Handleplan for informationssikkerhed 2025

Forord

I en tid præget af ustabilitet og krig i Europa står vi over for et højt cybertrusselsniveau mod det danske sundhedsvæsen. Nye teknologiske løsninger skaber samtidig flere muligheder for cyberkriminelle for at udføre sofistikerede angreb mod kritisk infrastruktur og systemer. Da løsningen af sundhedssektorens kerneopgaver i stigende grad er bundet op på brug af sundhedsdata, der dagligt tilgås i mange kritiske it-systemer, er det vigtigere end nogensinde før, at vi har styr på vores informationssikkerhed.

Region Midtjylland udarbejder hvert år en handleplan for informationssikkerhed som et redskab til at samle udviklingsinitiativer, der skal styrke og modne arbejdet med informationssikkerhed i regionen. Handleplanen for informationssikkerhed 2025 består af fem tematiske spor, der danner rammen for arbejdet. I 2025 vil der bl.a. være fokus på implementering af NIS2-direktivet, som stiller skarpe cybersikkerhedskrav, og AI-forordningen, der handler om at sikre ansvarlig udvikling, brug og udbredelse af AI-løsninger. Vi vil desuden følge den kommende EHDS-forordning (European Health Data Space), som skal skabe mulighed for mere fleksibel deling af sundhedsdata på tværs af EU-lande.

Sideløbende med indsatserne i handleplanen har Region Midtjylland også vedvarende fokus på de mange driftsopgaver, der hver dag bidrager til at øge regionens sikkerhedsniveau. Vi har bl.a. en stærk styring af bruger- og adgangskontrol, og det sikres, at nye systemer risikovurderes, samt at der udarbejdes letforståelige retningslinjer og vejledninger til regionens medarbejdere.

Handleplanen har til formål at sikre, at regionen kontinuerligt arbejder målrettet med de mest relevante informationssikkerhedsindsatser. Derfor skal handleplanen også forstås som det udgangspunkt, regionen arbejder ud fra. Lovgivning, teknologi og de konkrete trusler mod cyber- og informationssikkerheden udvikler sig hele tiden. Derfor tilpasser Region Midtjylland løbende sine prioriteringer og fokusområder efter behov, og handleplanen skal derfor ses som en dynamisk plan, der kan ændres og tilpasses efter det aktuelle trusselsbillede.

Handleplanen for informationssikkerhed viser Region Midtjyllands engagement i at beskytte de følsomme og fortrolige data, som borgerne betror os hver dag. Målet er at sikre, at dataene håndteres korrekt i forbindelse med patientbehandling, og at borgerne forsat kan have tillid til, at deres oplysninger beskyttes på betryggende vis. Samtidig er handleplanen et udtryk for, at ikke alle sikkerhedsrisici kan nedbringes fuldstændigt, og at der derfor er behov for en skarp prioritering af indsatserne. På den måde får regionen – og dermed også borgere og patienter - mest mulig sikkerhed for de tilgængelige ressourcer, hvilket er i tråd med Region Midtjyllands risikobaserede tilgang til arbejdet med informationssikkerhed.

Oversigt

Spor 1 AI - Anvendelse og lovgivning

De seneste år har vi set store fremskridt inden for kunstig intelligens (AI). Selvom AI ikke er et nyt koncept, har teknologien først for nylig fået en væsentlig rolle i vores hverdag, især med udbredelsen af generative AI-systemer som ChatGPT. Siden lanceringen 2022 har sådanne systemer skabt både begejstring og bekymring på verdensplan. AI er blevet identificeret som en nøglekomponent i løsningen af komplekse udfordringer, også inden for sundhedssektoren. Med en forventet mangel på sundhedspersonale i fremtiden er der et presserende behov for effektive løsninger. AI kan spille en afgørende rolle ved at understøtte, effektivisere og smidiggøre kliniske og administrative arbejdsgange.

I sundhedssektoren kan AI også forbedre diagnosticeringen betydeligt. AI-værktøjer kan analysere medicinske billeder hurtigt og præcist, hvilket kan føre til tidligere og mere præcise diagnoser. Dette er afgørende for sygdomme som bl.a. kræft, hvor tidlig opdagelse kan redde liv. Selvom AI kan effektivisere og løse mange opgaver, er der også stor usikkerhed forbundet med disse løsninger. Derfor har EU fokuseret på regulering af området, og i 2024 blev AI-forordningen vedtaget. Denne stiller en række krav til organisationer, der udvikler, bruger eller tilbyder AI-løsninger inden for EU's grænser.

Region Midtjylland skal i 2025 arbejde med implementering af AI-forordningens krav samt dokumentation herfor. Forordningen klassificerer AI-systemer efter risikoniveau, og højrisikosystemer, som mange sundhedsrelaterede AI-systemer falder ind under, skal overholde strenge krav til transparens, dokumentation og sikkerhed. Regionen skal sikre, at disse systemer underkastes grundige risikovurderinger, konsekvensanalyser og løbende overvågning. Brugen af AI-løsninger kan også medføre store databeskyttelsesretlige udfordringer, da AI løsninger indebærer behandling af store mængder af ofte følsomme personoplysninger. Selskaberne bag AI-løsningerne har ikke altid tilstrækkelig kontrol over de data, der bruges til at træne de bagvedliggende modeller eller de data, som brugerne indtaster. Ved brug af AI-løsninger skal regionen derfor fremadrettet samtænke efterlevelse af AI-forordningen med vores kontinuerlige fokus på GDPR. Region Midtjylland vil i samarbejde med de øvrige regioner søge at afdække samspillet mellem disse to lovkomplekser og de krav, de sammen stiller til brug af AI, så regionen kan bygge videre på det fundament og de erfaringer med GDPR-efterlevelse, vi allerede har opbygget.

Region Midtjyllands arbejde med AI forordningen skal sikre, at teknologien udnyttes på en forsvarlig og betryggende måde med respekt for etiske retningslinjer og gældende lov. Dette indebærer at etablere klare retningslinjer og procedurer for brugen af AI. Derudover skal der være fokus på løbende uddannelse og træning af medarbejdere i brugen af AI-teknologier - i overensstemmelse med de krav, som AI-forordningen stiller til uddannelse af medarbejdere, der skal udvikle, anvende og føre kontrol med AI-systemer. Dette er afgørende for at opnå en bæredygtig, lovlig og effektiv anvendelse af AI.

I 2025 vil informationssikkerhedsfunktionen understøtte Region Midtjyllands arbejde for at inkorporere de bedste AI-løsninger til det daglige arbejde, samtidig med at regionen følger lovgivningen og interne retningslinjer. Et eksempel kunne være en generativ AI-løsning, som skanner alle interne retningslinjer og giver medarbejderne hurtige, brugbare svar på konkrete spørgsmål og dermed understøtter regionens arbejde med at overholde interne retningslinjer i hele organisationen. Regionen arbejder også på anskaffelse af en AI-løsning til skanning af billeder fra brystkræftscreening, som skal effektivisere arbejdet med vurderingen af billeder fra screening af lavrisikopatienter. Løsningen forventes implementeret i løbet af 2025.

Spor 2 Compliance og rapportering

Der har længe været fokus på regulering af den digitale sfære i EU. Også i 2025 er der nye krav til informations- og cybersikkerhed på vej i form af nye EU-forordninger og -direktiver. Foruden den allerede omtalte AI-forordning skal Region Midtjylland arbejde videre med implementering af NIS2-direktivet og den nye EHDS-forordning (European Health Data Space).

NIS2 udvider det oprindelige NIS-direktiv omkring net- og informationssikkerhed fra 2016 og skærper cybersikkerhedskravene til organisationer, der leverer samfundskritiske tjenester i EU. Selve NIS2-direktivet er vedtaget og finder anvendelse fra oktober 2024, men den danske lov, som skal fortolke direktivet og implementere det i dansk ret, er forsinket og forventes først vedtaget i starten af 2025. Arbejdet med NIS2 implementering er allerede igangsat i Region Midtjylland, hvor fokus i første omgang har ligget på at identificere de dele af direktivteksten, som uanset den danske implementeringslov kommer til at kræve øget fokus i regionens arbejde med cybersikkerhed. Der er bl.a. krav om øget fokus på uddannelse, leverandørstyring, risikostyring og rapportering af sikkerhedshændelser, som regionen skal arbejde målrettet med i 2025. Herudover skal regionen i 2025 analysere den danske implementeringslov for at afdække, hvilke yderligere krav denne stiller til vores arbejde med cybersikkerhed, hvorefter indsatsen justeres ved behov.

I april 2024 blev der indgået en politisk aftale om den nye EHDS-forordning (European Health Data Space), som forventes at blive endeligt vedtaget i 2024 og få virkning gradvist i løbet af 2026-2030. EHDS-forordningen har til formål at give individer øget kontrol over egne sundhedsdata og fremme muligheden for fleksibel sundhedspleje – via øget deling af data - på tværs af unionens landegrænser. EU-forordninger - modsat direktiver - finder direkte anvendelse i medlemslandene uden behov for en national implementeringslov. Derfor vil Region Midtjylland, i samspil med de øvrige regioner, arbejde med at analysere lovteksten fra EHDS-forordningen, når den er endeligt vedtaget – i første omgang med fokus på at identificere de nye krav der stilles, som forventeligt vil gøre sig gældende allerede fra 2026.

I arbejdet med informationssikkerhed anvender Region Midtjylland den internationale standard ISO27001/2 som rammeværk. Herudover arbejdes der i samarbejde med de øvrige regioner målrettet med de mere tekniske CIS-18 kontroller inden for cybersikkerhedsområdet. Regionens arbejde med at efterleve kravene i disse rammeværker er med til at skabe kontinuerlige forbedringer på informations- og cybersikkerhedsområdet og danner et solidt fundament, der vil bidrage effektivt til regionens overholdelse af de mange nye lovkrav, der er på vej – lige så vel som arbejdet også understøtter den fortsatte indsats omkring efterlevelse af bl.a. databeskyttelsesforordningen.

Region Midtjylland vil i 2025 arbejde på at værktøjsunderstøtte arbejdet med informationssikkerhed ved at anskaffe og implementere et ISMS (Information Security Management System). Dette skal facilitere en mere holistisk og ensartet tilgang til arbejdet og skabe overblik over udfordringer og resultater af kontroller, som kan anvendes til en endnu bedre rapportering, der kan danne grundlag for prioritering af indsatserne. Dette værktøj har potentiale til at skabe et overblik over den nødvendige dokumentation for compliance på ét sted.

Spor 3 Beredskab og cybersikkerhed

I takt med at teknologien fylder mere og mere i behandlingen, og trusselbilledet samtidig bliver mere komplekst, er en god it-beredskabsplan afgørende. Beredskabsplanens vigtigste funktion er, at alle skal vide, hvordan de skal handle, hvis teknologien svigter - men også at sikre, at de teknologiske løsninger virker optimalt. Der stilles krav til både håndtering og indhold i regionens beredskabsplan fra flere fronter, ligesom it-beredskabet indgår som en central del af regionens samlede beredskabsplanlægning. I NIS2-direktivet stilles der krav til, at regionen løbende udvikler beredskabsplanerne for at minimere virkningen af sikkerhedshændelser. Derudover indeholder CIS-18 konkrete anbefalinger og målinger, der viser regionens evne til at reagere og håndtere angreb såvel som evnen til at komme tilbage til normal drift.

Opgaven med at opdatere Region Midtjyllands it-beredskabsplan er igangsat i 2024 for at sikre, at både teknologiske og regulatoriske krav bliver indarbejdet, og så det fremtidige arbejde med vedligeholdelse af beredskabsplanen bliver rammesat i et årshjul. Ud over opdateringen af planen vil der i 2025 især være fokus på test af beredskabsplanen. Der vil fremover findes årshjul med testplaner for både egne interne test samt deltagelse i de fællesregionale og nationale initiativer for test af beredskab.

Aktivering af beredskabet stiller krav til de værktøjer, der anskaffes til sikring og overvågning af it-infrastrukturen. Region Midtjylland har løbende haft fokus på anskaffelse af effektive systemer, der følger den hastige udvikling inden for cybersikkerhed. Disse systemer sikrer dels, at hackere får sværere ved at komme ind, men også at afvigende adfærd hurtigt spottes og stoppes. I 2025 vil der især blive sat fokus på penetrationstest, så disse test i højere grad bliver systematiseret og udføres efter årshjul, hvor graden af fortrolighed i data og systemets kritikalitet danner grundlag for prioritering.

Typisk har cyberangreb været rettet mod infrastrukturer via computere og mobiltelefoner, men trusselsbilledet er i dag mere komplekst. Center for Cybersikkerhed har den seneste tid hævet trusselsniveauet på IoT (internet of things) og OT-udstyr (operational technology). IoT-udstyr er udstyr, der er designet til at have internetforbindelse. Det kan f.eks. være overvågningskameraer, konferenceudstyr, kliniske patientovervågningssystemer samt måleudstyr og sensorer. OT-udstyr er udstyr, der i højere grad er designet til at være en del af et netværk, men ses i stigende grad også på internettet. Fælles for disse typer af udstyr er, at det ofte har svage passwords, mangler brugerstyring og sikkerhedsopdateringer kan være mangelfulde eller ikke-eksisterende. For mange, der anvender udstyret, er driftsstabiliteten og tilgængeligheden ofte vigtigere end sikkerhed.

Den øgede anvendelse af udstyr på det medicotekniske område, der netværksopkobles (OT eller IoT), stiller krav til et større fokus på sikringsforanstaltninger på dette område. Der kan være tale om både øget overvågning, øget fokus på sikkerhedsopdateringer og bedre muligheder for at segmentere og isolere eventuelle sårbare komponenter.

I forbindelse med de årlige målinger på CIS-18 af regionens sikkerhedsniveau vil OT- og IoT-området fra 2024 gradvist blive inddraget, således at sikkerhedsniveauet på dette område bliver afdækket med henblik på mulige forbedringer af sikkerheden.

Spor 4 Awareness

Region Midtjylland arbejder målrettet med awareness i forhold til informationssikkerhed. Hver hospitalsenhed samt social- og psykiatriområderne har fået ansat lokalt forankrede persondatakonsulenter, som bidrager til at hæve vidensniveauet på enhederne. Persondatakonsulenterne hjælper bl.a. det kliniske personale med at afklare og sikre de rette kommunikationskanaler, og de rådgiver om opbevaring af personoplysninger og GDPR-regler.

Hvert år udarbejdes en række awarenesskampagner med forskellige temaer, der er med til at klæde medarbejderne yderligere på i forhold til at håndtere forskellige udvalgte situationer korrekt. Disse kampagner bliver tilrettelagt i samspil mellem regionens centrale awarenessteam og de lokale persondatakonsulenter, der bidrager med nyttig viden om de informationssikkerhedsmæssige problemstillinger, som klinikerne står overfor. I 2025 vil disse kampagner f.eks. fokusere på sikker brug af AI-løsninger samt opmærksomhed på diskretion i venteværelser.

Som medarbejder i Region Midtjylland er den primære opgave at gøre en positiv forskel for patienter og borgere. Til denne opgave benyttes rigtig meget teknologi. For at sikre at regionens medarbejdere kan have fokus på kerneopgaven, er det vigtigt, at alle har klare og letforståelige retningslinjer at følge omkring brugen af disse teknologier. Derfor vil der i 2025 blive udarbejdet "Vilkår for anvendelse af Region Midtjyllands computere, mobiltelefoner og tablets samt regionens data". Det er en beskrivelse til alle ansatte, der indeholder oplysninger om, hvilke betingelser der er gældende for f.eks. mobiltelefoner. Dette skal sikre, at alle brugere har en klar forståelse for, hvad der forventes af dem og hvilke handlinger, der ikke er tilladte. Dette vil hjælpe med at opretholde en sikker og stabil brugeroplevelse og sikre, at regionens data ikke bruges til uautoriserede formål eller eksempelvis opbevares uforsvarligt på private mobile enheder.

Med implementering af kontorpakken M365 er der mange nye muligheder for optimerede arbejdsgange og for en lettere dokumenthåndtering. Desværre giver det også mulighed for, at data placeres uhensigtsmæssigt og glemmes, så regler og krav til journalisering og sletning ikke overholdes. Der skal derfor udarbejdes vejledningsmateriale til medarbejderne i god journaliseringsskik.

Sociale medier anvendes til flere formål i Region Midtjylland. For at sikre at vi til stadighed beskytter patienters privatliv og overholder gældende lovgivning, er der sat et arbejde i gang med at udarbejde retningslinjer, der beskriver korrekt og sikker brug af sociale medier. Retningslinjerne forventes implementeret primo 2025.

NIS2-direktivet stiller også skærpede krav til awarenessindsatsen. I 2025 skal regionen, foruden de planlagte kampagner, arbejde målrettet med uddannelse af topledere inden for cybersikkerhed, så de opnår en basal forståelse for arbejdet med cybersikkerhedsrisici. Region Midtjylland underviser allerede den brede kreds af ansatte i basal informationssikkerhed i form af et e-læringskursus, som alle nyansatte skal gennemføre. Men NIS2 stiller krav til uddannelse af den brede medarbejderkreds, der rækker ud over regionens nuværende indsats. Derfor skal regionen i 2025 undersøge, om den nuværende e-læring skal revideres og/eller suppleres med nyt materiale, samt hvordan denne awarenessindsats kan dokumenteres.

Spor 5 Kontrakt- og leverandørstyring

Region Midtjylland har mange samarbejdsflader til eksterne partnere, der leverer forskellige it-systemer og -services til regionen. At holde styr på de mange kontrakter og de nødvendige informationssikkerhedskrav er en kompleks opgave. I 2024 er der igangsat et projekt, der skal sikre, at Region Midtjylland i højere grad arbejder risikobaseret, kosteffektivt og i overensstemmelse med lovgivningen i leverandørsamarbejder. Projektet er forankret på tværs af relevante enheder og har et særligt fokus på at få indarbejdet og forankret informationssikkerhed ved kontraktindgåelse, i leverandørstyringen samt ved leverandørkontrol.

En af projektets centrale dele er at sikre, at informationssikkerhedsmæssige krav bliver tænkt ind tidligt i processen, når nye it-løsninger anskaffes. Dette skyldes, at sen inddragelse af krav til informationssikkerhed kan skabe unødige forsinkelser og øgede omkostninger i forbindelse med eksempelvis påkrævede systemjusteringer hos leverandøren, såvel som det kan hindre et gnidningsfrit samarbejde mellem de interne og eksterne interessenter, der er involveret i samarbejdet.

Projektet omkring kontrakt- og leverandørstyring viderebringer det tidligere handleplansinitiativ, *Informationssikkerhed fra start*, som havde til formål at udvikle et værktøj til tidlig screening af potentielle nye leverandørsamarbejder. Dette screeningsværktøj skulle sikre, at de rette informationssikkerhedsmæssige krav fastlægges tidligt i processen for anskaffelse af nye it-løsninger, og at kravene som resultat heraf stilles rettidigt til leverandørerne, når nye kontrakter skal indgås.

Screeningsværktøjet er udviklet og har været afprøvet i en pilotfase i regionens proces for mindre udviklingsopgaver i Digitalisering og It. Yderligere implementering af dette værktøj spiller ind i det bredere arbejde omkring kontrakt- og leverandørstyring, hvor screeningsværktøjet inkorporeres i de indledende faser af kontrakt- og leverandørstyringsprocessen.

Arbejdet med kontrakt- og leverandørstyring skal dække både nye anskaffelser og leverandørsamarbejder, såvel som de kontrakter vi allerede har indgået, og som har en historik, der rækker tilbage til en tid, hvor kompleksiteten ikke var så høj, og der ikke på samme måde blev stillet krav til leverandører og samarbejdspartnere omkring informationssikkerhed.

Målsætningen er, at der skal defineres og implementeres en samlet styringsmodel. Styringsmodellen skal bidrage til effektivisering af kontrakt- og leverandørstyring, så processen i højere grad understøtter organisationens daglige arbejde og sikrer efterlevelsen af de informationssikkerhedsmæssige krav.

I 2025 vil Region Midtjylland påbegynde arbejdet med at implementere og idriftsætte den overordnede styringsmodel for kontrakt- og leverandørstyring - inkl. *Informationssikkerhed fra start* - bredt i organisationen.