Delstrategi for cyber- og informationssikkerhed 2025-2028

Region Syddanmarks digitaliseringsstrategi fra 2025 sætter rammen for arbejdet med cyber- og informationssikkerhed i de kommende år. Delstrategien for cyber- og informationssikkerhed skal med udgangspunkt heri beskrive, hvordan ambitionerne i digitaliseringsstrategien indfries frem til 2028 ved bl.a. at ”identificere målrettede indsatser, som kan bidrage til at forbedre regionens evne til at forudse, forebygge, opdage og håndtere sikkerhedstrusler”.

Borgere og patienter er omdrejningspunktet

Digitale løsninger spiller allerede en stor rolle i sundhedsvæsenet i dag, og vil fremover kun komme til at spille en endnu større rolle. Ambitionerne for den digitale udvikling på sundhedsområdet er høje, og Region Syddanmarks digitaliseringsstrategi giver rammerne for at sætte yderligere skub i den digitale transformation i de kommende år. Målet er bedre og smidigere digital understøttelse af både borgere, patienter og sundhedspersonalet, der kan frigøre tid til opgaver med behandling og pleje og til den enkelte patient.

Med den øgede digitalisering af sundhedsvæsenet skabes der samtidig øgede trusler og sårbarheder, både i forhold til cybersikkerhed og informationssikkerhed. Jo flere arbejdsgange, der er digitalt understøttede, og jo flere oplysninger, der alene opbevares og deles digitalt, jo større er risikoen for, at nedbrud af it-systemer kan lamme sundhedsvæsenets muligheder for at yde behandling og pleje til patienter.

At håndtere og opbevare borgernes og patienternes data på en sikker måde er afgørende for tilliden til sundhedsvæsenet. Det gælder både generelt i forhold til at leve op til lovgivningen f.eks. GDPR-forordningen, men også i forhold til cybertrusler, hvor beskyttelsen af data kan blive kompromitteret.

For at højne it-sikkerheden fastsætter Region Syddanmark hvert år en række konkrete mål, der sætter fokus på de emner, hvor implementeringen af regionens retningslinjer for informationssikkerhed og dermed beskyttelsen af data og følsomme oplysninger med fordel kan styrkes yderligere. Erfaringen fra tidligere år viser, at fastsættelsen af konkrete årlige mål skærper organisationens opmærksomhed på relevante arbejdsgange og sikkerhedstiltag i det daglige. Arbejdet med årlige mål for informationssikkerhed videreføres derfor også i denne strategiperiode med det formål at konsolidere regionens efterlevelse af gældende lovkrav og internationale standarder yderligere.

Hvad er it-, informations- og cybersikkerhed?

It-sikkerhed består af såvel cybersikkerhed som informationssikkerhed. Det dækker blandt andet over sikkerhed omkring data og it-systemer. It-systemer omfatter hardware og software.

Informationssikkerhed er en bred betegnelse for de samlede foranstaltninger til at sikre informationers fortrolighed, integritet og tilgængelighed. Informationssikkerhed relaterer sig til forskellige typer foranstaltninger: herunder både organisatoriske, personrelaterede, fysiske og teknologiske.

Cybersikkerhed omfatter de tiltag og handlinger, som regionen foretager for at forebygge og sikre sig mod sikkerhedsbrud, der kan opstå som følge af angreb mod regionens digitale systemer eller data. Det omhandler blandt andet sikkerheden i netværksforbundne it-systemer. Netværket kan være isoleret eller forbundet til andre netværk som for eksempel internettet.

Kilde: Styrelsen for Samfundssikkerhe

Sundhedssektorens cyber- og informationssikkerhedsmæssige kendetegn:

- Stigende digitalisering
- Komplekst it-landskab
- Behandling og deling af sundhedsdata
- Mange aktører med forskellig modenhed på cyber- og informationssikkerhed
- Personale med forskellige forudsætninger for cyber- og informationssikkerhed

Kilde: Sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025

Trusselsniveauet er højt

De seneste års udvikling i den geopolitiske situation særligt i Europa betyder, at det generelle trusselsbillede er langt mere alvorligt end tidligere. Med oprettelsen af Ministeriet for Samfundssikkerhed og Beredskab og udstedelsen af generelle anbefalinger om at forberede sig på kriser, hvor der er mangel på strøm, vand og dagligvarer mm., er alvorligheden i trusselsbilledet kun blevet mere nærværende for hele befolkningen. For Region Syddanmark – og helt generelt - er det særligt cybertruslen, som er stigende, og det er derfor også den mest sandsynlige form for angreb, som sundhedsvæsenet kan blive ramt af.

Sundhedssektoren er en samfundskritisk sektor, som cyberkriminelle eller fjendtligt indstillede stater kan have store interesser i at ramme. Men sundhedssektoren kan også blive ramt af fjendtlige angreb på kritisk infrastruktur som strømforsyning, vandforsyning, netværksforbindelser mm. Der er derfor mere end nogensinde brug for at investere i at sikre regionens interne systemer såvel som eksterne systemer (via leverandører) mod cyberangreb og afværge de skader, som et evt. angreb ville kunne have.

Der er i den forbindelse også behov for fornyede overvejelser om fysisk sikkerhed på regionens lokationer, som ikke indgår i cyber- og informationssikkerhedsopgaven – og dermed denne delstrategi - men er nært beslægtet.

I Sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025 identificeres fire strategiske målsætninger for sundhedssektorens arbejde med cyber- og informationssikkerhed. Arbejdet med disse målsætninger indgår i denne strategi, og afspejles således i aktiviteterne under de fire spor: Forudse, forebygge, opdage og håndtere, som er beskrevet i de næste kapitler.

Strategiske målsætninger fra Sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025:

- Sektoren skal øge robustheden overfor cyber- og informationssikkerhedshændelser
- Et højt niveau af cyber- og informationssikkerhed skal sikre tryghed hos borgeren
- Sundhedspersonalet skal kunne arbejde sikkert med teknologi og data
- Samarbejdet skal styrkes på tværs af de kritiske sektorer og sundhedssektorens egne aktører.

En risikobaseret tilgang

Risikobilledet er i konstant bevægelse – og det er afgørende at kunne tilpasse sig den udvikling. Derfor fortsætter Region Syddanmark sin risikobaserede tilgang til sikkerhedsarbejdet i denne strategi. Det indebærer, at strategiens aktiviteter undervejs i strategiperioden kan justeres og tilpasses i forhold til de aktuelle risici og trusler, som regionen står overfor. Strategien beskriver derfor de overordnede generelle områder, værktøjer og metoder, som indgår i sikkerhedsarbejdet. Mens de specifikke tiltag og aktiviteter kan skifte undervejs alt efter udviklingen i teknologier, trusselsbillede og sårbarheder. En risikobaseret tilgang muliggør, at sikkerhedsarbejdet løbende kan prioriteres og sættes ind der, hvor behovet og effekten er størst.

I den digitale udvikling af sundhedsvæsenet er det afgørende, at cyber- og informationssikkerhed er en aktiv medspiller, og at sikkerhed er et væsentligt og naturligt hensyn i udvikling, anskaffelse og implementering af alle it-systemer og digitaliseringsprojekter.

Denne delstrategi for cyber- og informationssikkerhed tager derfor som nævnt ovenfor afsæt i Region Syddanmarks digitaliseringsstrategi, sundhedssektorens strategi for cyber- og informationssikkerhed 2023-2025, den tidligere strategi for cyber- og informationssikkerhed i Region Syddanmark og andre relevante strategier på området.

Sikkerhedsarbejdet rammesættes desuden af standarder inden for ISO-2700-serien, GDPR-forordningen, NIS2-direktivet samt AI-forordningen, og internationale standarder for sikkerhedsarbejdet. For uddybning se faktaboksen.

ISO27000-serien:

ISO27000-serien er en international standard til etablering af et ledelsessystem for informationssikkerhed. Standarden tager udgangspunkt i en risikobaseret tilgang.

GDPR-forordningen:

GDPR står for “General Data Protection Regulation” og kaldes i almindelig tale for persondataforordningen. Databeskyttelsesforordningen er en EU-forordning, som har til formål at styrke og harmonisere beskyttelsen af personoplysninger i Den Europæiske Union.

NIS2-direktivet:

Formålet med EU's Net- og Informationssikkerhedsdirektiv (NIS2) er at yderligere styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU for virksomheder inden for en lang række sektorer og for offentlige myndigheder, som anses for at være kritiske for økonomien og samfundet.

AI-forordningen:

Forordningen om kunstig intelligens (Artificial Intelligence) er en EU-forordning, der har til formål at regulere anvendelsen af kunstig intelligens inden for EU. Forordningen etablerer en fælles lovgivningsmæssig ramme for kunstig intelligens i Den Europæiske Union.

Skal understøtte et øget sikkerhedsniveau

Sikkerhedsniveauet måles ved hjælp af rammeværktøjet CIS18, der er udviklet af Center for Internet Security (CIS). Rammen repræsenterer en omfattende og struktureret tilgang til cybersikkerhed inden for 18 overordnede temaer.

Region Syddanmark har sammen med de øvrige regioner forpligtet sig til at nå et fælles sikkerhedsmål på 3,75 på CIS18-skalaen. I 2024 opnåede Region Syddanmark en score på 3,08, som repræsenterede en væsentlig fremgang fra den seneste måling i 2022 på 2,70 og fra den første måling i 2019 på 1,70. Sikkerheden er dermed allerede væsentligt forbedret gennem arbejdet med de tidligere strategier for cyber- og informationssikkerhed, og denne delstrategi bygger videre på det arbejde.

FORUDSE

At forudse handler om at have kendskab til potentielle cybertrusler, sikkerhedsrisici og sårbarheder, inden de udgør en reel fare for sikringen af følsomme personoplysninger og patientbehandlingen. Det handler om hele tiden at være et skridt foran og at styrke sikkerheden omkring sygehusenes it-drift og håndteringen af borgernes data. Det er en forudsætning for, at regionen som helhed kan træffe de rette beslutninger i forhold til styringen af risici, og at den enkelte medarbejder kan iværksætte de nødvendige sikkerhedsprocedurer. Regionens evne til at forudse potentielle sikkerhedshændelser skal derfor fortsat styrkes.

Risikostyring

Den risikobaserede tilgang anvendes allerede i dag i forhold til mange arbejdsgange i Region Syddanmark. En proaktiv tilgang til styringen af potentielle risici er afgørende for at kunne forudse it-kriminelles metoder og forsøg på cyberangreb. Det handler om hele tiden at være på vagt og indhente viden om mulige trusler og sårbarheder, der kan kompromittere sikkerheden. Det handler også om at sætte ind der, hvor risikoen er størst. Når risici opgøres harmoniseret på tværs af fagområder og sygehusenheder, bliver det muligt at identificere "det svageste led", og dermed målrette indsatsen der, hvor risikoen er størst.

Risikostyringskoncept – roller og ansvar

For at styrke en mere ensartet tilgang skal det fælles risikostyringskoncept styrkes, så det i højere grad tydeligt definerer fælles principper og arbejdsgange for risikostyring på tværs af regionens enheder. Som organisation er Region Syddanmark bygget op i en kompleks struktur med mange niveauer af ledelse og forskellige fag- og funktionsområder. Det stiller særlige krav til tydelighed i roller og mandat, herunder placering af ansvar for koordinering af sikkerhedstiltag på tværs af organisationen. Der er på samme måde behov for tydeligt at beskrive opgaver for it-systemansvarlige i regionen. Denne proces er allerede i gang, og skal i løbet af strategiperioden udbygges yderligere. Udbredelsen af fælles sprog og referencerammer bidrager til at minimere misforståelser og styrke kvaliteten i beslutnings- og løsningsprocesser.

Systemunderstøttelse til risikovurdering

Systemunderstøttelse er væsentligt for at gøre det nemmere og mere ensartet for medarbejderne at praktisere en systematiseret risikostyring, og giver mulighed for relevant dataindsamling. Den eksisterende systemunderstøttelse til udarbejdelse af risikovurderinger (Integrated Risk Management-modul i Service-Now) skal derfor optimeres og udbygges til at favne flere systemer.

Dette understøtter opbyggelsen af en endnu stærkere sikkerhedskultur, og gør det samtidigt nemmere for medarbejdere, borgere og patienter at anvende it-systemer og digitale løsninger sikkert og trygt. Det skal være nemt at gøre det rigtige, og svært at begå fejl, der potentielt kan føre til sikkerhedshændelser.

Dokumentation

For at sikre en effektiv og relevant risikostyring er der brug for et aktuelt og tidstro overblik over organisationens sikkerhedssituation. Dette understøttes blandt andet ved hjælp af løbende dokumentation og rapportering. Det drejer sig eksempelvis om dokumentation for risikovurderinger, tilsyn med indgåede databehandleraftaler, log og logopfølgning eller hvornår og hvordan kontrol på brugeradgange til systemer er gennemført, mv. Korrekt dokumentation anvendes også til at sammenholde og analysere data for at kunne vurdere forskellige risici og prioritere tiltag i forhold til konkrete sårbarheder og trusler.

Det styrker samtidig regionens evne til at samarbejde med eksempelvis andre regioner og myndigheder, hvor der kan være behov for at indrapportere sammenlignelige data omkring bestemte forhold. Når man ved hjælp af den løbende dokumentation har de nødvendige data til rådighed, kan man hurtigt på baggrund heraf

vurdere og forudse konkrete trusler. Sidst men ikke mindst understøtter et godt datagrundlag og løbende dokumentation muligheden for at skabe tillid og tryghed hos borgere og patienter og samarbejdspartnere, når organisationen til hver en tid kan dokumentere gennemførelsen af sikkerhedstiltag.

Denne dokumentation skal systemunderstøttes, og så vidt muligt integreres i regionens it-styringsplatform ServiceNow. De eksisterende procedurer for dokumentation og rapportering skal derfor skærpes yderligere, og udbygges i et fælles koncept for hele organisationen for at skabe et endnu bedre overblik over den samlede sikkerhedssituation. Der skal være fokus på både digital og fysisk sikring af information. Konceptet skal ledsages af kompetenceudvikling for berørte ledere og medarbejdere.

Netværkssamarbejde - videndeling om globale trusler og sikkerhedsbehov
Sparring med interne og eksterne samarbejdspartnere om aktuelle risici og angrebsflader skærper regionens opmærksomhed og evne til at forudse potentielle farer. Region Syddanmark har gennem årene etableret et stærkt netværkssamarbejde med relevante aktører, der blandt andet har til opgave at overvåge og analysere truslen fra cyberkriminelle mod danske virksomheder og offentlige myndigheder. Dertil har Region Syddanmark også opbygget et samarbejde med europæiske og internationale sikkerhedsaktører, der kan dele viden om globale trusler og sikkerhedsbehov. Dette netværkssamarbejde vil fortsat være i fokus i den kommende strategiperiode med henblik på løbende at styrke regionens evne til at forudse potentielle risici. Det samme gælder videndeling og sparring i forhold til at forebygge, opdage og håndtere sikkerhedstrusler.

FOREBYGGE

Forebyggelse af sikkerhedshændelser relaterer sig til en bred vifte af indsatsområder, herunder medarbejderadfærd, samarbejdet med leverandører, sikkerhedsarkitektur, kontrol med brugeradgange til regionens it-systemer m.m. Det handler også om implementeringen af de regler og retningslinjer, der skal skabe sikre rammer og arbejdsgange i forhold til sikker håndtering af data og it-udstyr.

Regionen skal fortsat styrke sikkerheden i centrale it-systemer såvel som borgernært behandlingsudstyr og leve op til de gældende lovkrav og regulering på området.

Sikkerhedsarkitektur og –infrastruktur

Region Syddanmark har fokus på at skabe sammenhæng og ensartethed på tværs af organisationens applikationslandskab og it-infrastruktur. Det er en væsentlig forudsætning for at kunne implementere sammenhængende og ensartede sikkerhedstiltag. Det er nødvendigt at kende it-landskabet for at kunne beskytte det, og et mere enkelt digitalt landskab er nemmere at beskytte. Det handler blandt andet om at identificere de områder, som med fordel kan forenkles og konsolideres for at skabe et bedre overblik og dermed større robusthed. Denne indsats bygger videre på tidligere tiltag til styring af it-systemer og it-udstyr. I den kommende strategiperiode skal indsatsen fortsat have fokus på, at implementering af nye it-løsninger samt ændringer i de eksisterende systemer sker baseret på et fælles og mere harmoniseret sikkerhedsgrundlag. Formålet er hele tiden at nedbringe kompleksiteten og opretholde et effektivt overblik. Dette understøtter for eksempel opgaven med løbende at føre kontrol over hvilket udstyr, der har adgang til netværket, samt hvilke netværksadgange, der tildeles det enkelte udstyr.

Netværkssegmentering
Indsatsen med at robustgøre regionens netværk gennem segmentering for at forebygge spredning af angreb fortsættes. Dette opnås ved at inddele it-systemer i indhegnede segmenter med henblik på at kunne standse en fjendtlig aktørs indtrængen og afgrænse angrebet til det pågældende segment. Dermed forebygges det, at cybertrusler kan sprede sig fra en del af netværket til resten af netværket i andre dele af organisationen.

Identitets- og adgangsstyring

Formålet med identitets- og adgangsstyring er at understøtte, at kun de relevante personer kan få adgang til organisationens data og ressourcer. Region Syddanmark har allerede implementeret grundige procedurer for oprettelse, nedlæggelse og regelmæssig kontrol af adgange til regionens it-systemer. Dermed understøttes det, at det kun er de rette brugere, der har adgang til de rette systemer og på de rette tidspunkter. Denne indsats skal have fokus på at forbedre de eksisterende procedurer gennem blandt andet øget it-understøttelse og automatisering af kontroller. Dertil skal indsatsen have fokus på skærpet kontrol af de brugere, der qua deres rettigheder potentielt kan udsætte regionen for øget risiko. Det gælder eksempelvis brugeradgange for administratorer med privilegerede rettigheder. Parallelt fortsættes det løbende modningsarbejde i at oprette, flytte og nedlægge brugeradgange rettidigt og korrekt samt løbende kontrol med adgange.

På forskningsområdet er der en særlig opmærksomhed på, hvordan data deles, opbevares og styres for at forebygge, at uvedkommende kan få adgang til følsomme oplysninger. Forskningsprojekter involverer nemlig ofte udveksling af store mængder data, herunder data indeholdende følsomme personoplysninger. Forskningsprojekter gennemføres dertil ofte i et tæt samarbejde mellem forskellige aktører – heriblandt kliniske afdelinger på sygehusene, eksterne forskningsinstitutter og evt. andre nationale eller internationale samarbejdspartnere. Der skal derfor fortsat være fokus på en sikker håndtering og udveksling af data i regi af de forskningsprojekter, som Region Syddanmark er deltagende i.

Leverandørstyring

Leverandørstyring handler om beskyttelse af regionens data og systemer, når disse håndteres af eksterne leverandører. Med det følger en stor opgave i forhold til at stille de nødvendige lov- og sikkerhedskrav ved kontraktindgåelse. Øget anvendelse af digitale løsninger medfører nemlig øget forbundethed og afhængighed af eksterne leverandører. Regionen har derfor fokus på digital suverænitet og muligheden for at være i kontrol med systemer og data. Også når data eksempelvis opbevares ved hjælp af cloud-løsninger.

Region Syddanmark har derfor gennem mange år haft fokus på de kontrakter og databehandleraftaler, der indgås med leverandører med henblik på at monitorere, at eksterne samarbejdspartnere overholder et tilfredsstillende sikkerhedsniveau. For at kunne opretholde et højt sikkerhedsniveau er der behov for løbende at føre tilsyn med og tilpasse de indgåede aftaler i tilfælde af, at krav eller trusselsbilleder ændrer sig. Der kan eksempelvis overfor eksterne leverandører være behov for at stille skærpede krav såsom kryptering af data eller begrænset brugeradgang til bestemte data og systemer.

I strategiperioden fortsættes arbejdet med en systematisk gennemgang og vurdering af leverandører med henblik på at opretholde et højt og ensartet sikkerhedsniveau. Denne indsats skal forankres i et fælles leverandørstyringskoncept, og denne indsats skal endvidere understøttes af brugervenlig information til ledere og medarbejdere, der til dagligt arbejder med kontrakter og aftaler, således disse har gode vilkår for at overholde politikker og lovgivning på området.

Den menneskelige faktor (awareness)

Uhensigtsmæssig menneskelig adfærd som f.eks. fejl og utilsigtede handlinger udgør statistisk set en af de største sårbarheder i forhold til cyber- og informationssikkerhed. Det kan dreje sig om, at en medarbejder fejlagtigt sender følsomme personoplysninger til en forkert modtager. Eller at en medarbejder utilsigtet klikker på et link i en phishing mail. I en travl hverdag kan uhensigtsmæssig adfærd hyppigere forekomme, hvis det er vanskeligt og kompliceret at gøre det rigtige. Dette understreger behovet for at skabe en god sikkerhedskultur i regionen, som kendetegnes ved en vedvarende opmærksomhed på de sikkerhedstrusler, som regionen står overfor. Udgangspunktet for en god sikkerhedskultur er også, at personalet forstår, hvorfor det er vigtigt, at alle gør en indsats for at forebygge sårbarheder og sikkerhedshændelser. Indsatsen skal understøtte personalets almene forståelse for sikkerhedsarbejdet, og dermed bidrage til en forbedret sikkerhedsadfærd på tværs af alle afdelinger og medarbejdergrupper i Region Syddanmark.

Målsætningen er at informere og motivere alle medarbejdergrupper i Region Syddanmark til at udøve en passende sikkerhedsadfærd gennem øget oplysningsarbejde og målrettede uddannelsestilbud. Det skal tilstræbes at gøre det nemmere for den enkelte medarbejder at anvende sikre værktøjer og metoder, der forebygger risikoen for fejl og sikkerhedshændelser. Denne indsats skal eksekveres som en del af regionens eksisterende koncept for 'human risk management'. De enkelte tiltag skal løbende registreres og evalueres, således at indsatsen bliver datadrevet.

OPDAGE

Region Syddanmarks it-landskab er stort og komplekst. Det skal hver dag håndtere en omfattende udveksling af data mellem it-systemer og applikationer, der understøtter løsningen af regionens daglige kerneopgaver. For at kunne reagere hurtigt og effektivt ved mistanke om sikkerhedsbrud, er det afgørende, at der sker en proaktiv og konstant overvågning af aktiviteter, systemer og netværk.

Sikkerhedsovervågning

Region Syddanmark har gennem mange år gjort brug af automatiseret overvågning af netværkstrafikken, analyse af datastrømme og 24/7 rapportering på mistænkelige aktiviteter. Formålet er at opdage mønstre, der indikerer unormal trafik, der potentielt kan relatere sig til it-kriminelles forsøg på angreb.

Set i lyset af, at it-kriminelle hele tiden tager nye metoder i brug, skal regionen tilsvarende have fokus på løbende at optimere og modne den etablerede overvågnings- og analysekapacitet. Herunder gennem brug af løsninger baseret på kunstig intelligens, som kan overvåge med endnu højere hastighed og understøtte en hurtigere reaktionstid.

Forbedret overvågning og analyse af sikkerhedsrisici
Region Syddanmark vil fortsat anvende tekniske løsninger til analyser af risikobilleder, monitorering af netværkstrafik samt analyser af systemlogdata, der understøtter en proaktiv og datadreven overvågning for at opdage eventuelle sårbarheder, anomalier og mistænkelig adfærd. Forbedringen skal ske dels gennem øget overvågning, men også gennem optimeret teknologiunderstøttelse af selve overvågningen og de følgende analyser af data baseret på kunstig intelligens.

Samtidig skal der arbejdes med en struktureret indsats for opbygning af relevante kompetencer (Cyber Threat Intelligence), der kan styrke regionens forståelse af trusselsaktører og deres metoder og sikre rettidig tilpasning af sikkerhedstiltag. Gennem målrettet træning (Cyber Incident Response) opbygges operationelle kompetencer, der forbedrer reaktionstid og kvalitet i hændelseshåndtering.

Derudover skal der være fokus på løbende forbedring af regionens Security Operation Center (SOC) som helhed. Der skal fortsat arbejdes med faste procedurer for test, validering og tuning af sikkerhedsværktøjer for at sikre høj funktionalitet og kvalitet i detektionsmekanismerne og overvågningsprocedurer. Dermed sikres grundlag for at forbedre overvågningen af de mest kritiske dele af regionens it-infrastruktur.

Sårbarhedsstyring

Når der bliver opdaget en sårbarhed - for eksempel i et it-system eller en manuel arbejdsgang - gælder det om hurtigst muligt at danne sig et samlet overblik over, hvor udbredt den fundne sårbarhed er i organisationen, og hvordan man hurtigst muligt kan afhjælpe problemet. Det kræver ofte ekstra ressourcer til at undersøge problemets omfang og til at gennemføre de tiltag, der skal til for at imødegå sårbarheden. Gennem et tæt tværgående samarbejde har Region Syddanmark fokus på at udveksle viden og erfaringer mellem sygehusene for at understøtte, at der sættes ind overfor eventuelle sårbarheder på alle enheder.

Sårbarheder i applikationer, platforme og infrastruktur kan optræde i mange forskellige sammenhænge og mange forskellige steder i organisationen. Med et stort og komplekst it-landskab i regionen er håndteringen af sårbarheder ofte på bagkant, og en sårbarhed et sted påvirker potentielt hele regionen. Der er derfor behov for at styrke en sårbarhedsstyringen, således at indsatserne prioriteres og styres bredt for hele regionen. Der er behov for at styrke processerne til rettidig og korrekt identifikation, analyse og håndtering af væsentlige sårbarheder på regionens systemer og platforme for derved at robustgøre angrebsfladen og minimere risiko for sikkerhedsbrud forårsaget af cyberangreb.

I denne sammenhæng er det væsentligt, at risici afvejes, når prioriteringen af indsatserne igangsættes. Der vil i arbejdet være særligt fokus på eksempelvis sårbarheder skabt af medicoteknisk udstyr og platforme på forskningsområdet.

Håndtere

Når en sikkerhedshændelse opdages, er tiden en afgørende faktor i at afgrænse og begrænse skaden. Først og fremmest skal skaden hurtigt og effektivt forhindres i at sprede sig til flere systemer og enheder. Dernæst gælder det om hurtigt og effektivt at genoprette vitale systemers funktion og genskabe eventuelt mistet data.

Det er vigtigt, at regionen konstant styrker sin indsigt i og evne til at identificere og håndtere trusler. Denne indsats skal fortsat baseres på et tæt samarbejde med relevante samarbejdspartnere, der specialiserer sig i identifikation og vurdering af trusler, herunder Center for Cybersikkerhed, DCIS Sund, EU-Kommissionen, forskningsinstitutter m.fl. Udveksling af viden kan således understøtte regionens evne til at håndtere nye trusler og risici, der kræver målrettet beskyttelse og overvågning. Det handler om at beskytte borgere og patienter imod, at eventuelle sikkerhedshændelser indebærer risici i forhold til deres data og behandlingsmuligheder.

For at opretholde og styrke et højt sikkerhedsniveau er der behov for løbende at optimere den måde, som it-beredskabet i regionen er organiseret på. Regionen skal være i stand til effektivt at aktivere sit it-beredskab med henblik på at håndtere en kritisk situation med det formål at inddæmme og minimere skadevirkningen, samt effektivt og kontrolleret at komme tilbage til en normaliseret situation.

IT-beredskabsmodel

I 2024 er der gennemført en større omorganisering af it- og digitaliseringsområdet i Region Syddanmark. Dertil ser regionerne ind i række nye forandringer de næste år, som knytter sig til implementeringen af regeringens sundhedsreform. Det er derfor relevant i løbet af strategiperioden at genbesøge beredskabet i regionen for at styrke en aktuel og sammenhængende organisering af beredskabet. Denne indsats skal baseres på et tæt samarbejde med regionens arbejde med hændelsesstyring, Security Operation Center (SOC), de decentrale it-funktioner samt relevante tværregionale, nationale og internationale myndigheder og andre aktører for hurtigt at kunne dele varsler og viden om aktuelle trusler og hændelser.

Modellen skal have fokus på risikoejerskab, korte beslutningsveje, mulighed for hurtig eskalering og effektiv reaktionstid. Der skal endvidere sikres en fælles forståelse af de anvendte koncepter (nød-, beredskabs- og reetableringsplaner) og trænes i anvendelse af beredskabsmodellen. Modellen skal fortsat forankres bredt og integrere med regionens øvrige organisatoriske beredskabsniveauer, herunder sundhedsberedskabet. Modellen skal også relateres til beredskabsplaner i forhold til forsyningssikkerhed og fysisk sikkerhed.

Beredskabsplanlægning og -test

Beredskabsplaner er et praktisk og effektivt redskab, som ledelse og medarbejdere kan bruge, når ekstraordinære kriser og hændelser skal håndteres. Beredskabsplanlægningen skal løbende optimeres for at styrke regionens evne og kapacitet til at kunne håndtere kritiske hændelser og krisesituationer. Det handler som sagt om hurtigst muligt at genskabe en stabil og sikker drift for at kunne videreføre regionens kritiske kerneopgaver – herunder særligt de mest kritiske sundhedsydelser til borgere og patienter.

Løbende opdatering af beredskabsplaner

For at styrke regionens evne til at håndtere eventuelle beredskabssituationer er det nødvendigt løbende at have fokus på at opdatere og vedligeholde beredskabsplaner. Her er det væsentligt at forholde sig til et bredt spektrum af trusler, der potentielt kan indebære en risiko for regionens virke. Herunder også scenarier som kræver utraditionelle metoder – eksempelvis opbevaring af fysiske beredskabsplaner i tilfælde af manglende adgang til internettet, m.v. for de mest kritiske systemer. Det skal ligeledes sikres, at alle aktører har opdaterede og effektive beredskabsplaner. Det gælder også relevante eksterne samarbejdspartnere. For særligt kritiske leverandører skal der udarbejdes beredskabsplaner, der beskriver, hvordan sikkerhedshændelser skal håndteres og rapporteres. Formålet er at sikre, at de pågældende leverandører er forberedt på at reagere hurtig og effektivt i tilfælde af en sikkerhedshændelse, hvor regionen henvender sig.

Beredskabstest

Test af beredskabsplaner er afgørende, og giver først og fremmest træning i at håndtere beredskabs- og sikkerhedsmæssige situationer. Test leverer også vigtig viden til det fortsatte arbejde med at optimere beredskabsplanerne. I CIS 18- rammeværket er test og afprøvning af sikkerheden integrerede elementer, som der fortsat skal være fokus på for at leve op til det beredskabsmæssige ansvar. Det gælder særligt afprøvning af beredskabsplaner for kritiske systemer samt afprøvning af genetablering (restore) af kritiske systemer.

Træning i håndtering af sikkerhedshændelser

For at sikre, at de forbedrede procedurer for overvågning og håndtering af sikkerhedshændelser udnyttes optimalt, skal der gennemføres træningsprogrammer for de medarbejdere, der er ansvarlige for sikkerhedsovervågning, beredskab og genetablering af en stabil og sikker drift. Træningen skal understøtte, at medarbejderne kontinuerligt har opdateret viden og færdigheder til at opdage og håndtere sikkerhedshændelser som eksempelvis i forbindelse med et cyberangreb.

Den økonomiske ramme

Regionsrådet har som en del af Region Syddanmarks Digitaliseringsstrategi afsat 29,1 mio. kr. ekstra investeringer i cyber- og informationssikkerhedsområdet. Hertil kommer 10,9 mio. kr., der er afsat af regeringen i forbindelse med økonomiaftalen for 2025. Dermed beløber den forventede investering i årene 2025-2028, som delstrategien dækker, sig til i alt 4040 mio. kr. Hvis der i sammenhæng med kommende økonomiaftaler prioriteres yderligere midler til sikkerhedsområdet, skal de samlede økonomiske rammer til området revurderes.

Initiativerne i strategien ventes at kunne gennemføres inden for den samlede afsatte investeringsramme, og fordeler sig således under de fire spor:

Område	**Økonomisk ramme (mio. kr.)**
Forudse	8,0
Forebygge	14,0
Opdage	12,0
Håndtere	6,0
I alt	**40,0**

Erfaringerne fra tidligere udmøntninger af midler til styrkelse af cyber- og informationssikkerhed viser, at udgifter almindeligvis har karakter af driftsudgifter, og kun i mindre udstrækning omfatter anskaffelser mv. af anlægsmæssig karakter. Det anbefales derfor, at den afsatte anlægsramme konverteres til en driftsbevilling via konsolideringsrammerne for drift og anlæg.