Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

ANMÄLAN
2023-02-01

SLSO 2023-0500

Årsrapport informationssäkerhet för verksamhetsåret 2022

Årsrapport informationssäkerhet för verksamhetsåret 2022 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2023-01-27

Diarienr 2023-0500

Årsrapport informationssäkerhet

För verksamhetsåret 2022

Innehållsförteckning

1. Inledning 3

2. Informationssäkerhetsorganisation 3
2.1 Bedömning 3
2.2 Åtgärd 4

3. Identifiering av skyddsvärd information 4
3.1 Bedömning 4
3.2 Åtgärd 4

4. Utbildning 5
4.1 Bedömning 5
4.2 Åtgärd 5

5. Compliance – regelefterlevnad 5
5.1 Bedömning 6
5.2 Åtgärd 6

6. Styrdokument 6
6.1 Bedömning 7
6.2 Åtgärd 7

7. Incidenthantering 7
7.1 Bedömning 8
7.2 Åtgärd 8

8. NIS-anpassning 8
8.1 Bedömning 9
8.2 Åtgärd 9

9. Konklusion 9

1. Inledning

I detta dokument redovisas Stockholms läns sjukvårdsområdes (SLSO) informationssäkerhetssamordnares iakttagelser och arbete under verksamhetsåret 2022.

2. Omvärldsbevakning

Rådande situation i omvärlden med konflikten i Ukraina och Sveriges NATO-ansökan har medfört en förändrad hotbild mot informationshanteringen inom myndigheten som leverantör av samhällsviktiga tjänster.

2.1 Bedömning

Region Stockholms CERT (Computer Emergency Response Team) har i dagsläget inte sett någon ökning i antagonistisk aktivitet, t.ex. ökat antal virusangrepp.

2.2 Åtgärd

SLSO:s informationssäkerhetssamordnare håller sig uppdaterade genom att bland annat ingå i Regions Stockholms informationssäkerhetsråd samt regelbundna avstämningar med Region Stockholms CERT.

3. Informationssäkerhetsorganisation

För att underlätta och förbättra det systematiska arbetet med informationssäkerhet behöver SLSO skapa en organisation med koordinatorer på vårdområdesnivå och i stödjande verksamhet.

Tillsammans med informationssäkerhetssamordnaren och Dataskyddsombudet (DSO) ska dessa koordinatorer samordna arbetet med informationssäkerhet samt arbete kopplat till dataskyddsförordningen inom respektive vårdområdesnivå och stödjande verksamhet.

3.1 Bedömning

Under verksamhetsåret 2022 har arbetet med att etablera en dataskyddsorganisation tillsammans med SLSO:s DSO påbörjats i den verksamhetsstödjande verksamheten. Dataskyddskoordinatorer har utsetts och inledande utbildning genomförts.

Struktur för organisationens funktion och genomförande framtagen.

3.2 Åtgärd

Förberedande och genomförande av utbildningsinsatser för kärnverksamheten.

Förberedande och genomförande av planerade aktiviteter för redan utbildade koordinatorer

4. Identifiering av skyddsvärd information

Skyddsvärd information inom SLSO behöver identifieras och klassificeras i syfte att värdera informationen så att tillräcklig nivå av säkerhetsåtgärder finns kopplat till respektive informationsskälla. Detta arbete ger SLSO en ökad trygghet gällande informationstillgångarnas tillgänglighet, riktighet och konfidentialitet.

Arbetet med att driva kartläggningen av SLSO:s digitala verktyg med alla system/applikationer/verktyg har under verksamhetsåret 2022 hanterats inom verksamhetsstöd Digitala tjänster.

4.1 Bedömning

En kartläggning med förslag till prioritering av SLSO:s digitala verktyg har tagits fram och presenterats för SLG.

Arbetet med att kvalitetssäkra kartläggningen och prioriteringen av de digitala verktygen har påbörjats under ledning av SLSO:s informationssäkerhetssamordnare.

4.2 Åtgärd

Verksamhetsstödet Digitala tjänster har under året drivit kartläggningen av SLSO:s digitala verktyg med syfte att skapa kontroll genom en gemensam ”kartbild” över digitala verktyg.

Kartläggningen kvalitetssäkras genom representanter för kärnverksamhet och verksamhetsstöd.

Målbilden är att alla system/applikationer/verktyg som används på SLSO ska vara omhändertagna och det gäller:

- både kärnverksamhet och verksamhetsstöd
- såväl lokala, regionala som nationella
- indelade i logiska områden utifrån vilken verksamhetsförmåga tekniken stödjer
- omhändertagna vilket är att likställa med att de är förvaltade på ändamålsenligt sätt

5. Utbildning

SLSO:s medarbetare ska visa upp en medvetenhet och ett kunnande gällande informationssäkerhet vilket medför att utbildning och kommunikation måste vara en integrerad del i all utveckling och implementation av ett systematiskt informationssäkerhetsarbete.

Datorstödd informationssäkerhetsutbildning för användare (DISA) är Region Stockholms grundutbildning i informationssäkerhet vilken även är obligatorisk för alla medarbetare inom Region Stockholm. DISA-utbildningen är ett led i att öka medvetenheten och kunskapen om informationssäkerhet och SLSO ska arbeta för att alla medarbetare genomför utbildningen.

5.1 Bedömning

En grundlig genomgång av statistiken bakom genomförandegraden genomfördes vilket presenterats för SLSO:s ledningsgrupp. Informationssäkerhetssamordnarna har under 2022 arbetat aktivt med att följa upp genomförandegraden i verksamheterna och informera om utbildningen samt att den är obligatorisk att genomföra.

Genomförandegraden för SLSO:s medarbetare är dock fortsatt förhållandevis låg, 57% har genomfört utbildningen per januari 2023 jämfört med 48% januari 2022.

SLSO når inte upp till de mål som är satta för DISA i Riktlinjen för informationssäkerhet (4.4.2).

5.2 Åtgärd

Informationssäkerhetssamordnarna kommer att fortsätta den aktiva uppföljningen av genomförandegraden i verksamheterna och genomföra ytterligare informationssatsningar.

6. Compliance – regelefterlevnad

Målet med compliance-processen är att stödja SLSO att verka i enlighet med gällande policy och riktlinjer för informationssäkerhet. Genom att tillämpa compliance-processen kan avvikelser och brister upptäckas i ett tidigt skede och den faktiska informationssäkerheten i SLSO:s verksamheter och IT-miljöer förbättras. Ett systematiskt

informationssäkerhetsarbete bidrar ytterst till att minska risken för verksamhetsstörningar.

Compliance-processen används av SLSO för att kontrollera så kallad regelefterlevnad.

Användningsområden för compliance-processen är:

- Strategisk styrning – Används för egenkontroll och för att identifiera förbättringsåtgärder av SLSO:s informationssäkerhet ur ett styrnings- och ledningsperspektiv.
- Verksamhet – Används för att genomföra egenkontroll av den administrativa informationssäkerheten hos en verksamhet
- IT-system – Används för att genomföra egenkontroll av ett IT-systems informationssäkerhet samt för att identifiera och genomföra åtgärder för förbättring av IT-säkerheten.
- Driftmiljö – Används för att bedöma informationssäkerheten i en driftmiljö.
- Datahallar och IT-utrymmen – Används för att bedöma skalskyddet av datahallar och IT-utrymmen.
- Upphandling – Används för att filtrera ut krav vid upphandling

6.1 Bedömning

Arbetet med regelefterlevnadsgranskningar av såväl IT-system som verksamheter inom ramen för Compliance-processen har fortskridit enligt den framtagna handlingsplanen för verksamhetsåret 2022, där de uppsatta målen är uppnådda och mer därtill. Likaså gällande strategisk styrning.

6.2 Åtgärd

Arbetet med regelefterlevnadsgranskningar fortsätter enligt handlingsplan för kommande år.

7. Styrdokument

Styrdokument är viktig del av arbetet med informationssäkerhet då arbetet utgår från dessa samt att SLSO måste kunna visa att organisationen lever upp till riktlinje och policy för informationssäkerhet.

SLSO:s arbete med informationssäkerhet utgår från följande styrande dokument:

- Region Stockholms Verksamhetsskyddspolicy
- Riktlinjer för informationssäkerhet inom Region Stockholm

De vägledande dokumenten är:

- Vägledning – systematiskt arbete med informationssäkerhet
- Vägledning till riktlinjer för informationssäkerhet
- Vägledning Compliance-processen
- Vägledning för riskhantering informationssäkerhet
- Instruktion för informationsklassificering
- E-postanvändning – övergripande anvisning för SLSO

För att SLSO ska kunna bedriva ett systematiskt och kvalitativt informationssäkerhetsarbete krävs att relevant information finns lättillgänglig för alla medarbetare därav finns samtliga styrdokument samlade för anställda att ta del av på intranätet samt i ärende- och dokumenthanteringssystemet Platina.

7.1 Bedömning

SLSO:s informationssäkerhetssamordnare bedömer att 2021 års beslut att frångå den egna riktlinjen och policyn och istället följa de regionalt framtagna styrdokumenten har underlättat arbetet med samordning såväl som arbete med verksamheten. Detta då antalet styrande och stödjande dokumentation minskat och har en gemensam inriktning över hela Region Stockholm.

7.2 Åtgärd

Informationssamordnarna ser för närvarande inget behov av åtgärder med avseende på styrdokument förutom årlig revidering i enligt processen i Platina.

8. Incidenthantering

Incidenthantering via Helpdesk omfattar alla händelser som stör eller kan störa IT-miljön oavsett om händelsen sker hos SLSO eller underleverantör. Detta inkluderar händelser som rapporteras in såväl av användarna som av tekniker som upptäcker avvikelser från normal IT-drift.

Inkommande incidenter anses vara en informationssäkerhetsincident vid en klassificering av 1 (kritisk) eller 2 (hög) enligt fastställd prioriteringsmatris som HelpDesk använder sig av. Prioriteringar sker enligt en femgradig skala vilken baseras på incidentens angelägenhet och påverkan för vårdgivare och patientsäkerhet. Prioritering görs i första linjens support och kan vid behov ändras av en incident manager (IM).

Personuppgiftsincidenter rapporteras av verksamheten direkt till Integritetsskyddsmyndigheten (IMY) och dataskyddsombud informeras i

samband med rapportering. Förutom den årliga återrapporteringen rapporteras även uppkomna personuppgiftsincidenter i anslutning till ledningsgruppsmöten.

8.1 Bedömning

Bedömningen är att SLSO:s incidenthantering lever upp till de krav som ställs i avsnitt 13.1 i riktlinjen för informationssäkerhet. Det vill säga att SLSO har processer och rutiner för att hantera händelser och sårbarheter som kan utgöra ett hot mot SLSO:s informationstillgångar.

Likt föregående år så kan det konstateras att det inte finns ett specifikt systemstöd när det gäller informationssäkerhetsincidenter. Ett sådant stöd skulle eventuellt göra det lättare för informationssäkerhetssamordnaren att arbeta mer med analyser av förekomna incidenter. SLSO:s informationssäkerhetssamordnare följer utvecklingen på regional nivå där bedömning är att det behövs en regional samordning snarare än lokala initiativ kring denna fråga.

Under 2022 har även IT-stödet HändelseVis börjat användas i liten utsträckning för informationssäkerhetsincidenter. Informationssäkerhetssamordnarna har haft avstämning med objektspecialisterna för HändelsVis under senare del av 2022.

8.2 Åtgärd

Informationssäkerhetssamordnarna håller sig uppdaterade kring utvecklingen på regional nivå om eventuella IT-stöd för incidenthantering. I tillägg fortsätter informationsspridning att även HändelseVis är en rapporteringskanal när det gäller incidenter.

9. NIS-anpassning

Den svenska NIS-regleringen, lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, trädde i kraft 2018 och innebär i korthet krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga- och vissa digitala tjänster.

Tjänster som omfattas av NIS-direktivet delas in i samhällsviktiga tjänster och digitala tjänster. Samhällsviktiga tjänster är tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. De är indelade i sju sektorer: bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt transport.

SLSO är en leverantör av samhällsviktiga tjänster inom sektorn hälso- och sjukvård. För samhällsviktiga och digitala tjänster inom hälso- och sjukvårdssektorn är Inspektionen för vård och omsorg (IVO) tillsynsmyndighet. Anmälningsskyldigheten är ett lagkrav.

9.1 Bedömning

SLSO:s informationssamordnare har haft NIS-anpassning som fokusområde under den senare delen av 2022, vilket har inneburit framtagande av process för incidentrapportering enligt de tre skeden som föreskrivs i NIS-direktivet men även deltagande i aktiviteter kring kartläggning och prioritering av SLSO:s digitala verktyg och tjänster.

9.2 Åtgärd

Fortsatt arbete med NIS-anpassning kommer att innebära vidare arbete med att säkra att adekvata analyser och säkerhetsåtgärder är tillämpade enligt den färdigställda kartläggningen och dess ingående prioriteringsnivåer. Löpande uppföljning av arbetet sker i SLSO:s IT-säkerhetsforum.

10.Konklusion

Det krävs fortsatt fokus på att öka medvetenhetande och kunnandet inom organisationen genom utbildningsinsatser och att få till stånd en ökning av den fortsatt förhållandevis låga genomförandegraden av den obligatoriska utbildningen, DISA.

Etableringen av en informationssäkerhetsorganisation i syfte att bygga upp lokala stöd- och resurspersoner som påbörjats under 2022 kommer att fortskrida under 2023.

Arbetet med NIS-anpassning kommer även under 2023 vara ett särskilt fokusområde för informationssäkerhetssamordnarna för att tillse att SLSO kan leva upp till de lagkrav direktivet föreskriver.

I övrigt har arbetet med informationssäkerhet har fortlöpt enligt den framtagna handlingsplanen för åren 2021–2024. Som en del av handlingsplanen genomförs kontinuerligt regelefterlevnadsgranskningar av såväl IT-system som verksamheter inom ramen för den s.k. Compliance-processen i syfte att säkerställa så att SLSO lever upp till Region Stockholms riktlinje och policy för informationssäkerhet. Handlingsplanen för informationssäkerhet revideras och uppdateras årligen.

Rapporteringssätt och regelbundenhet av detsamma kan utökas och utvecklas om SLSO:s nämnd så önskar.

Stockholm, januari 2023

Sara Daniels-May
Informationssäkerhetssamordnare

Henrik Strand
Informationssäkerhetssamordnare