på ett ställe och därmed blir informationen enklare för chefer och medarbetare att hitta.

Under 2023 har Microsoft Office 365 införts i folktandvården. Ett projekt har startats för att ta fram riktlinje och handlingsplan för Folktandvårdens dokumenthantering för de olika lagringsytorna SharePoint, OneDrive, (G:\) och (H:\) och genom det kvalitets- och informationssäkra dokumenthanteringen.

Det sker säkerhetsronder 1gg/år (– fysiskt vartannat år och via mejl vartannat år) där Folktandvårdens säkerhetssamordnare går igenom informationssäkerhet med klinikledningen och påminner om regionens e-learningutbildning ”DISA” där målet är att alla medarbetare ska genomföra utbildningen 1gg/år.

Det finns även en utsedd verksamhetsansvarig för digitala vårdmöten vilket innefattar ansvar för att dessa sker på rätt sätt enligt framtagen riktlinje. Riktlinjen innehåller rekommendationer om när vilken plattform ska användas för att säkerheten ska vara den rätta i de alternativa plattformarna Teams, Pexip, Visiba Care samt Videokonferensutrustningen. Samtliga medarbetare har tillgång till riktlinjen och den är kommunicerad på chefsmöten och utskickad via Folktandvårdens ledningsnytt.

6.1.3 Regional utveckling

Regional utveckling har arbetat med att säkerställa säkerhet i de IT-stöd som finns inom förvaltningen. Det har skett genom att stärka kontinuitet, förnyat avtal och personuppgiftsbiträdesavtal samt genom utbyte av gamla servrar. Ett flertal klassningar och riskanalyser har genomförts för att bland annat kunna ge underlag till beslut om förändringar.

Genomgång av informationssäkerhet har skett på förvaltningens ”fredagsmöte” där alla verksamheter deltar. Information har delgetts alla chefer att alla nya medarbetare ska gå e-learningutbildningen “DISA”. Inför införandet av Teams genomfördes en genomgång av de riktlinjer och rutiner som är framtagna för hur Teams ska användas.

Säkerhetssamordnaren har under 2023 påbörjat diskussioner med chef för att hitta rätt struktur att arbeta med informationssäkerhetsfrågorna inom Regional utveckling i syfte att få detta mer regelbundet och repetitivt.

6.1.4 Företagshälsa och Tolkförmedling

Dialog sker löpande på informationssäkerhetsområdet och en avvägning görs kring hur mycket resurser som kan avsättas för informationssäkerhetsarbetet inom förvaltningen. Det finns en god kännedom om vilka kontaktvägar som ska användas vid frågor på informationssäkerhetsområdet inom förvaltningen. Sedan 2021 finns ett introduktionsprogram för nya medarbetare där vägledning till var information finns att tillgå samt att nya medarbetare ska gå e-learningutbildningen ”DISA”. Information

om alternativa plattformar för digitala möten har kommunicerats under 2022 och vid införandet av Teams 2023.

6.1.5 Regionkansliet Staben Digitalisering

Det finns en medvetenhet och engagemang i informationssäkerhetsfrågor. En återkoppling sker från de grupperingar som representanter staben, där informationssäkerhetsrådet är exempel på en sådan gruppering. Utöver det är digitaliseringsstaben engagerade i informationssäkerhetsfrågor kopplat till de uppdrag, projekt samt förvaltningsobjekt.
Nya medarbetare genomgår e-learningutbildningen "DISA" samt får en genomgång av rutiner och var information finns att tillgå på intranätet.
Checklistor inför start av nya projekt och uppdrag innehåller beaktande och värdering utifrån informationssäkerhetsaspekterna. I arbetet med informationsklassning och riskanalys finns det medarbetare som leder och är behjälpliga vid behov. Uppstår ytterligare behov tas konsult in som hjälp.

6.1.6 Regionkansliet Staben Administration juridik och säkerhet

Staben administration, juridik och säkerhet har i det dagliga arbetet pågående dialoger med regionens verksamheter samt som en del i uppdraget att fungera som rådande och stöttande för hantering av information gällande säkerhetsskyddsklassad information samt vid hantering av utlämnande av information på begäran av medborgare.

Informationssäkerhet en del av det dagliga arbetet som sker. Nya medarbetare genomgår e-learningutbildningen "DISA" samt får en genomgång av rutiner och var information finns att tillgå på intranätet.
En informationsklassning har genomfört som grund till vilken information som är lämpad att använda Teams till både gällande samarbetsyta och som mötesform. Regionens mötesform Pexip används då Teams inte är tillämplig. Exempelvis för de politiska möten som sker digitalt.

Staben Juridik och säkerhet ingår i olika forum och samarbeten regionalt och lokalt samt är ansvariga för exempelvis regionens informationssäkerhetsråd där information delges samt dialoger förs.
Det finns behov av en ökad kännedom för regionens process för det systematiska informationssäkerhetsarbetet inom enheterna i staben.

6.1.7 Regionservice Stab

Under året har Regionservice stab arbetat aktivt för säker hantering av personuppgifter som sänds via mejl och internposten. Framför allt genom att efterfråga krypterade mejl innan sändning samt att återkoppla när personuppgifter sänds utan kryptering.
I möjligaste mån handläggs direkt i berörda system för att minimera mängd skickad eller sparad information.

I november 2021 genomförde samtliga medarbetare den webbaserade utbildningen DISA. Något som behöver utvecklas under 2024 är att säkerställa att nya medarbetare får e-learningutbildningen i introduktionsprogrammet.
Resultatet av våra genomförda aktiviteter förväntas minimera risk för bristande informationssäkerhet.

6.1.8 Regionservice IT

IT-säkerhetsansvarig och IT-säkerhetspecialist leder IT-säkerhetsforum såsom IT-SIRT och IT-säkerhetsgruppen IT-SIRT (IT Security Response Team) är en operativ funktion med deltagare från samtliga teknikområden inom RSE IT, där RSE Fastigheter och RSE Shared Services samt regionens informationssäkerhets-samordnare ingår.
IT-säkerhetsgruppen har deltagare från samtliga avdelningar inom RSE IT, representant från RSE MT, Fastigheter och Shared Services samt regionens informationssäkerhetssamordnare.
Syftet med dessa grupper är att informera och diskutera aktuella informations- och IT-säkerhetsrisker samt vara ett stöd för de olika deltagande verksamheterna.

Samtliga medarbetare inom RSE IT har fått information om regionens lednings-process för systematiskt informationssäkerhetsarbete genom att regionens informationssäkerhetssamordnare och dataskyddsombud har bjudits in till respektive avdelning för en genomgång av processen och GDPR gällande aktuellt rättsläge avseende tredjelandsöverföringar.

Pexip används vid videomöten där känslig information kan behandlas.

6.1.9 Regionservice Medicinsk Teknik

Medicinsk Teknik arbetar kontinuerligt med informationssäkerhet i anslutning till medicintekniska utrustningar och system. I anslutning till upphandlingar sker ett samarbete med lokala informationssäkerhetssamordnare inom hälso- och sjukvården för att ställa krav till leverantörer och verksamhet. Möten i samband med

upphandlingar som omges av sekretess genomförs i första hand som fysiska möten, där fysiska möten inte är möjliga används säkra möteslösningar såsom Pexip.

På checklistan för nya medarbetare på MT trycks särskilt på informationssäkerhet. En punkt på checklistan är bland annat att genomföra e-learning för informationssäkerhet.
Det är en ökad medvetenhet och kunskap bland medarbetare kring ämnet informationssäkerhet som har genererat att det ställs tydligare krav till leverantörerna i samband med anskaffning av medicintekniska utrustningar och system.

6.1.10 Regionservice Avdelning Upphandling

Området har kontinuerliga dialoger med verksamheterna i samband med upphandlingar och avtalsförvaltning. Alla medarbetare har genomfört e-learningutbildning i informationssäkerhet. Rutiner och information finns upprättade genom checklista gås igenom med nya medarbetare.
Området har även ett forum, upphandlarakademin, som är ett internt utbildningsforum tillsammans med MT där bland annat frågor och diskussioner tas upp rörande informationssäkerhet.

6.1.11 Regionservice Regionarkiv och registratur

Dialoger inom informationssäkerhetsområdet sker i olika sammanhang och lyfts kontinuerligt i det löpande arbetet. Exempelvis i arbetet med informationshanteringsplaner och inom E-arkivprojekten.

Samtliga medarbetare inom Regionarkiv och registratur har fått information om regionens ledningsprocess för systematiskt informationssäkerhetsarbete på APT av regionens informationssäkerhetssamordnare.
Introduktion av nya medarbetare innefattar genomgång av rutiner och var information finns att tillgå på intranätet. Nya medarbetare ska genomgå e-learningutbildningen ”DISA” vilket även är en uppmaning att alla medarbetare årligen ska gå.

6.1.12 Regionservice Shared Service Center

Introduktion av nya medarbetare innefattar genomgång av rutiner och var information finns att tillgå på intranätet. Nya medarbetare ska genomgå e-learningutbildningen ”DISA”.

Det arbetas aktivt med ansvar och säkerhet vid digitala möten och det har ökat medvetenheten hos alla medarbetare.

6.1.13 Regionservice Område Fastigheter

Område fastigheter har inte ett löpande arbete kring informationssäkerhet (dialog, rutiner, utbildning). Diskussioner förs dock kring detta och det finns ett arbete att förbättra.

6.1.14 Genomförda förbättringar kopplat till IT

Följande har rapporterats in:

Regionalutveckling:
Nytt avtal är tecknat med leverantören Align för att säkerställa kraven på informationssäkerheten.

Folktandvården:
Folktandvården har implementerat ett verktyg och IT-system för säker digital kommunikation (SEFOS) samt genomfört aktiviteter för en ökad användning, vilket har fallit väl ut. SEFOS används idag i interna flöden inom Folktandvården och regionen samt externa flöden vid journalutlämning.
Folktandvården Direkt/ tidbok har aktiverats med tvåfaktorsautentisering. Länkar har tagits bort i SMS utskick

Regionservice IT:
Installation av ”Authenticator”
”Authenticator” används i dagsläget endast på regionägda mobiltelefoner för att de ska kunna köra Teams-appen, och används än så länge således inte på våra regiondatorer.

6.2 Rapporterade planerade aktiviteter för 2024

Informationssäkerhet delas in i administrativ **säkerhet** (regler och rutiner), **teknisk säkerhet** (säkerhet i IT-stöd samt andra tekniska system) samt **fysisk säkerhet** (skalskydd, larm och tillträdeskontroll). Nedan listas de planerade aktiviteter som har rapporterats från verksamheterna.

6.2.1 Teknisk säkerhet

- Implementation av nytt tandvårdssystem FRENDA
- Slutföra arbetet med införandet av Objekt tandvård digitala system för att skapa ett samlat arbetssätt för digitala processer inom Folktandvården. (ITIL)
- Informationsklassning och riskanalys för IT-infrastruktur för framtagande av åtgärdsplaner.
- Uppdatering av Kontinuitetsplan i samverkan med verksamheterna (IT)

6.2.2 Administrativ säkerhet

- Fortsatt implementation av tandvårdssystemet Frenda enligt arbetssätten i det systematiska informationssäkerhetsarbetet.
- Översyn och revidering av riktlinjer.
- Handbok för systematiskt och riskbaserat IT-säkerhetsarbete.
- Fortsatt följa och implementera arbetet med informationssäkerhet i verksamhetens processer.
- Utbildningsinsatser för att höja kunskapen hos medarbetare gällande digitala möten samt behandling av information i vardagen.

6.3 Ett verktyg för informationsklassning och riskanalys

Regionen använder idag verktyget Isak för informationsklassning. Isak är en äldre Excelfil som är framtagen tillsammans med Region Dalarna. Verktyget/Excelfilen innehåller en mall för informationsklassning och riskanalys samt kravställning utifrån de tre säkerhetsaspekterna. Isak är framtagen för att utföra informationsklassning riktat till it-stöd. För att bedriva ett systematiskt informationssäkerhetsarbete ska all information klassas oavsett var i verksamheten den finns. Det kan exempelvis handla om system, processer eller arbetsflöden där olika informationsmängder hanteras. Detta arbete försvåras idag eftersom Isak primärt är lämpat för informationsklassning av it- stöd.

SKR har under 2021 och 2023 tagit fram ett webbaserat verktyg för informations-klassning och riskanalys, KLASSA, för att stödja kommuner och regioner i informationssäkerhetsarbetet med möjlighet att genomföra en informationsklassning och riskanalys kopplat till it-stöd, enskilda dokument och processer. Regionens informationssäkerhetssamordnare har varit delaktig i arbetet tillsammans med SKR och andra regioner och har därmed haft möjlighet att påverka hur klassningsverktyget på ett lämpligt sätt ska kunna stötta verksamheterna i sitt arbete med informations-klassning och riskanalyser.

KLASSA bygger på modellen för informationsklassning enligt MSB:s metodstöd för systematiskt informationssäkerhetsarbete utifrån standard (SS-ISO/IEC 27001:2017) för ledningssystem och innehåller fyra delar: informationsklassning, kravställning/ handlingsplan, upphandlingskrav och riskanalys. KLASSA innehåller vidare utbildningsmaterial och stödjande texter för informationsklassning och riskanalys som tillses av SKR.

Regionens informationssäkerhetssamordnare fortsätter att bevaka och delta i arbetet med KLASSA.

6.4 Utbildningsinsatser

Ett flertal utbildningar genomförs löpande. Exempelvis utbildning för chefer inom ramen för Formellt ledarskap, utbildning för ST-läkare, utbildning för BT-läkare, utbildning för studerande vid läkarprogrammet termin 8 ”Juridik, informations- och patientsäkerhet”.

Informationsinsatser har skett gällande roller och ansvar kopplat till informationssäkerhetsarbetet till ett antal ledningsgrupper. Vidare har informationsinsatser om hur informationsklassningar och riskanalyser ska ske ägt rum, även dessa till några grupper i regionen.

Det finns en rekommendation att samtliga anställda ska genomföra den e-learningutbildning om informationssäkerhet (DISA) som finns att tillgå i regionens utbildningsportal PingPong. DISA är en utbildning som MSB har tagit fram som tar upp olika aspekter av informationssäkerhet. Utbildningen består av kortare filmer samt påståenden med efterföljande frågor. Utbildningen tar bland annat upp; säkert beteende, lösenord, e-post, skadlig kod, sociala medier, mobila enheter, molntjänster, säkerhetskopiering och loggning och spårbarhet.

Informationssäkerhetssamordnare och dataskyddsombud har genomfört ett flertal informationsinsatser kopplat till processen för det systematiska informationssäkerhetsarbetet samt behandling av personuppgifter (GDPR) och överföring till tredjeland på verksamheternas arbetsplatsträffar.

7. Incidenter/avvikelser

Incidenter och avvikelser sker ofta genom systemfel och misstag. System och infrastrukturen är i dag både stora och komplexa samtidigt som de yttre hoten ökar i takt med digitaliseringen och vår föränderliga omvärld. Ett systematiskt informationssäkerhetsarbete är ett stöd vid kravställning av säkerhet och administrativa rutiner. Verksamheterna behöver därför prioritera informationssäkerhetsarbetet genom att avsätta tid för kartläggning av processer och identifiering av informationstillgångar, identifiera informationsägare, genomföra informationsklassningar med tillhörande riskanalys och när krav ställs genomföra konsekvensbedömning.

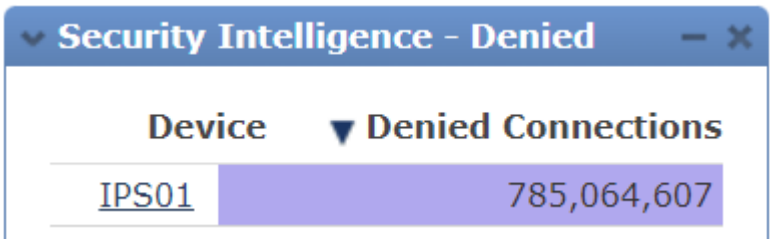
7.1 IT incidenter, ransomware och phising med mera

7.1.1 Granskade och stoppade intrång via internet

Regionens intrångsskydd (IPS = Intrusion Prevention System) arbetar utifrån två huvudprinciper, det stoppar trafik utifrån avsändar-/destinationsadress och det analyserar övrig trafik efter ”signaturer” (det vill säga kännetecken) som tyder på

skadligt beteende. Regionen har ett abonnemang och det kommer fortlöpande information till regionen om svartlistade adresser och intrångs-signaturer som är förknippade med it-brottslighet och skadlig mjukvara.

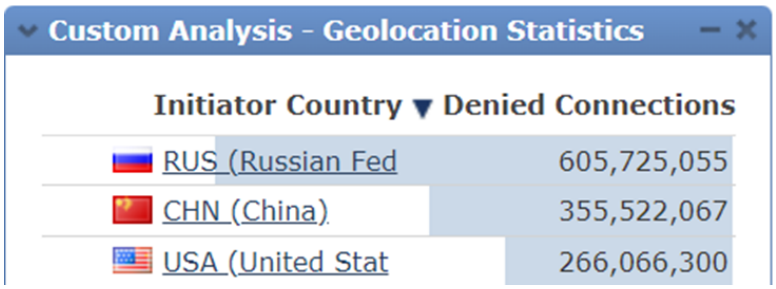
Den första sortens trafik (från/till svartlistade adresser) har ökat och ligger på en högre nivå än tidigare. Nivån låg på 320 miljoner blockerade requests under 2022. Nivån under 2023 låg på 785 miljoner blockerade requests det vill säga cirka 2,2 miljoner per dag (mer än en fördubbling jämfört med 2022). Totalt antal blockerade requests på grund av svartlistning under det senaste året:



Det mesta av denna trafik genereras säkerligen av automatiska genomsökningar efter sårbarheter, men en del är också manuellt initierade attackförsök. Denna sorts bakgrunds-brus pågår hela tiden, utan avbrott, och blockeras direkt av intrångsskyddet. ”785 miljoner blockeringar” betyder inte att miljontals olika hackers har försökt attackera regionen utan det innebär att ett antal ihärdiga förövare eller automatiserade processer har försökt många tusentals gånger var.

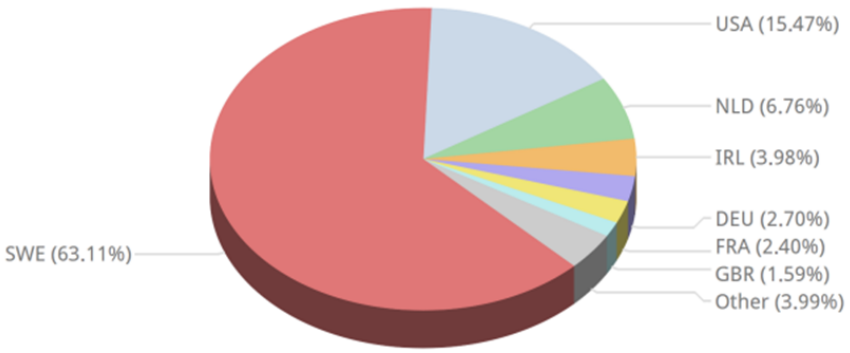
Den andra sortens trafik (som matchar signaturer och kan tyda på mer riktade attacker) har varit mera konstant över tid.
På grund av hotläget så ”Geo-blockeras” trafik till/från vissa länder. De absolut mest aktiva länderna med offensiva it-aktiviteter har i detta fall varit Ryssland och Kina. Följande siffror visar blockerade requests från Ryssland, Kina och USA. Mängden trafik från Ryssland har varierat över tid men har tidvis varit flera miljoner request per dag.

Antal blockerade requests per geografiskt område under det senaste året:



Nedanstående diagram visar fördelning av tillåten trafik vid en specifik tidpunkt och representerar inte medel över hela perioden. Regionen har inte möjlighet att få ut denna typ av statistik över en längre period. Det kan noteras att det land regionen kommunicerar mest med är Sverige, USA, Irland och Holland.

Trafik mot regionen, fördelning per sourceland:



7.1.2 E-post filter

Det e-postfilter som regionen använder är Exchange Online Protection från Microsoft. Det är en extern tjänst utanför regionens datahallar som kontrollerar mailflödet innan e-post släpps in i regionens miljö. E-postfiltret har också funktionen att sätta inkommande misstänkt e-post i karantän där mottagaren, och administratörer, kan granska e-posten utanför regionens egen miljö för att kunna släppa in mejl som av mottagaren bedöms vara ok. Baserat på hur e-posten i karantän hanteras av respektive användare kommer filtret att ”lära sig” hur inkommande mejl bör klassificeras.

Merparten av den blockerade e-posten klassar filtret som "Spam" eller "Skräppost". I de fall e-post innehåller en av tjänsten ej provad och godkänd länk så skrivs länken om så att man först landar hos den externa tjänsten som undersöker målsajten, vilket minskar risken avsevärt för att klicka sig igenom till en skadlig länk. E-post från mejlservrar på ökända IP-adresser blockeras direkt och listorna på adresser underhålls löpande av leverantören.

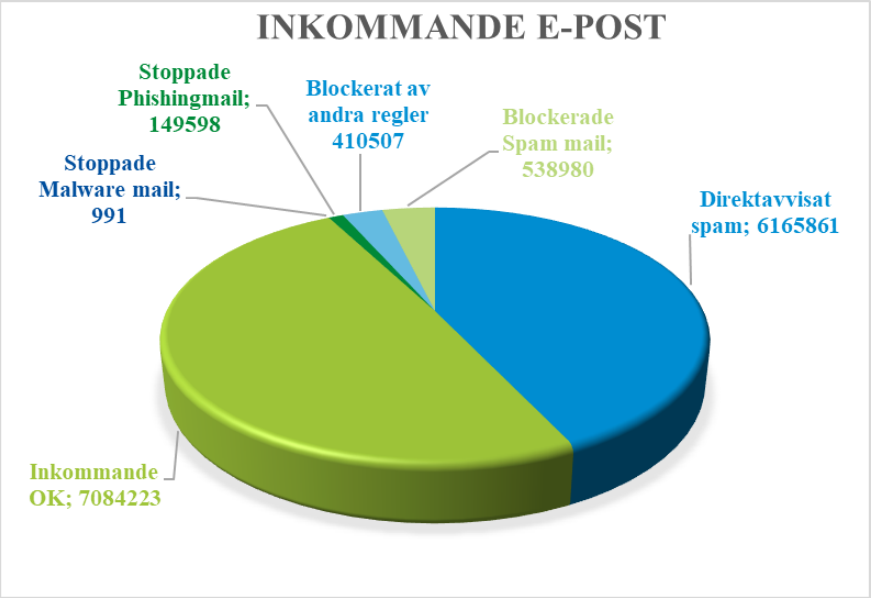
Regionen vitlistar inte e-postadresser. Det rådande säkerhetsläget medger inte det. En av de vanligaste orsakerna till att e-post fastnar i filtret är att det inte går att verifiera att avsändaren är vad eller vem den utger sig för att vara. Det som visas som avsändare är väldigt lätt att förfalska (spoofa) och utnyttjas frekvent i phishing-attacker.

I slutet av 2023 infördes en informationstext (banner) längst upp i inkommande e-post från extern part för att mottagaren lättare ska kunna avgöra falsk avsändare och vara vaksam på innehållet i denna e-post.
Noterbart är att om det e-postsystem som avsändaren använder inte är rätt konfigurerat så går det inte att spåra vem avsändaren är vilket kan medföra att legitim e-post fastnar i karantän på grund av spårbarhetsregler.

Totalt under år 2023 har det till alla regionens domäner adresserats drygt 14 miljoner e-post. Av totalen har cirka 7,3 miljoner e-postleveranser blockerats, det mesta har klassats som spam sedan kommer blockering på grund av förfalskade avsändar-adresser (spoofing) högt i statistiken.

Under större delen av året följer inflödet av spam samma veckovisa mönster där det egentligen inte sticker ut några värden sett över året, Däremot ser man att det är en ökande trend av inkommande e-post av alla kategorier, inte minst av e-post klassat som nätfiske (phishing).

Ur statistiken från mejlfiltret går det att se vad som av en eller annan anledning har stoppats och i viss mån varför. Det går dock inte att se vilket innehåll som har släppts igenom utan någon åtgärd.



7.2 Världsomfattande hotbild

Hela samhället står inför utmaningar i takt med att vår omvärld ständigt förändras. Regionen måste anpassa sig till en ständigt förändrad och alltmer komplex hotbild. Det blir alltmer sofistikerade affärsmodeller för cyberkriminella, som lätt kan hyra ransomware som en tjänst utan att behöva ha en nämnvärd teknisk kompetens. Samtidigt kan de anpassa sina angrepp med hjälp av artificiell intelligens. För regionens medarbetare gäller det därför att vara mer vaksam och ställa sig frågan varför man får ett meddelande, från vem och bedöma om innehållet ser riktigt ut. Detta gäller oavsett om man får ett meddelande via mejl eller sms.

Informationssäkerhet är inte enbart en IT-fråga. Informationssäkerhet handlar även om riktlinjer, rutiner och hur vi användare agerar.
I oktober utspelades en händelse på Helsingborgs lasarett då personal uppmärksammade en man som rörde sig inne på en av sjukhusets avdelningar. Han påstod då att han skulle kontrollera brandskyddet men hade ingen legitimation. Några dagar senare upptäcktes samma man med andra kläder då han den gången påstod att han hade uppdrag att utföra utbyte av datorer, vilket inte var fallet. Även här är det viktigt att alla har god kunskap och engagemang samt förståelse av vikten att endast personer som har behörighet vistas i våra lokaler.

Under 2023 kom det till regionens kännedom att bedrägeriförsök skedde då flera länsbor hade fått falska sms på sina mobiler från en avsändare som såg ut att vara Region Örebro län. I sms:et saknades information om vad meddelandet gällde, däremot fanns en uppmaning att klicka sig vidare via en länk.
Även om en cyberattack mot ett sjukhus inte stänger ner ett sjukhus helt, så kan den slå ut digital teknik och begränsa tillgången till digital information under en period såsom medicintekniska it-stöd, patientjournaler och vårdrekommendationer.

Det systematiska informationssäkerhetsarbetet är därför extra viktigt genom att analysera hotbild och risker samt att medarbetare har kännedom om riktlinjer och rutiner. Världen har förändrats och det är av vikt att vara uppmärksam på både attacker, påverkanskampanjer och vilka personer som rör sig i våra lokaler. Vi ska arbeta så proaktivt som möjligt genom samverkan, omvärldsbevakning samt identifiera tänkbara risker.

7.3 Driftavbrott it-system

I oktober inträffade en incident hos en leverantör till Region Örebro län. Denna resulterade i en kedjereaktion av systemberoenden och ledde till en större incident gällande att e-tjänstekorten tappade behörigheter till regionens kortläsare för lås och inpassering i passersystemet. Detta berörde ett flertal områden inom regionen och

påverkan inom hälso- och sjukvården bedömdes så stor att incidenten eskalerades till en särskild händelse i krisledning.

När det gäller driftavbrott i andra system har det rapporterats ett antal sådana av mindre karaktär. Dock inte något som avviker från det normala.

7.4 Personuppgiftsincidenter

Under 2023 har det registrerats 272 personuppgiftsincidenter i Platina, av dessa är det 28 incidenter som anmälts vidare till Integritetsskyddsmyndigheten, IMY. Det som är återkommande är kallelse/brev/läkarintyg som skickas till fel patient och dokumentation av patientuppgifter i fel journal.

8. Fokusområden 2024

8.1 Det systematiska informationssäkerhetsarbetet

Regionen behöver fortsatt förbättra informationssäkerhetskulturen. Kunskapen och medvetenheten behöver öka för de krav som ställs vid behandling av information i alla former. Informationssäkerhetsarbetet kan då bli mer effektivt och systematiskt och ge mera nytta för regionen i helhet.

Genom det systematiska och riskbaserade arbetet ökar kunskapen, avvikelser upptäcks tidigt och kan åtgärdas och allvarliga störningar kan undvikas. All information och de kritiska it-stöd inom regionen ska skyddas och det ska tillses att informationen är riktig och tillgänglig när den behövs. Vidare behöver även säkras att regionens verksamhet kan bedrivas med så liten konsekvens som möjligt om en incident inträffar genom att snabbt kunna reducera och återgå till normalläge.

Informationsklassningar och riskanalyser kommer alltid att behöva ske i verksamheter som hanterar information. Det ingår i det systematiska informationssäkerhetsarbetet och dataskyddsarbetet som ska finnas inom alla regioner och kommuner. Således är det här ett ständigt återkommande arbete för regionen liksom för alla andra organisationer som hanterar information. Processen för det systematiska informationssäkerhetsarbetet är ett stöd och vägledning då kompetensen för att genomföra de principer och arbetssätten ofta efterfrågas.
Processen upplevs som ett bra stöd och är väl känd i de förvaltningar som har avsatt resurser som arbetar för sitt informationssäkerhetsarbete.
Informationsinsatser kommer fortsatt att genomföras för det systematiska informationssäkerhetsarbetet.

8.2 NIS-direktivet och NIS- lagstiftningen

Den 6 juli 2016 antogs” The directive on security of network and information systems, the NIS directive, det så kallade NIS direktivet, av Europaparlamentet. Direktivet har implementerats i den svenska lagstiftningen genom Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagstiftningen omfattar leverantörer av samhällsviktiga och digitala tjänster. Regionen omfattas utifrån området hälso- och sjukvård inklusive tandvård.

Reglerna ställer bland annat krav gällande säkerhetsåtgärder, incidentrapportering och tillsyn. Regelverket ställer krav på att de verksamheter som omfattas ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Här handlar det om att identifiera de system som kan vara kritiska för att den samhällsviktiga tjänsten, hälso- och sjukvård inklusive tandvård ska kunna bedrivas.

Ett NIS2 direktiv kom under 2022 och ska implementeras i svensk lag under 2024. Genom NIS2 direktivet kommer hela regionen att omfattas, inte bara hälso- och sjukvården och folktandvården. Ytterligare krav kommer således att ställas gällande kontinuitet för det systematiska och riskbaserade arbetet.

Parallellt med detta kommer också det så kallade CER- direktivet som ska implementeras på ett samordnat sätt med NIS2-direktivet. CER-direktivet ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet

8.3 Lämplighetsbedömning vid utkontraktering av it-drift

Tillgång till säker och effektiv it-drift är en grundläggande förutsättning för att regionen ska kunna bedriva en ändamålsenlig verksamhet. Detta tillgodoses genom att regionen utkontrakterar delar av sin it-drift till externa tjänsteleverantörer. Utkontrakteringen kan exempelvis innebära tillhandahållande av teknisk infrastruktur eller teknisk plattform, it-system eller it-baserade funktioner. Vid utkontrakteringen tillgängliggörs i regel en stor mängd uppgifter för tjänsteleverantören. En sekretess--belagd uppgift som görs tillgänglig för en extern tjänsteleverantör betraktas som utlämnad eller röjd i offentlighets- och sekretesslagens mening. Ett sådant röjande är bara tillåtet om inte sekretess hindrar att uppgiften lämnas ut. Av den sekretess-brytande regeln i 10 kap. 2 a § offentlighet- och sekretesslagen följer dock att sekretess inte hindrar ett tillgängliggörande eller utlämnande av uppgifter till en extern tjänsteleverantör som av regionen getts i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.

Detta innebär att regionen, innan utkontraktering ska genomföra en lämplighets-bedömning och pröva om det finns skäl som talar för att ett utlämnande inte bör ske. Genomförda avvägningar och bedömningar bör dokumenteras, i synnerhet om utlämnandet omfattar en större informationsmängd och/eller information av känslig karaktär. En mall har tagits fram för att genomföra lämplighetsbedömning som kommer att implementeras under 2024 i det systematiska informations-säkerhetsarbetet.

8.4 Nytt vårdinformationsstöd, Cosmic

Framtidens vårdinformationsstöd är en helhetslösning som omfattar grundläggande stöd för vårddokumentation, vårdadministration och läkemedel, stöd för operationsplanering, anestesi/intensivvård, obstetrik, cytostatika samt drifttjänst, support och underhåll. Det nya vårdinformationssystemet ska införas i regionen under 2024 och informationssäkerhetsarbetet kommer att behöva löpa på parallellt med detta.

8.5 Upphandling och kravställning

Informationsklassning och riskanalys ska alltid föregås av en upphandling eller anskaffning då kraven för den informationsmängd som ska hanteras är specifik. En del av de krav som framkommer utifrån en informationsklassning kan ses som generella krav och kan därför hanteras på ett enklare sätt.

Ett arbete startades under 2022 gällande generell kravställning kopplat till informationssäkerhet vid upphandling och anskaffning inom regionen. Arbetet sker genom grupparbete där it-säkerhetsansvarig, informationssäkerhetssamordnare, upphandlingsjurist, informationssäkerhetshandläggare hälso- och sjukvården samt representanter från Regionservice Medicinsk teknik deltar. Detta arbete är fortsatt pågående under 2024 i syftet att utveckla kravställning i samband med informations-klassning och riskanalyser inför upphandling.