Gävle KOMMUN

24AFN11, 24SON10, 24ON16

Årsrapport informationssäkerhetsarbete 2023

Redogörelse för informationssäkerhetsarbetet inom Välfärd Gävle

2024-01-08

Förord

Denna årsrapport redogör övergripande för informationssäkerhetsarbetet inom sektor Välfärd, Gävle kommun. En stor del av informationssäkerhetsarbetet sker i det dagliga arbetet i linjeorganisationen. Den här rapporten tar snarare fokus på de andra operativa och strategiska insatser som sker från centralt håll hos Välfärd Gävle.

2024-01-08

Anita Härdelin
Informationssäkerhetssamordnare
Välfärd Gävle

Adrian Henriksson Severin
Övergripande informations-
säkerhetssamordnare (CISO)
Gävle kommunkoncern

Innehåll

Inledning

Kommunfullmäktige har beslutat om en policy för informationssäkerhet som säger att kommunens verksamheter ska bedriva ett systematiskt informationssäkerhetsarbete. Viss verksamhet i sektor Välfärd, hälso- och sjukvård, omfattas även av EU-direktivet Network Information Security, NIS samt nationell lagstiftning i form av Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Arbetet med att etablera systematiskt informationssäkerhetsarbete inom sektor Välfärd startade 2022 genom att en informationssäkerhetssamordnare (ISS) tillsattes. Hen har under 2023 arbetat heltid med informationssäkerhet och tillsammans med kommunens övergripande informationssäkerhetssamordnare (CISO).

Målsättningen med denna årsrapport är att beskriva vad vi hittills har åstadkommit men också belysa viktiga aktiviteter som behöver prioriteras i det fortsatta arbetet.

Om informationssäkerhetsarbetet inom Välfärd Gävle

Vid start av 2022 bemannades rollen som ISS vid Välfärd Gävle. Arbetet med att etablera ett systematiskt informationssäkerhetsarbete för sektorns verksamheter och implementera den svenska lagstiftningen från 2018 utifrån NIS-direktivet påbörjades av Informationssäkerhetssamordnare med stöd av CISO. Arbetet under 2023, med fortsatt etablering har skett mer och mer självständigt av Informationssäkerhetssamordnare och vid behov med stöd av CISO. ISS har under året deltagit i flera digitala utbildningar och seminarier i syfte att öka kompetensen på området för sektor Välfärd.

En ny Dataskyddssamordnare (DSS) tillträdde i början på 2023 och ett gott samarbete har utvecklats.

För det systematiska informationssäkerhetsarbetet tillämpas en ledningsmodell framtagen av Myndigheten för samhällsskydd och beredskap (MSB). Del ett, Identifiera och analysera har slutförts under året och delarna två och tre, Utforma och Använda pågår med avslutade och pågående aktiviteter som redovisas längre fram i rapporten.

GAP-analys

GAP-analyserna har genomförts med stöd av MSB:s verktyg ”Infosäk-kollen” och bör genomföras vart annat år. ISS ville ändå genomföra en GAP-analys även för 2023 för att se hur långt sektorn kommit i arbetet med etableringen.

Verktyget består av 40 frågor på 4 olika nivåer. På varje fråga finns olika alternativ beroende på om/i vilken omfattning det systematiska informationssäkerhetsarbetet bedrivs inom organisationen. Varje fråga kan ge poäng mellan 0 och 5 beroende på vilket svar som ges.

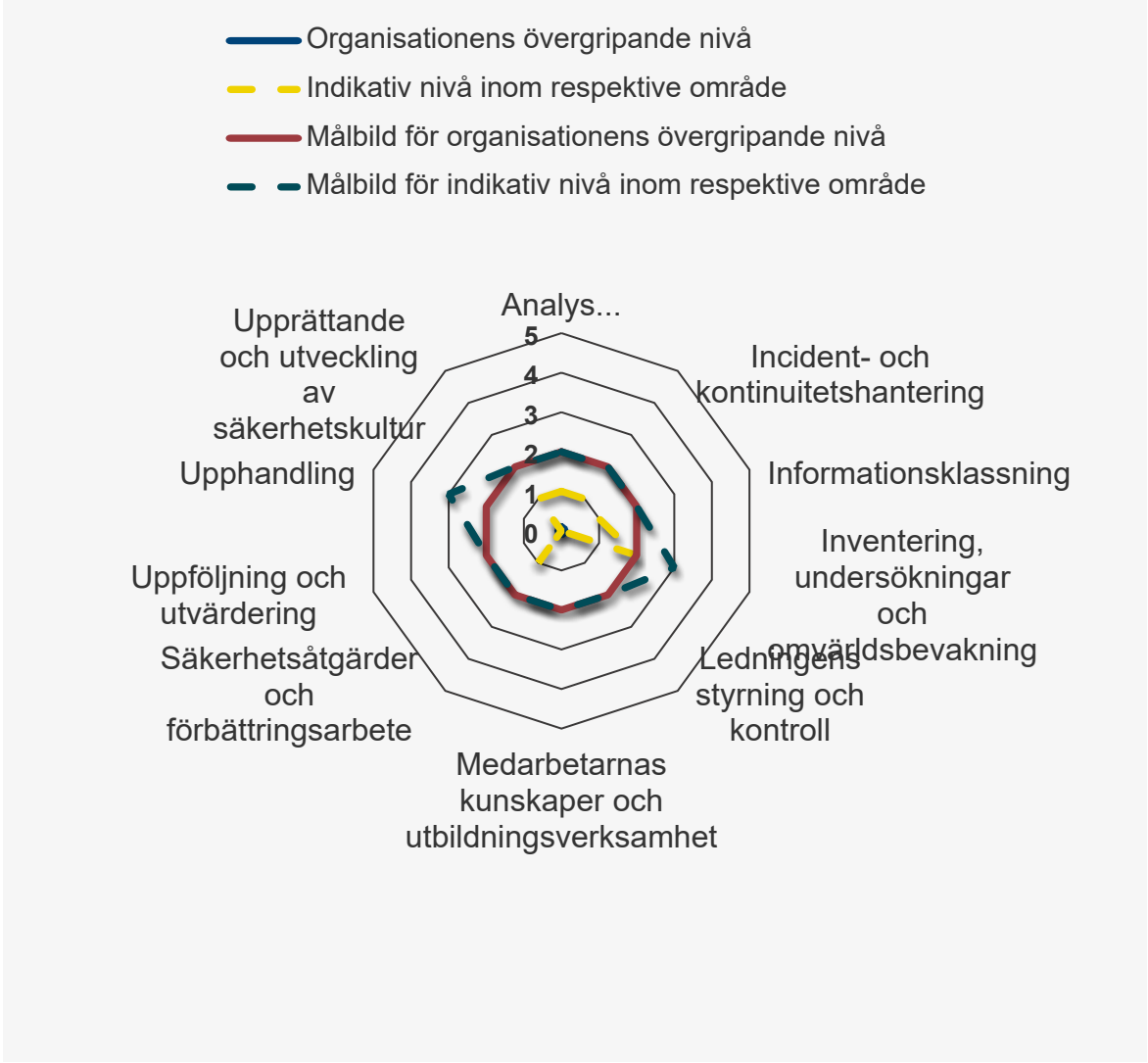
Resultatet visar på en liten positiv utveckling av det systematiska informationssäkerhetsarbetet. Dock har inte CISO:s mål uppnåtts.

Områden som har erhållit låga eller inga poäng och där en hel del arbete återstår är:

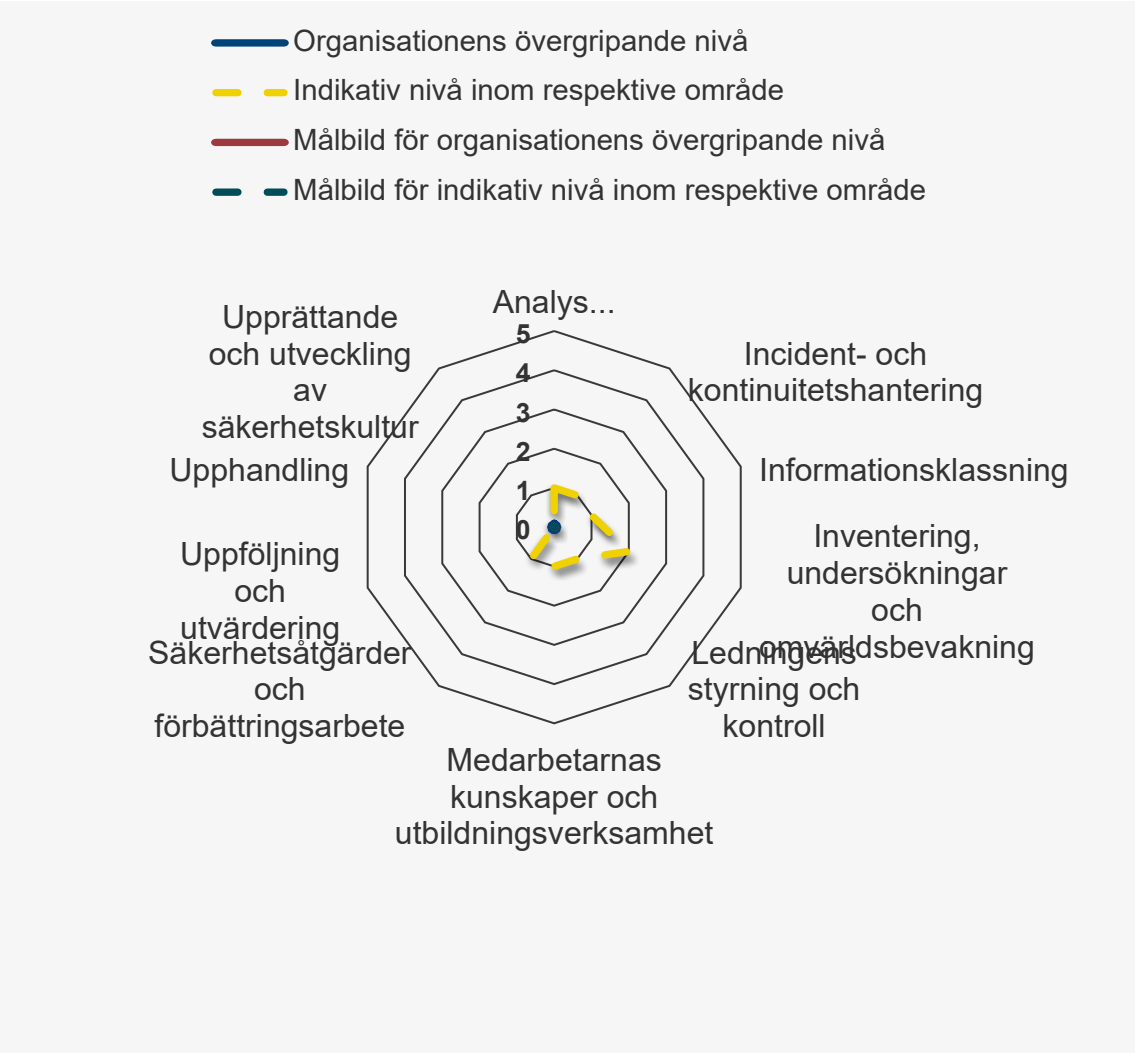
- Mål och inriktning för informationssäkerhetsarbetet*
- Inventering av system och nätverk samt informationssäkerhetsklassning av samtliga system och nätverk.
- Informationsägare – etablering av rollen
- Utbildning samt medarbetarnas kunskap om och agerande informationssäkert, informationssäkerhetskultur
- Kontinuitetshantering – beskrivning och regelbunden uppföljning
- Ledningens engagemang och uppföljning av informationssäkerhetsarbetet*
- Upphandling och uppföljning av leverantörer och deras leveranser*
- Riskhantering - analys, genomförande och utvärdering om åtgärd gav önskad effekt

*kommer som krav och lag i och med NIS2

Gap-analys 2022



GAP-analys 2023



Omvärldsbevakning

Cybersäkerhet

Den tekniska utvecklingen och digitaliseringen går snabbt. Säkerheten har inte följt med i samma tempo. Det innebär att både enskilda organisationer och hela samhället blir sårbart för olika cyberhot. För att uppnå en så god cybersäkerhet som möjligt är viktigt att arbeta både proaktivt och reaktivt. I dag är många IT-system inte längre enbart ett stöd för verksamheten, utan en förutsättning för att verksamheten ska fungera. Det finns också ett större beroende mellan olika IT-system i dagens samhälle. Dessa beroenden sträcker sig både inom och mellan organisationer och mellan länder. Därför är det viktigt för både privat och offentlig verksamhet att förebygga och åtgärda säkerhetsbrister i verksamhetskritiska

system. Att vara medveten om hur hoten ser ut och vad som går att göra för att skydda viktiga data och information är en nationell angelägenhet.[1]

Europeiska rådet/Europeiska unionens råd skriver att med mer än 10 terabyte data stulna varje månad är **utpressningsprogram ett av de största cyberhoten i EU**, och nätfiske är det vanligaste sättet på vilket sådana attacker inleds. DDoS-attacker hör också till de största hoten. Den årliga kostnad som it-brottsligheten åsamkar den globala ekonomin beräknas ha uppgått till **5,5 biljoner euro** i slutet av 2020, vilket är dubbelt så mycket som 2015.[2]

Rysslands militära aggression mot Ukraina har förändrat hotbilden i Europa under 2022. Konflikten har mobiliserat många hacktivister, cyberbrottslingar och statsstödda grupper.

Sjukvården har hamnat i cyberbrottslingarnas fokus och under de senaste sex månaderna och är den sektor som är hårdast drabbad av attacker i Sverige enligt statistik från säkerhetsföretaget Check Point. Och attackerna har ökat rejält under året. När Check Point lade fram sin halvårsstatistik i februari låg cyberattackerna på i snitt 662 i veckan och sjukvården hamnade på sjätte plats. Det senaste halvåret har attackerna ökat till i snitt 1 071 i veckan. Det är fler än myndigheter och försvar som i snitt utsätts för 1 059 attacker i veckan.[3]

Informations- och cybersäkerhet står högt upp på regeringens agenda. Regeringen har under 2023 inlett arbetet med att ta fram en ny informations- och cybersäkerhetsstrategi. Med en ny nationell strategi, som en del av implementeringen av NIS2-direktivet, finns förutsättningar att knyta samman satsningar nationellt, inom EU och inför ett svenskt Natomedlemskap.

Riksrevisionen menar att regeringens styrning av samhällets informations- och cybersäkerhet − både brådskande och viktig (RiR 2023:8) Digitaliseringen har slagit igenom i alla samhällssektorer på alla nivåer. Det ökar behovet av informations- och cybersäkerhet. Cybersäkerhetshotet sägs också öka. Ansvaret för att hantera riskerna, hoten och sårbarheterna samt öka säkerheten är delat, både inom Regeringskansliet och mellan

[1] 31 maj 2022, Myndigheten för samhällsskydd och beredskap, www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/
[2] www.consilium.europa.eu

[3] 22 nov 2023, Computer Sweden, computersweden.idg.se/2.2683/1.780449/cyberattackerna-okar-varden-extra-utsatt?utm_source=dmdelivery&utm_medium=email&utm_campaign=CS%20FIRST%20LOOK%20-%20Morning%202023%202023-11-23%2011%3A19%3A41

myndigheter. I regeringens informations- och cybersäkerhetsstrategi beskrivs ett antal målsättningar för arbetet. Sex år efter dess införande finns det fortfarande problem inom strategins samtliga områden. Riksrevisionen har därför granskat om regeringens arbete för att stärka Sveriges informations- och cybersäkerhet har varit effektivt. Riksrevisionens övergripande slutsats är att regeringens arbete inom området inte har varit det. Den centrala bristen är avsaknad av strategiska avvägningar och prioriteringar som inriktar informations- och cybersäkerhetsarbetet. Ett tydligt exempel på brister i strategiska avvägningar är hur Sverige arbetar med frågorna i och gentemot EU. Arbetet i EU bedrivs i hög takt och om Sverige inte är med och påverkar det arbetet tidigt är risken stor att det internationella regelverket inte gynnar svenska intressen i samma utsträckning som annars hade varit möjligt. [4]

Advenica skriver att kommunerna är särskilt utsatta för riskerna med digitaliseringen då de även ansvarar för många andra samhällsviktiga funktioner. En cyberattack kan därför resultera i stora samhälleliga effekter. Trots detta har sju av tio blivit utsatta och närmare nio av tio kommuner är oroliga för att bli utsatta för en cyberattack. Samtidigt är en hög andel osäkra kring sin kommuns förmåga att klara en cyberattack och två tredjedelar av de säkerhetsansvariga upplever att cybersäkerheten inte tas på tillräckligt stort allvar bland de kommunanställda tjänstemännen.[5]

Voister skriver att 44 procent av kommuner och regioner är utsatta för cyberattacker [6]

Enligt Verizon beror cirka 82 % av cyberintrången under 2022 på ett mänskligt fel. Den mänskliga faktorn fortsätter att vara en av de stora anledningarna bakom cyberattackerna på företag och organisationer. Medarbetares oförmåga att identifiera olika typer av cyberhot, som exempelvis nätfiske, gör att de är sårbara och lätt blir måltavlorna för cyberkriminella. Trenden av den mänskliga faktorn som ett av de största cyberhoten för verksamheter fortsätter under 2023.[7]

[4] 27 april 2023, Riksrevisionen, www.riksrevisionen.se/rapporter/granskningsrapporter/2023/regeringens-styrning-av-samhallets-informations--och-cybersakerhet---bade-bradskande-och-viktig.html
[5] 5 april 2023, Advenica, Kommunerna är inte förberedda på cyberattacker | Advenica
[6] 27 mars 2023, uppdaterad 2 otober 2023, Voister, 44 procent av kommuner och regioner utsatta för cyberattacker - Voister
[7] 1 februari, Team Tinia, tinia.se/insights/cybersäkerhetstrender-år-2023-den-mänskliga-faktorn

Cyberattacker i Sverige

Under året har vi läst om andra svenska verksamheter som drabbats av cyberattacker, och några exempel som hänt under november och december är Svenska kyrkan[8], Ljusdals kommuns[9] underleverantör av ekonomisystemet Å-data, Härjedalens kommun[10] och Coop Värmland[11] där antagonisterna nu publicerar anställdas personuppgifter på Darknet[12] som de kommit över vid attacken. Ja, listan kan göras lång!

Säkerhetskultur Gävle kommunkoncern

Under informationssäkerhetsmånaden genomförde Styrning och Stöd, Gävle kommun en aktivitet med syfte att mäta informationssäkerhetkulturen hos chefer. Ett fejkat mejl skickades ut till ca 350 chefer. Mejl såg ut som det kom externt och hade varningsbanner och med rubriken ”här kommer bilderna från senaste chefsmötet”. Budskapet i mejlet var dels att klicka på bifogad fil för att få åtkomst till bilderna, dels att lämna ifrån sig personlig inloggningsinformation. Resultatet visade att

- 15 chefer både klickade på bifogad länk samt lämnade sina inloggningsuppgifter.
- det tog 2 min 13 sekunder efter att mejlet skickats ut när första chefen klickat och lämnat inloggningsuppgifterna.
- 55 chefer laddade ner bifogade filen.
- Ingen rapport inkom till IT-supporten om att de upptäckt ett fejkat mejl.

Om det hade varit ett skarpt mejl från en antagonist hade det inneburit att

- 1 400 användarkonton hade blivit kapade.
- 2200 datorer infekterade med skadlig kod.

Vad gäller resultatet för Välfärd Gävle säger IT-säkerhetsansvarig så här:

”Av de mottagare som uppgav användarnamn och lösenord (15st) var:

- 40% från Välfärd Gävle

[8] Stora problem efter cyberattack mot Svenska kyrkan | SVT Nyheter
[9] Viktig information om kommunens ekonomisystem Å-data - Ljusdals kommun
[10] Härjedalens kommun är drabbad av en IT-attack - Härjedalens kommun (herjedalen.se)
[11] Svenskvaruhuskedjan Coop svarar på cyberattack (therecord.media)
[12] Coop-anställda hängs ut på darknet efter cyberattack | SVT Nyheter

Av de användare som klickade på den bifogade filen (55st) var:

- 47% från Välfärd Gävle

Detta behöver ställas i proportion till hur många av mottagarna (349st) som är chefer på Välfärd för att vara rättvisande.”

Frågor som kan ställas är

- Hur får vi tillgång till behövlig information om våra kunder och deras behov av insatser om/när vi blir drabbade? Har vi tillgång till analog information?
- Kan vi fortsätta vårt uppdrag att leverera en välfärd att lita på till våra kunder och med tryggheten att vi levererar rätt insats till rätt kund vid rätt tidpunkt?
- Om vi skulle misslyckas med våra uppdrag, vilka konsekvenser skulle det kunnat bli för våra kunder och särskilt våra mest utsatta kunder?

Aktiviteten visar att informationssäkerhetskulturen behöver utvecklas inom kommunen både för cheferna som är ytterst ansvariga för informationssäkerheten och för samtliga medarbetare så säkerhetskulturen blir lika självklar som sekretessen är.

Kommande lagstiftning – NIS 2

Under hösten 2022 beslutade EU parlamentet om att justera NIS direktivet, med benämningen NIS 2. Syftet är att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom Europeiska unionen som en följd av den ökade digitaliseringen och hotbilden av cyberhot. Kraven i NIS 2 avser att harmonisera införlivandet av reglerna i NIS inom unionen, utöka samarbetet mellan medlemsstaterna och att utöka antalet sektorer och aktörer som omfattas av regleringen. Medlemsstaterna har tid på sig fram till oktober 2024 att implementera direktivet i nationell lagstiftning. För Sveriges del kommer ett betänkande under februari 2024 då vi får mer information om hur Sverige har tänkt implementera direktivet i den svenska lagstiftningen. Bland nyheterna i NIS 2 och som MSB berättade mer om i december 2023 finns bland annat möjlighet för tillsynsmyndighet att ta ut högre vite vid misskötsamhet, personligt ansvar för ledningen, ytterligare entiteter som till

exempel offentlig förvaltning samt krav på kontroll och uppföljning av våra IT-leveranser, både från leverantörer och dess underleverantörer.

Förhandsinformationen från MSB sammanställdes i en rapport[13] med rekommendationer till aktiviteter att vidta under tiden innan lagstiftning börjar gälla. Rekommendationerna avser till exempel att redan nu organisera för ett arbete kring uppföljning av leverantörer och dess underleverantörers leveranser, kartlägga vilket stöd ledningen behöver utifrån ökade krav på ledningens ansvar, plan för att kommande ny lagstiftning - CER[14] ska implementeras parallellt med NIS 2 samt kartlägga vilka system, nätverk och verksamheter som kommer att påverkas att entiteten offentlig förvaltning även kommer att omfatta kommuner.

Verksamhet under året

Stödjande arbete

Riskanalyser har genomförts dels i samband med informationsklassningar och konsekvensbedömningar, dels vid enbart behov av riskanalys.

Stöd vad gäller **informationssäkerhetskrav** vid vissa direktupphandlingar och upphandlingar av IT-stöd.

Stöd i **specifika frågor** kring informationssäkerhet, såsom implementation av NIS inom Hälso- och sjukvård.

Rekommendationer och **avrådan** vid exempelvis anskaffning av IT-lösningar.

22 informationsklassningar har genomförts under året som lett till en handlingsplan som överlämnats för genomförande till Informationsägare (chef).

2 Rekommendationer om att inte köpa in/anskaffa har lämnats till chef samt informerats till biträdande sektorchef.

30 incidentrapporter har skrivits och överlämnats till ledningen, nämnd och informations- och/eller systemägare (chef).

[13] 23AFN245, 23ON548, 23SON266
[14] EU och arbetet med att stärka motståndskraften i samhällsviktig verksamhet (msb.se)

1 Riskrapport har skrivits och överlämnats till ledningen, nämnd och informations- och/eller systemägare (chef).

4 incidentrapporter till MSB, i enlighet med Lag om samhällsviktiga tjänster. (2018:1174)

Ett antal ringa informationssäkerhetsincidenter, utifrån brist i konfidentialiteten, har rapporterats tillsammans med incidentrapporteringen för personuppgiftsincident.

3 rapporter från **omvärldsbevakning** har skrivit och delgett Sektorsledningen.

1 Rapport med **rekommendation inför ny lagstiftning** kring NIS2 och CER har skrivits och delgett verksamhetschef och biträdande sektorchef.

Utbildning och information på APT:er och verksamhetsmöten.

- Nyanställd DSS, MAS och MAR
- 2 enheter inom Kontor Utveckling och stöd
- 2 enheter inom Kontor Myndighet
- 2 enheter inom Kontor Arbetsmarknad och funktionsrätt
- DISK[15] inom Komvux, Kontor Arbetsmarknad och funktionsrätt
- Vid stå-möte inom Kontor Utveckling och stöd
- Ledningsgruppen Kontor Hälso- och sjukvård
- Introduktion nyanställda inom Kontor Utveckling och stöd

Särskilt samarbete med anledning av NIS-direktivet

Samarbete har genomförts med kontoret Hälso- och sjukvård vad gäller NIS direktivet genom särskild utbildning för ledningsgruppen samt dialog kring de oacceptabla antal systemavbrott i Treserva/TES under året vilket påverkar kontorets förutsättningar för en trygg insatsverksamhet.

Samordnande arbete

Första fasen ”Identifiera och analysera” i metodstöd för införande av systematiskt informationsarbete har genomförts. Det planerade arbetet med det fortsatta arbetet med riskanalys med Sektorsledningen har tagits över av kontorsledningsgruppen för Utveckling och stöd. Ingen plan för fortsatta arbetet har kommunicerats.

Arbetet i fas 2 och 3 har startat och vissa aktiviteter är genomförda. Plan för fas 2 och 3 ska slutföras senast under Q1 2024.

Aktiviteter

Utbildning och informationssäkerhetskultur

Förslag till **utbildningsplan** togs fram 2022 och överlämnades för diskussion och beslut till biträdande sektorchef.

[15] Dataskydd- och InformationsSäkerhetsKoordinator

Organisation

Förslag till organisation togs fram under 2023 och överlämnades för diskussion till biträdande sektorchef. Två förslag var mest angelägna att få på plats. Dels föreslaget till att **inrätta en styrgrupp** för frågor kring informationssäkerhet och dataskydd. Biträdande sektorchef beslutade att befintlig styrgrupp kring strategiska och operativa IT frågor på sektor Välfärd skulle hantera även dessa frågor och beslut. ISS och DSS deltar i denna styrgrupp från och med hösten 2023.

Förslaget till att **utse chefstöd**, så kallade DISK:ar i organisationen i syfte att dels stödja chefer (Informationsägare) i deras ansvar för informationssäkerheten inom sin verksamhet, dels som samtalskontakt vid incidenter och registerutdrag och behov av stöd i varje verksamhet med ISS och DSS har inte genomförts. Dock finns en DISK utsedd i organisationen (Komvux) och som utsågs utifrån eget initiativ. En avgörande framgångsfaktor i att uppnå en acceptabel informationssäkerhetskultur inom sektorn är att etablera en organisation i hela sektorn så kunskap och kompetens kan spridas som ringar på vattnet och därmed bli en naturlig del i det dagliga arbetet på liknande sätt som sekretess. Att ha en organisation med få medarbetare centralt för dessa frågor kommer inte att bidra till en ökad informationssäkerhetskultur i sektorn, vilken är en stor risk för vår möjlighet att skydda vår information som vi har ett stort behov av för att utföra vårt uppdrag tryggt och en välfärd att lita på för våra kunder. Se även resultat av aktivitet kring fejkat mejl till chefer tidigare i denna rapport.

Inköp och upphandling

Förslag till komplettering i **checklistan vid direktupphandling togs fram 2022** och ett **uppdrag om rutin vid upphandlingar av IT-lösningar inom sektorn** gavs till chef IT inom sektorn. Rutinen ska bland annat innebär att informationssäkerhet alltid ska beaktas inför varje upphandling. Ingen rutin finns ännu på plats utan ISS försöker informera om behovet och nyttan med att tidigt säkerställa informationssäkerheten och dataskyddet i tänkt IT-lösning när hen får vetskap om upphandling som är aktuell.

Incidentrapportering

Process och ansvar för **incidentrapporteringen internt** har påbörjats och förbättras löpande. Processen har utformats så likformigt som möjligt med incidentrapportering inom dataskydd. Ansvar för uppgiften under kontorstid är ISS med DSS som vikarie.

Process och ansvar för incidentrapportering till MSB när rapporteringsskyldighet uppnåtts i Hälso- och sjukvårdsverksamheten är beslutat. Under kontorstid bedömer ISS om rapporteringsskyldigheten uppnåtts. Vid längre frånvaro för ISS är DSS i första hand vikarie och Systemförvaltningsenheten i andra hand.

Även en rutin för **incidentrapportering till sektorns tre nämnder** har införts. Processen är likformig med dataskyddsincidentrapporteringen. Införandet har skett tillsammans med nämndsamordnare och Dataskyddssamordnare.

Rutin för **incidenthantering vid avbrott i system som berör flera verksamheter**, så kallad Task Force har tagit fram i samarbete med systemförvaltning, informationssäkerhet och dataskydd samt kommunikation. Rutinen har dokumenterats under Q4 2023. Syfte med rutinen är att effektivisera kommunikationen till berörda verksamheter, ledning och mellan våra stödverksamheter under ett större avbrott.

Genomförande av åtgärder i syfte att öka informationssäkerheten

Vid informationssäkerhetsklassningar identifieras åtgärder för att minimera eller eliminera risker för att vi inte lyckas skydda informationen. Även vid incidentrapportering ges förslag till åtgärder, som godkänns av chef, för att motsvarande incident inte ska inträffa igen. Dessa åtgärder läggs in i ledningssystemet Stratsys som stöd för genomförandet och för uppföljning. Under året har 104 åtgärder lagts in och av dessa har 31 klarmarkeras och 56 har förfallit. Övriga 17 har ett slutdatum in på 2024. Det innebär att 36 % av åtgärderna har åtgärdats och därmed bidragit till att ökat informationssäkerheten medan 64 % av åtgärderna inte genomförts utan fortfarande är risker för att informationen inte har tillräckligt skydd. Konstaterat är att engagemanget att genomföra åtgärder och därmed öka informationssäkerheten är låg.

Frågan kring vem som ansvarar för att följa upp att åtgärder genomförts är oklar. Om vi inte genomför åtgärderna, som faktiskt har godkänts av ansvariga, finns ingen nytta med att

rapportera incidenter och arbeta med ständiga förbättringar i syfte att öka skyddet för vår information och därmed våra möjligheter att utföra vårt uppdrag på ett tryggt sätt och en välfärd att lita på för våra medborgare.

Hälso- och sjukvård och NIS

Förslag till vilka verksamheter och dess system och nätverk som **berörs av NIS direktivet** togs fram 2022. Förslaget har tagits fram tillsammans med Medicinskt ansvariga sjuksköterska samt verksamhetsnära systemförvaltning. Förslaget har setts över under 2023 utifrån ökad kunskap om befintliga system samt nytillkomna system. Förslaget kommer att behöva kompletteras med kartläggning av aktuella nätverk.

Behovet att förtydliga vad som omfattades av NIS-direktivet behövs för att underlätta införande av de krav som ställs enligt direktivet samt författningar utfärdade av MSB samt en tydlighet vid avbrottsincidenter. Inget beslut har kommunicerats utan ISS utgår från uppdaterat förslag vid bedömning om rapporteringsskyldighet har uppstått vid avbrott i system.

Årliga riskanalys

Rutin och tillämpning av rutin för årliga riskanalyser har beslutats. NIS ställer krav på årlig riskanalys för system och nätverk som används för Hälso- och sjukvård. En rekommendation finns också från CISO om att årliga riskanalyser bör genomföras för informationsbehandlingar klassats som en 2:a eller 3:a vad gäller konfidentialiteten.

Ett års hjul har skapats i Stratsys som stöd för när det är dags för respektive system. Input i riskanalysen kommer att vara inträffade incidenter under året, resultat av uppföljning av IT leverans och dess leverantörer och underleverantörer samt kunskap från omvärldsbevakning. Även resultat av uppföljning av Personuppgiftsbiträdesavtal ska tas med.

Uppföljning av IT-leveranser

En pilot är planerad och skall starta Q1 2024 för att prova sig fram och se hur en uppföljning skulle kunna genomföras. Piloten omfattar inte ett system som omfattas av NIS utan i en upphandlingen har innehållit tydliga informationssäkerhetskrav som kan användas vid en uppföljning och utvärdering. Tanken är att välja ut lämpliga krav som leverantören och eventuell underleverantör svarat att de uppfyller i offertsvaret. Resultatet av uppföljningen kommer att vara en input till årlig riskanalys. I och med lagstiftning utifrån NIS 2 kommer vi att behöva ha rutiner och arbetssätt på plats i oktober 2024.

I rapport från MSB:s förhandsinformation kring NIS 2 har ISS rekommenderat att en organisation med ansvar för genomförandet av uppföljning av IT-leveranser redan nu etableras och som deltar i piloten.

Avrådan

Teams för digitala möten

Frågan kring att använda Teams för digitala möten inom sektorn har under året varit en återkommande fråga. Under pandemin som innebar att vi inte kunde ses fysiskt i samma utsträckning beslutades att ta risken för en eventuell tredjelands överföring av personuppgifter genom att tillåta digitala möten via Teams.

När så pandemin var över fick DSS och ISS frågan om vad vi rekommenderade. Vi tog då stöd av CISO och Dataskyddsombud och skrev en avrådan som vi senare ryktesvägen fick höra att socialnämnden fattat samma beslut som. Eftersom det inte finns något annat alternativt IT stöd för digitala möten uppstod en frustration hos chefer och personal i vissa verksamheter då det upplevt att de kunnat arbeta mer effektivt digitalt. Frågan om alternativt IT stöd är olöst vid skrivande stund. Den generella frågan kring amerikanska tjänster och avtalet[16] mellan USA och EU hanteras även av kommunjurist och CISO vilka ska ha haft en dialog med Välfärd Gävle i frågan. Vilket beslut sektor Välfärd tar i frågan är i skrivande stund oklart.

[16] Data Privacy Framework

Appwriter

SFI hade önskemål om att köpa in 250 licenser för applikationen Appwriter som ger stöd vid läs- och skrivsvårigheter. Tanken var att studenterna skulle installera appen på sin privata telefon. Programmet samlar in informationen (personuppgifter) för marknadsföring samt kan/vill sprida informationen utanför EU vilket bedömdes av DSS och ISS samt dataskyddsombudet är en risk för tredjelandsöverföring, att vi inte har kontroll på vilken information som behandlas i privata telefoner samt att det kan vara svårt att beskriva risken för elever som inte har goda kunskaper i svenska. Vi avrådde ett inköp.

Canva

Canva är ett program som kan användas inom kommunikation genom text och bild. Informationen kan därmed innehålla bilder på personer (personuppgifter). På liknande sätt som Appwriter samlar Canva in information för marknadsföring och kan/vill sprida informationen utanför EU vilket bedömdes som risk för tredjelandsöverföring. Vi avrådde ett inköp och användning av gratisversion.

Mejl till funktionsbrevlådor i MS Office 365

Utredning kring inkommande fax/mejl med personuppgifter till funktionsbrevlådor och dess hantering påbörjades under året av IT enheten, Välfärd. Våra funktionsbrevlådor finns i MS 365 vilket innebär en risk för tredjelandsöverföring av personuppgifter. Bland annat så anmäldes en incident utifrån att personuppgifter och till och med skyddade personuppgifter behandlas i funktionsbrevlåda och rutiner och tillämpning av riktlinjer för säker e-post för att minimera exponeringen inte finns på plats. Förslag på åtgärder gavs i samband med incidentrapporteringen.

Säker digital kommunikation (SDK) är en tjänst som är i uppstart inom Gävle kommun och kommer kanske vara en lösning framöver.

Nätverkande och vidareutbildning

ISS har deltagit på

KIS nätverkets två digitala möten under året. KIS nätverket är ett nationellt nätverk för kommuner. Under nätverkandet erhålls information kring informationssäkerhet och det ges tillfälle att diskutera aktuella frågor med andra kommuner.

CISO:s nätverk för alla verksamheter inom Gävle kommunkoncern inkl bolagen. Även här ges information/utbildning samt möjlighet att diskutera aktuella frågor med andra kommuner.

Ett fysiskt möte med Länsstyrelsens nätverk för kommuner, region och andra aktörer inom Gävleborgs län.

Ett antal kortare gratis digitala seminarium med MSB, SKR och privata aktörer om Informationssäkerhet, Välfärdsteknik och kommande NIS2.

Ett fysiskt heldagsseminarium om kommande NIS 2, anordnat av MSB i Stockholm.

Granskning

Ingen granskning av CISO har genomförts.

Incidenter

Vi har haft 30 incidenter under året. I de allra flesta fallen har orsaken var brist i tillgängligheten genom systemavbrott eller nätverksavbrott på grund av tekniska fel eller mänskliga faktorn.

Av dessa avsågs 12 systemen Treserva Vo och TES som används i huvudsak av verksamheterna Hemsjukvård och Hemtjänst vilket statistiskt sett har inneburit 1 avbrott per månad. Avbrotten har ställt stora krav på verksamheten och personalen att trots så ofta förekommande avbrott till digital information ändå lyckats leverera sina uppdrag. En reflektion är att Treserva IFO inte haft något avbrott under året vilket är märkligt då flera avbrott i Treserva VO har berott på driftsrelaterade orsaker.

Även verksamheten för nattliga larm har haft 5 avbrott under året vilket också skapat ökade krav på verksamheten och personalen. Speciellt när tjänsten digital nattlig tillsyn haft avbrott och ett stort antal digitala tillsyner fick ersättas med fysiska oplanerade och ej schemalagda besök. En ny upphandling har under året genomförts och ny leverantör finns på plats inför 2024.

Plan för kommande år

För 2024 är ambitionen av ISS och planen att

- Bidrag till ökad informationssäkerhetskultur i hela sektor Välfärd genom utbildning och ge stöd till chefer och medarbetare.
- Verka för fler medarbetare som agerar ambassadörer för informationssäkerhet och dataskydd.
- Stödja Informationsägare/Systemägare/chef vid information säkerhetsklassning och riskanalys.
- Incidentrapportera
- Genomföra årliga riskanalyser enligt rekommendation från CISO (skyddsklass 2 och 3) och beslutad rutin.
- Förberedelse och implementation av NIS 2 (tillsammans med utsedd för CER)
    - Rutiner för uppföljning av IT-leveranser
    - Samarbeta med utsedd för införandet av CER
    - Stöd till ledningen utifrån deras behov
    - Utreda innebörden för Välfärd att offentlig förvaltning blir en entitet.
- Ta fram förslag på rutiner som bidrar till ökad informationssäkerhet.
- Delta i aktiviteter kring organisation, roller och ansvar
- Påbörja fjärde delen i MSB:s ledningsmodell för informationssäkerhet genom att framföra frågan kring uppföljning av åtgärdsförslag i syfte att eliminera eller minimera incidenter utifrån att enbart 36 % av åtgärdsförslag har genomförts 2023.

Bedömning av informationssäkerhetsarbetet hos Välfärd Gävle

Arbetet har under året periodvist varit intensivt utifrån stort intresse för stöd i informationssäkerhetsklassning och riskanalys, ett stort antal incidenter som skulle rapporteras och samtidigt etablera systematiskt informationssäkerhetsarbete med utbildningar, utforma arbetssätt och rutiner och diskussioner kring informationssäkerhet med mera. ISS tillsammans med DSS har genomfört mycket under året vilket denna rapport visar och vi kommer att fortsätta så även under 2024. Det är mycket kvar att göra visade GAP-analysen!

Arbetet har fungerat väldigt bra tack vare goda samarbetspartners, med bland annat dataskyddssamordnare Välfärd och CISO, två olika dataskyddsombud, IT-

säkerhetsansvarig och driftschef samtliga på SG. Dessutom många intresserade medarbetare i olika roller, av informationssäkerhet och dataskydd inom sektor Välfärd.

Intresset och insikten av viktigheten med informationssäkerhets- och dataskyddsarbetet upplevs har ökat på sektorn men mycket arbete kvarstår för att öka informationssäkerhetskulturen i hela sektorn.

Kommunkoncernens CISO Adrian Henriksson Severin säger så här:

”Välfärd Gävles informationssäkerhetsarbete visar tydliga tecken på framsteg. Informationssäkerhetssamordnare och Dataskyddssamordnare är aktiva och engagerade i sina roller. Deras insatser bidrar till att förbättra och utveckla arbetet hos såväl sektorn som hela kommunen. Sektorns verksamheter visar ökande engagemang i informationssäkerhetsarbete, vilket är ett positivt tecken. Detta ökade intresse bidrar till en bättre förståelse och hantering av informationssäkerhets- och dataskyddsfrågor. Trots detta engagemang finns det fortfarande arbete att göra för att ytterligare stärka informationssäkerheten. Fortsatta insatser behövs för att säkerställa att säkerhetsarbetet blir en integrerad och kontinuerlig del av alla verksamheters rutiner och processer.

För att uppnå detta behöver ledningen involvera sig regelbundet i informationssäkerhetsarbetet. En årlig genomgång av informationssäkerhetsarbetet skulle inte bara understryka vikten av informationssäkerhet, utan även säkerställa att det blir en fast förankrad del av verksamhetskulturen. Kontinuerlig utbildning och medvetenhet bland alla anställda är också avgörande för att ytterligare stärka informationssäkerheten inom organisationen.”