Rapport

informationssäkerhet och dataskydd 2022

Ledningens genomgång

Typ av styrdokument: Rapport
Beslutande instans: Kommunstyrelsen
Datum för beslut: ÅÅÅÅ-MM-DD
Diarienummer: 2023.059 KS

Gäller för: Kommunövergripande
Giltighetstid: --
Revideras senast: --
Dokumentansvarig: Informationssäkerhetsansvarig

Innehåll

Sammanfattning

Genom uppföljning och utvärdering av informationssäkerhets- och dataskyddsarbetet ges uppgifter om arbetet i stort är ändamålsenligt utformat, har avsedd verkan, samt att säkerhetsåtgärder existerar och fungerar tillfredsställande. Resultatet från denna rapport ligger bland annat till grund för fortsatt arbete med det systematiska informationssäkerhet- och dataskyddsarbetet inom kommunen.

Året har på flera sätt varit präglat av Rysslands invasion av Ukraina med en bedömd ökad hotbild gällande IT-attacker mot svenska intressen, däribland har kommuner pekats ut som tänkbara mål för angripare. Omvärldsläget påvisar relevansen att arbeta med dessa frågor och därmed göra organisationen mer motståndskraftig.

I Alingsås kommun finns goda förutsättningar att nå resultat i arbetet med informationssäkerhet och dataskydd. Det finns både en intern organisation och arbetsmetoder på plats vilket möjliggör ett systematiskt arbetssätt.

Av genomförda mätningar framgår att kommunen utvecklats inom områdena informationssäkerhet och dataskydd under 2022. Mätningarna påvisar dock även att det finns mycket arbete kvar att göra för att uppnå fullmäktiges långsiktiga målsättningar. Planeringen i arbetet har en tidshorisont på flera år då förändring och utveckling tar tid.

Av genomförda mätningar framgår att kommunen för 2023 särskilt behöver fokusera på incidenthantering, upphandling, medarbetarnas kunskaper, uppföljning/utvärdering och säkerhetskultur.

Om informationssäkerhet och dataskydd

Informationssäkerhet handlar om att hindra information från att läcka ut, förvanskas och förstöras. Det handlar också om att rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Information ska inte kunna hamna i orätta händer och missbrukas.

Alingsås kommuns arbete med informationssäkerhet är uppbyggt utifrån MSB:s metodsstöd för systematiskt informationssäkerhetsarbete. Metodstödet består av fyra olika metodsteg som tillsammans bildar helheten av det systematiska informationssäkerhetsarbetet och utgör ett årshjul. Till årshjulet har även arbetet med dataskydd lagts till.

Dataskydd handlar om skyddet av enskildas personuppgifter och är en integritetsskyddsfråga. De personuppgifter som Alingsås kommun behöver behandla för att utföra sitt uppdrag ska endast användas med stöd i lag och skyddas från obehöriga. Regler för hantering av personuppgifter återfinns i EU:s dataskyddsförordning.

Underlag för genomgång

Omvärldsanalys

Omvärld i förändring och förändrad hotbild

Oron i vår omvärld gör sig påmind på flera sätt, inte minst inom informations-, it-säkerhet- och dataskyddsområdet. Den senaste tiden kan vi se en ökad rapportering gällande olika IT-attacker mot såväl privata som offentliga organisationer. Alingsås kommun är givetvis inte undantaget denna problematik.

De cyberhot som riktas mot Sverige är mångfacetterade och kan kopplas till flera olika typer av hotaktörer. I huvudsak utgörs dessa av statliga aktörer, kriminella och i viss omfattning även av ideologiskt motiverade aktörer, sk. hacktivister. Metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas spelplan förändras i takt med teknikutvecklingen. Hotaktörerna använder sig ofta av enklast möjliga metod för att uppnå önskat resultat och i många fall krävs inte att de använder sig av avancerade metoder.

Förflyttningen av vår information till digitala miljöer innebär ofta effektivare arbetssätt, men det leder också till nya och ökade hot mot våra verksamheter från omvärlden. Detta ska inte ses som kritik eller en invändning mot digitalisering utan det är ett faktum som vi måste förhålla oss till. Vi behöver öka arbetet med att förhindra och försvåra för aktörer som på olika sätt vill störa ut vår verksamhet (t.ex. genom en IT-attack), likaså förbereda för oss för att bli bra på att hantera en situation när aktörer lyckas störa ut verksamhetskritiska system.

Nationellt cybersäkerhetscenter

Under 2022 inrättades ett nationellt cybersäkerhetscenter vars huvuduppdrag är att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot. De statliga myndigheterna bidrar till centrets verksamhet inom ramen för sina befintliga uppdrag och förmågor inom svensk cybersäkerhet.

Nytt NIS-direktiv
EU-parlamentet fastställde i slutet av 2022 NIS2-direktivet. Det är en uppdaterad version av det tidigare NIS-direktivet och innebär ökade krav och skyldigheter för långt fler aktörer än tidigare. Direktivet ställer krav på att de som levererar samhällsviktig verksamhet ska bedriva ett riskbaserat och systematiskt informationssäkerhetsarbete. Syftet är att uppnå en ökad gemensam motståndskraft mot informationssäkerhetsrelaterade hot inom EU. I dagsläget omfattas Alingsås kommun av direktivet kopplat till vattenförsörjning och delar inom hälso- och sjukvård, men fler delar av kommunen kommer träffas av lagstiftningen framöver. NIS 2-direktivet väntas träda i kraft under 2024.

Tredjelandöverföring av personuppgifter
EU-kommissionen har publicerat ett utkast till nytt beslut om adekvat skyddsnivå för USA gällande överföring av personuppgifter. EU-domstolen ogiltigförklarade sommaren 2020 Privacy Shield i den så kallade Schrems II-domen.I korthet kom EU-domstolen fram till att det amerikanska rättssystemet inte ger ett tillräckligt skydd för personuppgifter som överförs till USA, dels för att det saknas tillgång till effektiva rättsmedel, dels för att amerikanska myndigheter har alltför vidsträckta möjligheter att få tillgång till uppgifter som förs över dit. I mars 2022, träffade EU-kommissionen och USA en principöverenskommelse om ett nytt transatlantiskt ramverk för skydd av personuppgifter: Trans-Atlantic Data Privacy Framework. I oktober undertecknade USA:s president Biden en så kallad ”Executive Order” som en del av implementeringen av överenskommelsen. Presidentordern introducerar åtgärder som syftar till att möta de krav som EU-domstolen ställer i Schrems II-domen. I slutet av 2022 publicerade EU-kommissionen ett utkast till nytt beslut om adekvat skyddsnivå för USA. Ett adekvansbeslut för USA kommer sannolikt att fattas till sommaren. Det återstår dock att se om adekvansbeslutet och överenskommelsen står sig vid en eventuell ny prövning i EU-domstolen. Organisationen NOYB med Max Schrems i spetsen har nämligen redan annonserat att man sannolikt kommer att utmana även detta beslut som, enligt organisationen, preliminärt inte bedöms uppfylla kraven.

Uppföljning av tidigare beslut

Kommunstyrelsen fastställde den 13 december 2021, § 220, handlingsplan för informationssäkerhet och dataskydd 2022 i Alingsås kommun. Under 2022 har merparten av de aktiviteter som ingått i handlingsplanen genomförts eller påbörjats. De aktiviteter som inte genomförts under 2022 föreslås flyttas över till 2023 års handlingsplan. Flera aktiviteter under både 2021 och 2022 år har varit introducering av metoder som framöver kommer ingå i ett årshjul för informationssäkerhet och dataskydd.

Se bilaga 1 för vidare läsning om genomförda/påbörjade/ej påbörjade aktiviteter.

Utvalda delar av genomfört arbete 2022

Mot bakgrund av förändrad hotbild gav kommunledningen i början av 2022 samtliga verksamheter i uppdrag att kontinuitetsplanera sina mest verksamhetskritiska processer. Utgångspunkten för planering var att allt IT-stöd var helt ur funktion i en månad eller mer. Som ett led i detta arbete genomfördes en övning där framtagna kontinuitetsplaner testades. De flesta ledningsgrupper genomförde under sommaren 2022 en övning med scenariot IT-attack.

Genom det kommunövergripande nätverket för informationssäkerhet och dataskydd har arbetet fortsatt med att bringa systematik i kommunens informationssäkerhets- och dataskyddsarbete. Under senare delen av 2022 har momentet ”Riskanalys” genomförts i de flesta verksamheter. Momentet syftar till att identifiera hot och sårbarheter gentemot respektive verksamhets informationstillgångar, samt att ta fram åtgärdsförslag för att reducera identifierade risker. De största riskerna som identifierats är driftstopp av viktiga IT-system, att känslig information röjs/sprids och att information förstörs och inte går att återskapa.

En ny central dataskyddsorganisation har beslutats och implementerats på kommunledningskontoret. Under 2022 har fokus varit att tydliggöra roller och ansvar och därifrån fortsätta utvecklandet av kommunens personuppgiftshantering. Att ha en organisation som gemensamt arbetar med dataskyddsfrågorna bedöms göra arbetet med dataskydd betydligt mer redundant är tidigare, samt skapar förutsättningar för en höjd kompetens gällande dataskydd inom kommunorganisationen.

Under året har flera informationsinsatser genomförts i ledningsgrupper och nämnder/styrelser. En digital informationssäkerhetsutbildning för samtliga anställda lanserades under hösten 2022 och kommer att fortgå 12 månader framåt. Syftet är att höja den generella medvetenheten och kompetensen kring informationssäkerhet och dataskydd.

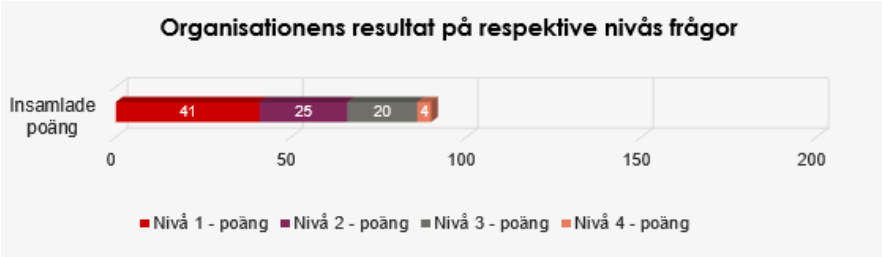
Flertalet IT-säkerhetsrelaterade insatser har genomförts under året. Arbete med att införa två-faktorsautentisering pågår och kommer fortsätta vidare 2023. Detsamma gäller utvecklandet av kommunens behörighetshantering och även arbetet med att skapa redundans i vår IT-miljö.

Resultat från revisioner (interna och externa) och andra granskningar

Informationssäkerhet
Alingsås kommun använder sig sedan 2021 av MSB:s verktyg, Infosäkkollen, för revision av internt informationssäkerhetsarbete. Verktyget innehåller självskattande frågor om centrala delar av det systematiska informationssäkerhetsarbetet. Frågorna rör olika områden, exempelvis ledningens engagemang, centrala arbetssätt, systematik, utbildning, ständiga förbättringar osv. Frågorna har besvarats av informationssäkerhetsansvarig och IT-säkerhetsansvarig tillsammans.

Kommunen har höjt sin nivå på informationssäkerhetsarbetet i stort jämfört med 2021 års mätning. Dock är det tydligt att mycket arbete kvarstår för att uppnå önskade säkerhetsnivåer. Över tid är önskat läge att Alingsås kommun närmar sig nivå fyra av verktygets olika graderingar, resultatet för 2022 visar att vi ligger på nivå noll av fem. Detta förklaras med att vi har några delar som vi inte jobbat med ännu, men dessa kommer omhändertas under 2023.

2022



2021

De delar som kommunen kommit längre med är att beslut om långsiktiga målsättningar och principer finns på plats, att det grundläggande analysarbetet påbörjats ute i verksamheterna samt kontinuerlig omvärldsbevakning. Kommunen har under det senaste två åren byggt upp en grund för ett systematiskt informationssäkerhets- och dataskyddsarbete. Genom det övergripande säkerhetsarbetet finns utpekade resurser på varje förvaltning/bolag/förbund som ska jobba med informationssäkerhet och dataskydd.

Av resultatet framgår att kommunen under 2023 behöver fokusera särskilt på områdena incidenthantering, upphandling, medarbetarnas kunskaper, uppföljning/utvärdering och säkerhetskultur. Flera pågående arbetsinsatser kommer höja kommunens förmåga inom dessa utpekade områden men det kommer behövas ytterligare riktade insatser för att nå önskade säkerhetsnivåer. Aktiviteter för detta kommer föreslås i 2023 års handlingsplan.

Någon revision utförd av extern part har inte genomförts under 2022.

Dataskydd
Under hösten 2022 har kommunens dataskyddsombud begärt in uppgifter om hur respektive personuppgiftsansvarig i kommunen bedriver sitt dataskyddsarbete i form av en efterlevnadskontroll. De frågor som ställdes till kommunens personuppgiftsansvariga var i stora drag följande:

- Hur den personuppgiftsansvariges dataskyddsorganisation ser ut, vilka funktioner som är involverade samt hur organisationen fungerar.
- Hur den personuppgiftsansvariges behandlingsregister ser ut, en beskrivning av hur verksamheten arbetar med val av rättslig grund för behandlingar samt om den rättsliga grunden samtycka används.
- Hur den personuppgiftsansvarige arbetar för att identifiera, dokumentera och följa upp personuppgiftsincidenter.
- Hur det personuppgiftsansvarige arbetar med och vilka rutiner som finns för att hantera de registrerades rättigheter, framförallt i form av begäran om registerutdrag, rättelse eller radering av personuppgifter.
- Den personuppgiftsansvariges förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt hur arbetsprocessen ser ut vid genomförandet av en konsekvensbedömning.

Svar på dataskyddsombudens frågor skickades in av respektive personuppgiftsansvarig under november månad och kommer resultera i återkoppling från dataskyddsombuden gällande de inlämnade svaren. Återkopplingen samt vilka åtgärder som behöver vidtas med anledningen av denna kommer att hanteras politiskt av varje personuppgiftsansvarig nämnd och styrelse.

Status när det gäller förebyggande och korrigerande åtgärder

Alingsås kommun har de senaste åren drabbats av flera IT-attacker. Detta har handlat om överbelastningsattacker, försök att utnyttja säkerhetshål i IT-system och applikationer samt nätfiske för att otillbörligen erhålla anställdas användaruppgifter.

Några av de mer utmärkande aktiviteterna som genomförts under 2022 är:

- Pilot gällande förhöjd säkerhet vid inloggning till verksamhetssystem med hjälp av 2-faktorautentisiering.
- Införande av permanent utökat överbelastningsskydd för Alingsås kommuns IT-nätverk.
- Utökad kapacitet, automatisering och effektivare hantering av skräppost samt nätfiske.
- Utökning av befintliga tekniska lösningar för 2-faktorautentisiering inom omsorg.
- Ytterligare begränsningar införda i vår kommuns IT-nätverk för att minimera säkerhetsrisker.

Då hotbilden ständigt förändras är detta ett kontinuerligt arbete att följa utvecklingen inom IT-säkerhetsområdet. Detta för att minimera riskerna och säkerställa våra långsiktiga mål samt att skyndsamt vara rustade för att anpassa oss till en föränderlig omvärld. Flera av de införda åtgärderna har tydligt mätbara förbättringar i hantering inom identifierade säkerhetsområden. Det har inneburit ökad tillgänglighet av verksamhetssystem, minskat antal lyckade nätfiske-attacker samt bekräftar att detta arbete behöver fortsätta med oförminskad styrka.

Incidenter

Avsnittet som följer redogör för incidenter inom informationssäkerhets- och dataskyddsområdet. Någon tidigare mätning likt det som följer har inte genomförts tidigare inom Alingsås kommun, därmed går det inte att jämföra med tidigare år.

IT-säkerhet

Alingsås kommun har under 2022 varit föremål för flera IT-attacker. Detta har handlat om försök till överbelastningsattacker, försök att utnyttja säkerhetshål i IT-system och applikationer samt nätfiske för att otillbörligen erhålla anställdas användaruppgifter.

Representant från NOA (Nationella operativa avdelningen) kontaktade i början av december 2022 Alingsås kommun och meddelade att användaruppgifter tillhörande Alingsås kommun låg ute för försäljning på Darknet (Russian market). NOA hade inte möjlighet att delge någon ytterligare information om omständigheterna. Omgående påbörjade IT-avdelningen genomföra säkerhetsåtgärder på såväl kort som lång sikt, däribland forcering av lösenordsbyte för alla anställda och förtroendevalda. IT-avdelningen gick omgående upp i stabsläge och hanterade incidenten med dagliga möten under några veckors tid. Det har inte gått att konstatera något intrång och likaså har ingen påverkan för kommunen konstaterats.

IT-säkerhetsincidenter 2022	Antal
Överbelastningsattacker där kommunens skydd aktiverats	13
Överbelastningsattacker som fått påverkan på verksamhet/system	0
Fullbordade kända intrång	0
Phisingattack	Ca 650
Lyckade phisingattacker	6
Skadlig kod - händelser där skadlig kod är stoppad i klienter (datorer)	Ca 1250

Fysisk säkerhet
Nedan tabell redogör för borttappad/stulen utrustning inom Alingsås kommun under 2022. Flest borttappade/stulna verktyg återfinns i skolans verksamhet, främst gäller det Chromebooks där 43 enheter försvunnit under året. Därutöver konstateras att antalet borttappade OTP-kort sticker ut, därutöver är det förhållandevis låga antal med borttappad/stulen utrustning.

Borttappad/stulen utrustning 2022	Antal
Chromebooks	43
OTP-kort	40
EDU iPad	9
ADM iPad	4
Mobiltelefoner och tillbehör	3
EDU PC	2
ADM PC	1

Någon insamling av incidenter gällande inbrott och övrig skadegörelse har inte genomförts under 2022.

Personell säkerhet
Någon insamling av incidenter gällande personell säkerhet har inte genomförts under 2022.

Administrativ säkerhet
Någon insamling av incidenter gällande administrativ säkerhet har inte genomförts under 2022.

Personuppgiftsincidenter
Antalet inrapporterade personuppgiftsincidenter uppgår till 22 stycken under 2022 vilket är förhållandevis lågt med hänsyn till den stora mängd personuppgiftsbehandlingar som dagligen sker i kommunen. Sannolikt tyder det på en viss underrapportering som i sig kan ha flertalet tänkbara orsaker vilket bör analyseras vidare.

Personuppgiftsincidenter 2022	Antal
Barn- och ungdomsnämnden	5
Kommunstyrelsen	2
Kultur- och utbildningsnämnden	2
Samhällsbyggnadsnämnden	1
Socialnämnden	4
Vård- och omsorgsnämnden	8
Överförmyndarnämnden	0

Riskarbete

Att genomföra riskanalyser med systematik och återkommande över tid är en viktig del i ett systematiskt informationssäkerhetsarbete. Genom metoden riskanalys identifieras och bedöms risker och sårbarheter som kan leda till negativa konsekvenser för verksamheten. Därtill ingår framtagande av säkerhetsåtgärder.

Förvaltningarnas riskanalyser

Varje förvaltning har under 2022 genomfört en riskanalys utifrån informationssäkerhet och dataskydd. Under året har tre informationstillgångar (ex system, journal, arkivskåp, lagringsyta o.s.v.) per verksamhet analyserats. Utkomsten av riskanalysen är att hot och risker har bedömts tillsammans med framtagande av säkerhetsåtgärder för att minska/förhindra verkan om hotet inträffar. Arbetet kommer vara årligen återkommande och riskanalyserna kommer utvecklas och bli mer heltäckande över tid.

Här följer några exempel av de hot och risker som återfinns i de flesta verksamheters riskanalyser:

Driftstopp – Att ett verksamhetskritiskt system drabbas av driftstopp ger stor negativ påverkan på flera verksamheter. Information går inte att nås och då går det inte att utföra sitt jobb enligt ordinarie arbetssätt. Orsaker till driftstopp kan vara flera, exempelvis en IT-attack, strömavbrott eller annat tekniskt fel.

Dataintrång – Risk för att sekretessbelagd information och personuppgifter röjs/sprids, risk att information förstörs och därigenom förloras, risk att skyddade identiteter röjs/sprids och därmed fara för enskilds individs säkerhet.

Informationsförlust – Att informationsmängder raderas och inte går att återskapa skulle få stor negativ konsekvens för flera verksamheter.

Exempel på framtagna åtgärdsförslag kopplat till hoten ovan är bland annat kontinuitetsplanering, utveckling av behörighetshantering och lösenordshantering, separering av nät, utbildning av medarbetare osv.

Informationsklassningar

Att klassificera information och därigenom utarbeta lämpligt skydd av information är en viktig del i ett systematiskt informationssäkerhetsarbete. Under 2022 har flera informationsklassningar genomförts i samband med upphandling och även i vissa skeenden för att kunna avgöra om det är lämpligt att vara kvar i en lösning eller ej. Under 2023 kommer arbetet med informationsklassning intensifieras och bli en del av kommunens ledningssystem.

Resultat från mätningar av informationssäkerhet och dataskydd

Resultatet från MSB:s Infosäkkollen visar på att Alingsås kommun har ett stort arbete framför sig gällande informationssäkerhet och dataskydd. Flera grundläggande delar har implementerats och ett systematiskt informationssäkerhets- och dataskyddsarbete har påbörjats. Pågående arbetsinsatser kommer över tid göra positiva verkan och höja nivån på kommunens informationssäkerhet och dataskydd, men processerna och förändring tar tid.

Överrensstämmelse med krav och mål

Inom kommunen finns två styrande dokument som anger långsiktiga målsättningar och grundläggande principer inom informationssäkerhet och dataskydd, informationsäkerhetspolicy och policy för behandling av personuppgifter. Nedan görs en redogörelse per område kring vilka krav och mål som finns i styrande dokument samt hur arbete går med att uppfylla dessa krav.

Informationssäkerhet
Kommunfullmäktige har i informationssäkerhetspolicyn angett följande långsiktiga mål:

Alingsås kommun ska uppnå och upprätthålla informationssäkerhet som:

- innebär en robust, säker och tillförlitlig informationshantering.
- i möjligaste mån motsvarar medborgares och externa verksamheters behov och förväntningar.
- möjliggör och underlättar digitalisering och att den sker med tillräcklig säkerhet.
- möjliggör att samtliga kritiska informationstillgångar informationsklassas.

Vidare anges att arbetet ska vara systematiskt och bygga på den vedertagna standardserien ISO/IEC 27000 medsträvan att ett ledningssystem för informationssäkerhet integreras i kommunens styrning.

Bedömningen är att fullmäktiges långsiktiga målsättningar med informationssäkerhetsarbete inte uppnås under 2022. Stort fokus under 2022 har varit att få till ett systematiskt arbetssätt med informationssäkerhet vilket har införts. Detta är en förutsättning för att fullmäktiges långsiktiga målsättningar ska uppnås. Det som behöver ske härnäst är att dessa metoder och arbetssätt ska genomföras med regelbundenhet och bli en naturlig del av kommunens arbete. Planeringen sträcker sig över flera år för att höja kommunens arbete med informationssäkerhet.

Utvärdering av lagefterlevnad

Krav på informationshantering kommer från flera olika lagstiftningar, i detta avsnitt lyfts för 2022 upp NIS-direktivet och Dataskyddsförordningen (GDPR). Kommande rapporter kommer inbegripa fler lagstiftningar som ställer krav på hur vi hanterar vår information.

Informationssäkerhet
NIS-direktivet trädde i kraft den 1 augusti 2018 i Sverige genom lagen om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster. NIS-direktivet syftar till att påskynda åtgärder och höja EU-medlemsstaternas skyddsnivå när det gäller samhällskritisk infrastruktur. Enkelt uttryck ska den verksamhet som träffas av lagstiftningen bedriva ett riskbaserat och systematiskt informationssäkerhetsarbete.

De verksamheter som pekats ut som samhällsviktig verksamhet är energi, transport, bank, finansmarknad, hälso- och sjukvård, dricksvattenförsörjning och digital infrastruktur. Alingsås kommun träffas av lagstiftningen gällande dricksvattenförsörjning och delar av hälso- och sjukvård inom vård- och omsorgsförvaltningens verksamhet. Centrala funktioner för informationssäkerhet har prioriterat stöttning till dessa verksamheter. Vattenverket hade tillsyn från Livsmedelsverket på sitt informationssäkerhetsarbete hösten 2020 utan anmärkning.

Under senhösten 2022 fastställde EU-kommissionen NIS 2-direktivet, det nu gällande direktivet bedöms inte ha önskade effekter utan nivån behöver höjas ytterligare. Den nya lagstiftningen kommer träffa fler kommunala verksamheter och därtill ställa hårdare krav på blanda annat incidentrapportering, ledningens styrning, striktare tillsynsåtgärder, sanktionsmöjligheter vid bristande efterlevnad m.m. NIS 2-direktivet väntas bli svensk lagstiftning under senare delen av 2024. Under 2023 kommer centrala funktioner inom informationssäkerhet följa utvecklingen med NIS-direktivet noggrant och föreslå åtgärder för att säkerställa regelefterlevnad.

Dataskydd
Bilden av regelefterlevnaden inom området dataskydd är att kommunens personuppgiftsansvariga följer dataskyddsförordningen i relativt hög omfattning. Samtliga obligatoriska styrdokument finns på plats. De registrerade informeras i aktuella fall om hur deras personuppgifter behandlas och det finns rutiner för att hantera begäran om rättelse och radering av personuppgifter samt begäran om registerutdrag. En medvetenhet om de krav som dataskyddsförordningens ställer finns, framförallt hos de medarbetare som arbetar med dataskyddsfrågor hos respektive personuppgiftsansvarig. Generell kunskap finns också i organisationen gällande uppgiftsminimering.

En utmaning som funnits under hela 2022 och fortsätter att vara aktuell under 2023 är hur kommunens samtliga personuppgiftsansvariga ska leva upp till gällande regler vad gäller överföring av personuppgifter till tredjeland. Som beskrivits under avsnittet *Omvärldsanalys* är det i dagsläget inte lagligt möjligt att låta länder som enligt EU inte uppfyller en adekvat skyddsnivå behandla personuppgifter som vi är ansvariga för. Det innebär i klartext att flera stora leverantörer av molntjänster inte uppfyller de krav som ställs och vi därmed inte har laglig rätt att använda dessa tjänster för hantering av personuppgifter. I sammanhanget bör

också nämnas att de krav som ställs gällande hantering av sekretessbelagda uppgifter enligt offentlighets- och sekretesslagen sammanfaller med de krav som ställs enligt dataskyddsförordningen. I likhet med personuppgifter får inte heller sekretessbelagda uppgifter göras tillgängliga för andra än de som har rätt att ta del av uppgifterna.

För att med tiden minimera det antal personuppgiftsöverföringar som sker till länder som inte kan garantera en adekvat skyddsnivå har kommunledningskontoret gjort ett ställningstagande. Ställningstagandet ser ut som följer:

- Försiktighetsprincipen råder och varje enskild molntjänst prövas var för sig.
- Alingsås kommun inte går in i nya molntjänster som innebär tredjelandsöverföring av personuppgifter till land som enligt EU-kommissionen inte uppnår adekvat skyddsnivå.
- Det är ej lämpligt att information som omfattas av sekretess delas i molntjänster/drifttjänster som inte lyder under svensk lag.

Ställningstagandet tillkom för att samtliga berörda tjänstepersoner dels kontinuerligt ska träffas och se över hur rättsläget ser ut på området, och dels för att dessa ska lämna stringent rådgivning i frågorna, både internt inom kommunledningskontoret som externt till övriga förvaltningar, bolag och förbund. Ställningstagandet är framförallt relevant vid upphandling av nya leverantörer. I och med detta blir dataskyddsorganisationens roll i upphandlingsprocessen av mycket stor vikt.

Under 2023 kommer fokus att läggas på att göra upp åtgärdsplaner för hur kommunens olika personuppgiftsansvariga ska kunna hitta alternativa leverantörer och lösningar för att så snart som möjligt kunna sluta använda de tjänster som inte är lagliga.

Utvärdering av ledningssystemets effektivitet

Historisk data saknas och därmed finns inget att jämföra med för bedömning om arbetes effektivitet. Arbetet är utarbetat utefter beprövade och standardiserade metoder för att på sikt säkerställa önskade resultat.

Rekommendationer

Rekommendationer till förbättringar och aktiviteter framgår av förslag till Handlingsplan för informationssäkerhet och dataskydd 2023, enligt kommunfullmäktiges informationssäkerhetspolicy.

Bilagor
Bilaga 1 – Uppföljning Handlingsplan för informationssäkerhet & dataskydd 2022