Stockholms läns sjukvårdsområde
Sjukvårdsdirektören

ANMÄLAN
2022-01-18

SLSO 2022-0300

Årsrapport informationssäkerhet för verksamhetsåret 2021

Årsrapport informationssäkerhet för verksamhetsåret 2021 överlämnas till nämnden för Stockholms läns sjukvårdsområde för kännedom.

Region Stockholm

Stockholms läns sjukvårdsområde

ÅRSRAPPORT
2022-01-27

Diarienummer
SLSO 2022-0300

Årsrapport informationssäkerhet

För verksamhetsåret 2021

Innehållsförteckning

1. Inledning 3

2. Informationssäkerhetsorganisation 3
2.1 Bedömning 3
2.2 Åtgärd 3

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

4. Utbildning 4
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. Incidentrapportering 7
7.1 Bedömning 8
7.2 Åtgärd 8

8. Omvärldsbevakning ..... **Fel! Bokmärket är inte definierat.**
8.1 Bedömning ..... **Fel! Bokmärket är inte definierat.**
8.2 Åtgärd ..... **Fel! Bokmärket är inte definierat.**

9. Konklusion 8

1. Inledning

I detta dokument redovisas SLSO:s informationssäkerhetssamordnares iakttagelser och arbete under verksamhetsåret 2021. Ett verksamhetsår präglat av den pågående pandemin och föräldraledighet.

2. Informationssäkerhetsorganisation

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

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

2.1 Bedömning

Givet en förhoppning att den ansträngda arbetssituationen under pågående covid-19 pandemi förbättras så behöver DSO driva på arbetet i skapandet av en dataskyddsorganisation tillsammans med SLSO:s informationssäkerhetssamordnare. Arbetet påbörjas lämpligen inom de mer administrativa verksamhetsstöden inom SLSO för att sedan spridas inom kärnverksamheten när så bedöms lämpligt.

SLSO:s externa revisorer (Bureau Veritas) delade uppfattningen att etablering av en organisation likt detta är viktigt för det systematiska arbetet med informationssäkerhet och dataskydd.

2.2 Åtgärd

Förbereda utbildningsinsatser för stödjande verksamhet så att arbetet kan påbörjas så snabbt det bedöms lämpligt.

3. 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.

3.1 Bedömning

Under 2020 togs en förteckning över SLSO:s IT-system fram i samarbete med VS eHälsa & IT och verksamhetsbaserad informationsredovisning (VIR)-projektet. Förteckningen behöver bearbetas ytterligare i syfte att identifiera och prioritera system utifrån skyddsvärdet på informationen som behandlas. Bedömningen är att den kartläggning som gjordes inte blev heltäckande och att det kan finnas luckor i förteckningen varpå ett omtag i detta arbete gjorts. Arbetet med att driva kartläggningen av SLSO:s digitala verktyg med alla system/applikationer/verktyg hanteras inom verksamhetsstödet e-Hälsa. En komplett förteckning av SLSO:s digitala verktyg gör att SLSO uppnår målen i Riktlinjen för informationssäkerhet 1.4.2 vilket är viktigt och grundläggande för det systematiska informationssäkerhetsarbetet.

Verksamhetsåret innebar en del uppdateringar av styrande och stödjande dokumentation från RLK inom området för informationssäkerhet där den regiongemensamma instruktionen för informationsklassificeringen (RS 2021–1018) bedöms underlätta arbetet med att bedöma informationsvärdet. Systemen ska granskas enligt compliance-processen (RS 2021–1019).

3.2 Åtgärd

Verksamhetsstödet e-Hälsa har under året påbörjat kartläggningen av SLSO:s digitala verktyg. Utifrån en sådan kartläggning kan arbetet med att identifiera och bedöma information påbörjas. I syfte att skapa kontroll så skapas en gemensam ”kartbild” över digitala verktyg med målbilden att alla system/applikationer/verktyg som används på SLSO är omhändertagna och det gäller:

- både kärnverksamhet och verksamhetsstöd
- omhändertagna =förvaltade på ändamålsenligt sätt
- gäller såväl lokala, regionala som nationella
- indelade i logiska områden utifrån vilken verksamhetsförmåga tekniken stödjer

4. 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.

4.1 Bedömning

Genomförandegraden för SLSO:s medarbetare för den obligatoriska DISA-utbildningen är förhållandevis låg, för åren 2017–2021 är genomförandegraden 47 %[1]. Under 2020 och 2021 har genomförandegraden varit 10%. SLSO når inte upp till de mål som är satta för DISA i Riktlinjen för informationssäkerhet (4.4.2).

Den låga genomförandegraden bekräftades även under den externa revisionen som genomfördes under hösten 2021vilket genererade en mindre avvikelse inom ramen för den re-certifiering SLSO genomgick.

Under 2021 har det funnits ett begränsat kommunikationsutrymme på grund av prioritering av covid-19 relaterad information.

4.2 Åtgärd

Året startar med en grundlig genomgång av statistiken bakom genomförandegraden för att bättre förstå grundorsak till den låga genomförandegraden samt lämpliga korrigerande åtgärder. Detta arbete kommer presenteras för SLSO:s ledningsgrupp.

5. 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.

Användningsområdet är för compliance-processen är

[1] Baserat på 12 000 anställda

- 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.

5.1 Bedömning

Arbetet med regelefterlevnadsgranskningar av såväl IT-system som verksamheter inom ramen för Compliance-processen har fortskridit enligt den framtagna handlingsplanen för verksamhetsåret 2021, där de uppsatta målen är uppnådda och mer därtill. Likaså gällande strategisk styrning.

5.2 Åtgärd

Arbetet med regelefterlevnadsgranskningar fortsätter enligt handlingsplan för kommande år.

6. 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 dokumenthanteringssystemen Platina.

6.1 Bedömning

Sent under året 2021 fastslogs de styrande dokumenten för informationssäkerhet med tillämpliga vägledande dokument. SLSO:s informationssäkerhetssamordnare bedömer beslutet att frångå den egna riktlinjen och policyn och istället följa de regionalt framtagna styrdokumenten kommer underlätta arbetet med samordning såväl som arbete med verksamheten. Detta då antalet styrande och stödjande dokumentation minskar och har en gemensam inriktning över hela Region Stockholm.

6.2 Åtgärd

SLSO:s policy och riktlinje för informationssäkerhet har arkiverats då nämnden nu på ett tydligare sätt följer de styrande dokument som är beslutade av regionfullmäktige. En översyn av de styrande dokumenten i syfte att identifiera om behov finns av förtydliganden eller lokala anpassningar för implementering inom SLSO.

7. 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 så rapporteras uppkomna personuppgiftsincidenter i anslutning till ledningsgruppsmöten.

7.1 Bedömning

I december upptäcktes säkerhetshålet Log4shell och SLSO blev omgående informerade av Region Stockholm CERT gällande denna sårbarhet. Sårbarheten tilldelades CVSS värdet 10, vilket är det högsta värdet som kan tilldelas en sårbarhet.
Sårbarheten finns i Java-biblioteket (Log4j) vilket är ett vanligt förekommande verktyg som används för att logga anrop mot tjänster. En lyckad exploatering av sårbarheten kan innebära att godtycklig kod exekveras på servrar, system och tjänster inom Region Stockholm och skulle kunna innebära att dessa skulle kunna bli kompromitterade i syfte att exfiltrera data eller användas i en senare attack.

Bedömningen är att det regionala samarbetet för att hantera denna mycket allvarliga sårbarhet fungerade väldigt väl och det finns en del lärdomar att ta med sig. Däribland kan det konstateras att det är av mycket stor vikt att alla system är dokumenterade så att det snabbt går att kartlägga till exempel systemsamband och vilka utvecklingsplattformar som används (t.ex. Java). Detta arbete pågår som nämnts ovan inom VS eHälsa inom ramen för det arkitektforum som etablerats.

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.

7.2 Åtgärd

Informationssäkerhetssamordnarna håller sig uppdaterade kring utvecklingen på regional nivå om eventuella it-stöd för incidenthantering.

8. Konklusion

Det krävs fortsatt fokus på att öka medvetenhetande och kunnandet inom organisationen genom utbildningsinsatser och framför allt en ökad förståelse till anledningen bakom den låga genomförandegraden av den obligatoriska utbildningen, DISA.

Arbetet med utformningen av en informationssäkerhetsorganisation i syfte att bygga upp lokala stöd- och resurspersoner har försenats på grund av

covid-19 och föräldraledighet, det kan konstateras att förseningen har haft negativ inverkan på framfarten för arbetet inom området. Detta kommer följas upp under 2022.

Arbetet med informationssäkerhet har i övrigt fortskridit 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.

Arbetet med att driva kartläggningen av SLSO:s digitala verktyg med alla system/applikationer/verktyg hanteras numera inom verksamhetsstödet e-Hälsa. Kartläggningen gör att SLSO uppnår målen i Riktlinjen för informationssäkerhet 1.4.2 vilket är ett stort steg framåt i informationssäkerhetsarbetet.

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

Stockholm, januari 2022

Sara Daniels-May
Informationssäkerhetssamordnare

Henrik Strand
Informationssäkerhetssamordnare