SUNDHEDSDATA-
STYRELSEN

2025
DCIS SUND

Tilslutnings- og samarbejdsgrundlag for Cyberalarmen

Indhold

1. Overordnede rammer 3

1.1 Visionære højder 3
1.2 Opdrag 3
1.3 Installation af Cyberalarmen i Praksis 4
1.4 Evaluering 4
1.5 Generelt om tilslutningen og samarbejdet 4
2 Lovhjemmel 12

1. Overordnede rammer

1.1 Visionære højder

Visionen med Cyberalarmen består i at styrke den langsigtede ambition om at øge sundhedsvæsenets kapacitet og evne til at opdage uvedkommende aktivitet og cyberhændelser i sektoren i videst muligt omfang. Dette gøres via et pilotprojekt, hvis formål består i at øge cyber- og informationssikkerheden hos praksis-delen af sundhedssektoren med faktisk teknisk værktøj. Vi har gjort det simpelt med en løsning i en boks – Cyberalarmen.

Cyberalarmen er sammensat som en *Network Detection and Response Unit (NDR-enhed)* og en tablet. Enheden, der udgør hoveddelen af Cyberalarmen, kobles og monteres til jeres netværk for at opdage hændelser uden for normalen i netværkstrafikken. Den anden del består af en tablet, hvor I kan følge med i tilstanden af jeres netværk. Vi sørger for at I modtager notifikationer hvis der sker væsentlige ændringer i jeres netværksmønster, såsom angreb på netværket eller sårbarheder på udstyr.

Cyberalarmen er både i stand til at opdage anomalier ude på jeres netværk, såkaldte afvigelser fra normal adfærd på netværket (NDR-enheden). Ligeledes har Cyberalarmen tilknyttet et internt sårbarhedsscanningsværktøj til at scanne jeres netværk. Dette værktøj beriges af viden fra hele sundhedssektoren, som sikrer aktiv detektering af sårbarheder, og sørger for at Cyberalarmen informerer og oplyser om kendte sårbarheder. Dette fremhæves med tabletten, som viser genkendelige glade og sure smileyer som indikator på, om alt er vel. Fx kan den komme med meddelelser om øget aktivitet fra en bestemt netværksadresse og opfordre jer til at kontakte jeres it-leverandør. Den kan også fortælle om jeres IT-systemer er opdateret med seneste software og sikkerhedspatches.

1.2 Opdrag

Konceptet der her udrulles til jer i pilotprojektet, har sin oprindelse i initiativ 3.2 i sundhedssektorens cyber- og informationssikkerhedsstrategi, der omhandler *sundhedssektorens overvågnings- og analyseplatform* (SAC). Med den overenskomst, som blev indgået mellem Praktiserende Lægers Organisation og Danske Regioner, kunne man således udvide dækningsgraden til hele sektoren. Det er den *Decentrale Cyber- og Informationssikkerheds Enhed for sundhedssektoren* (DCIS Sund) ved Sundhedsdatastyrelsen, der er tovholder på initiativet i samarbejde med sektoren.

Piloten og den økonomiske dækning

Sundhedsdatastyrelsen og DCIS Sund, har i samarbejde med Praktiserende Lægers Organisation og Danske Regioner indgået en samarbejdsaftale der dækker de økonomiske omkostninger for, at I kan modtage Cyberalarmen og hertil hørende services på enheden. Man kan vælge at komme på Cyberalarmen med selve enheden (boksen), samt tabletten med information om klinikkens it-tilstand. Det er også muligt at nøjes med selve boksen, som bidrager til information om sikkerheden i sektoren.

1.3 Installation af Cyberalarmen i Praksis

- Enheden tilknyttes DCIS Sund via et 4G/5G-modem (med eget SIM-kort), både for at identificere hændelser eller angreb, som går på tværs af sundhedssektoren og for at modtage information fra DCIS Sund om generelle tendenser, som kræver særlig opmærksomhed (fx "falske MitID-mails i omløb"). Regionerne og nogle kommuner er også koblet på denne løsning, som vil bidrage til at styrke sundhedssektorens samlede cybersikkerhedsniveau.
- DCIS Sund installerer Cyberalarmen. Her forventes fysisk adgang til netværksmodemet og at netværket må slukkes i 5-10 minutter imens den installeres. I kan godt tilgå jeres systemer imens. Alarmen fungerer uafhængigt af jeres systemer og vil ikke påvirke netværk, netværks- eller systemleverandøren. Cyberalarmen er kun virksom i det omfang I vælger at gøre brug af den. Den fungerer som en støtte, på samme måde som en teknisk rådgiver ville gøre, men det er op til jer at handle på det.

1.4 Evaluering

a) Evaluering motiveres én gang under og én gang efter piloten.
b) Evaluering tager afsæt i interface, brugervenlighed, og værdi for praksis etc.
c) Naturligvis, er man altid velkommen til at kontakte DCIS Sund vedr. Cyberalarmen for kontinuerlig forbedring.

1.5 Generelt om tilslutningen og samarbejdet

a) Praksis indgår i pilotprojektet ved skriftlig tilkendegivelse om, at en praksis ønsker at modtage Cyberalarmen.
b) Installationstidspunkt og opsætning aftales med DCIS Sund.
c) Nævnte opsætning påbegyndes ud fra præmisserne jf. punkt *1.3 Installation af Cyberalarmen i Praksis*.
d) DCIS Sund kan kontaktes i hverdage på DCISSund@sundhedsdata.dk.
e) Hvis praksis eller DCIS Sund i SDS ønsker at opsige tilslutning- og samarbejdet omhandlende Cyberalarmen, skal det ske skriftligt med rettidigt varsel.
f) Der skal ikke indgås nogle databehandleraftaler mellem parterne, da praksis ikke selv behandler egen data. Det juridiske grundlag for at Sundhedsdatastyrelsen foretager indsamling af data og overvågning ifm. Cyberalarmen, tager afsæt i Sundhedsloven § 220 a (se bilag).

Bilag til
Grundlaget for Cyberalarmen

2 Lovhjemmel

Det juridiske grundlag for indsamling af data med Sundhedsdatastyrelsen ifm. Cyberalarmen tager afsæt i Sundhedsloven § 220 a.

Jf. nedenstående

DANSKE LOVE

Forside › *Sundhedsloven* › § 220 a

Sundhedsloven § 220 a

§ 220 a Sundhedsdatastyrelsen er en styrelse under indenrigs- og sundhedsministeren, som udfører opgaver for henholdsvis indenrigs- og sundhedsministeren og ældreministeren vedrørende den centrale forvaltning af forhold angående digitalisering og data på sundhedsområdet og på ældreområdet. Sundhedsdatastyrelsen har til opgave at skabe sammenhængende data og digitale løsninger til gavn for borgere, patienter og sundhedspersoner samt til styringsmæssige, statistiske og videnskabelige formål i sundheds- og ældresektorerne.

Stk. 2. Sundhedsdatastyrelsen indsamler og stiller sundhedsdata og analyser om aktivitet, økonomi og kvalitet til rådighed for sundhedsvæsenet, herunder sundhedspersoner, administratorer i regioner og kommuner og patienter, borgere og andre centrale brugere. Sundhedsdatastyrelsen styrker endvidere den overordnede digitalisering og fremmer en sammenhængende data- og it-arkitektur i sundhedsvæsenet med fokus på internationale standarder tilpasset nationale behov og informationssikkerhed i henhold til gældende lovgivning. På udvalgte områder sikrer Sundhedsdatastyrelsen dækkende og valide sundhedsdata til patientbehandling m.v.

Stk. 3. Sundhedsdatastyrelsen koordinerer arbejdet med sundhedsdata og -it på tværs af sundhedsvæsenet og sætter fælles mål i form af strategier, aftaler og it-arkitektur. Sundhedsdatastyrelsen varetager endvidere overvågnings- og analysefunktioner i forbindelse med at sikre sammenhængende data og fremme informationssikkerheden i sundhedssektoren.

Specifik vurdering fra Sundhedsdatastyrelsens jurister:

"Af sundhedslovens § 220a, stk. 3, 2. pkt. fremgår det, at Sundhedsdatastyrelsen varetager overvågnings- og analysefunktioner i forbindelse med at sikre sammenhængende data og fremme informationssikkerheden i sundhedssektoren. Denne bestemmelse giver dermed styrelsens SAC-funktion ret til, at overvåge- og analysere sundhedssektoren i sin helhed, som også indbefatter Kommunerne. Kommunerne dækker dog mere end sundhedssektoren, hvorfor netværket for dem, godt kan indeholde andet datasæt end kun sundhedssektoren. Det vil være at foretrække, såfremt kommunerne kan opdele deres netværk, således at

Sundhedsdatastyrelsen kun overvåger sundhedssektoren. Såfremt netværksopdeling ikke er realistisk, er styrelsen dog af den opfattelse, at styrelsen fortsat gerne må overvåge hele netværket, for at kunne sikre generelle informationssikkerhed ift. fortrolighed, integritet og tilgængelighed i sundhedssektoren, som kommunerne er en stor del af."