



Risiko-og trusselsvurderinger i sundhedssektoren

Tanja Kaufmann
Sektionsleder DCIS Sund, Sundhedsdatastyrelsen



**SUNDHEDSDATA-
STYRELSEN**

Årets tema: Er tiden inde til at tale om en nødvendig digital omstilling af sundhedssektoren?



Risikovurderinger – But why?



Er det ikke bare de der folk fra sikkerhed, der er hysteriske?

Vejledning om kriterier og krav til operatører af væsentlige tjenester i sundhedssektoren

Behandlings

Forordningen kr
behandlings kar

Det er ikke dest
risikobaserede t

fysiske personer

forordningen

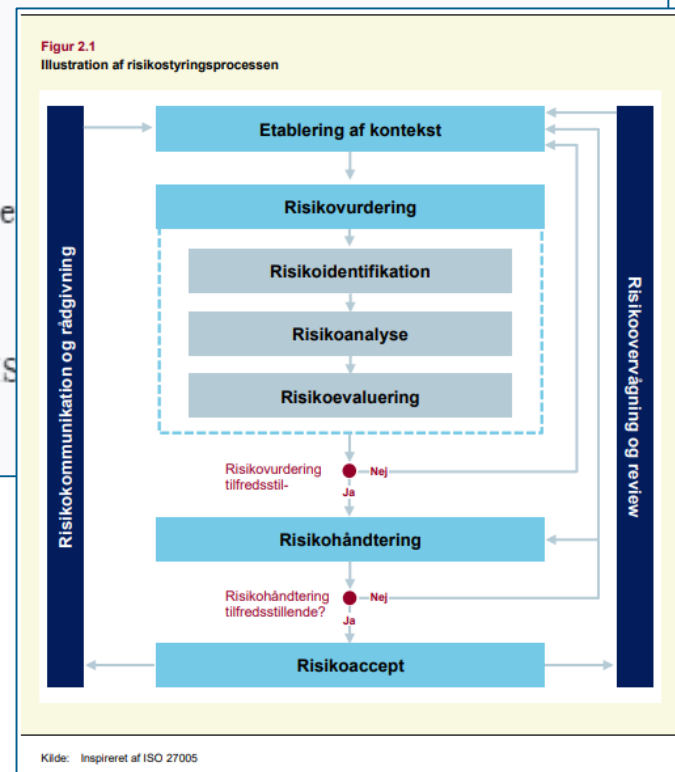
Indledning

Bekendtgørelse af krav til operatører af væsentlige tjenester i sundhedssektoren

2. Sikkerhedsforanst

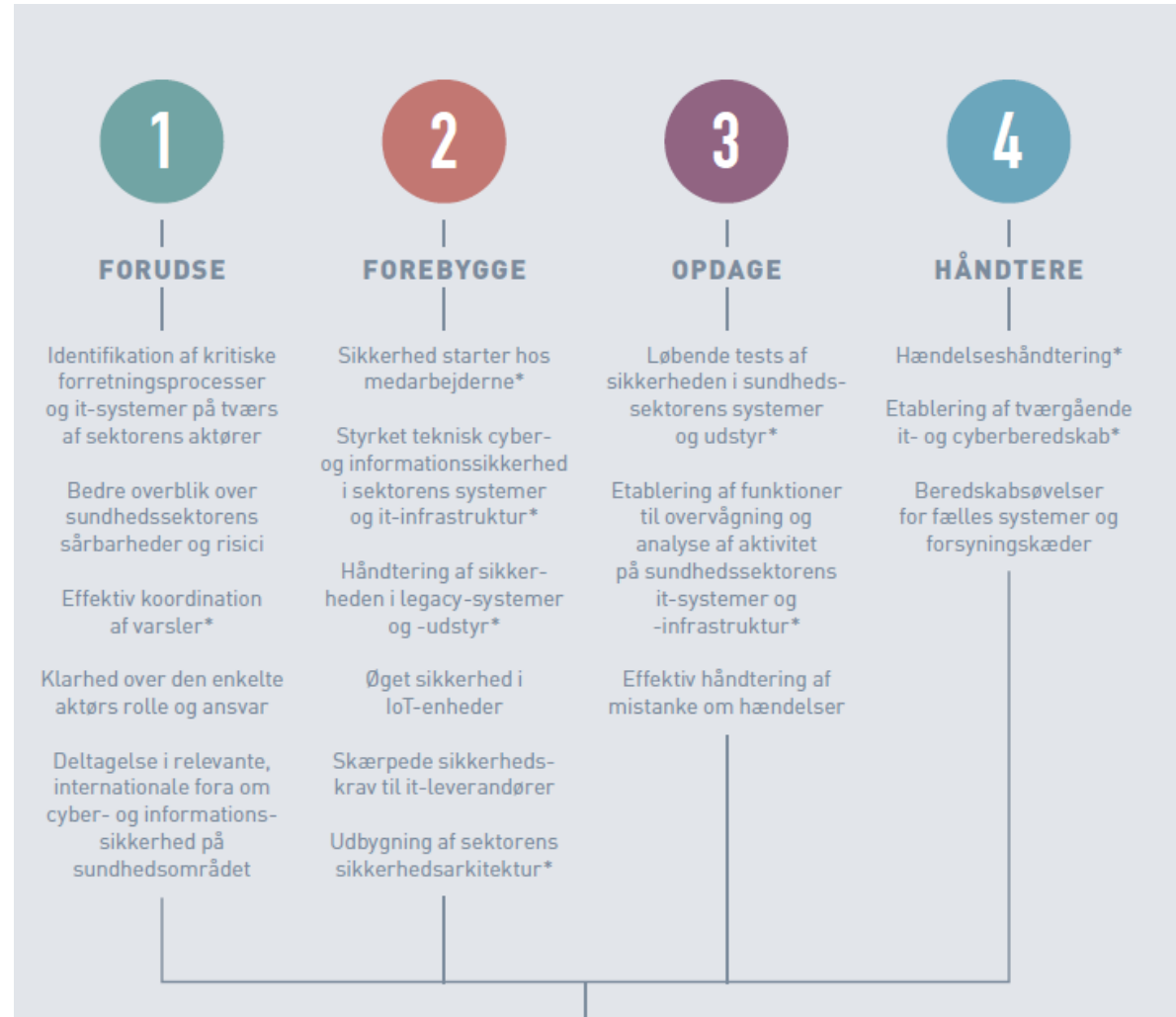
Operatører af væs
robusthed, tilgængel
væsentlige tjeneste.

Dette sker på bagg
forstyrrende virkni
risikovurderingen s
væsentlige tjeneste.



ici for

Et fælles fokus på tværs af sundhedssektoren



(For) Høje ambitioner (?)

INITIATIV 1.2.

Bedre overblik over sundhedssektorens sårbarheder og risici

Det er nødvendigt løbende at vedligeholde lokale og tværgående vurderinger af sårbarheder og risici. Det er de enkelte aktørers ansvar at udarbejde og opdatere egne sårbarheds – og risikovurderinger samt sikre ledelsesforankring. DCIS udarbejder i 2019 i samarbejde med sektorens aktører vejledninger til at understøtte arbejdet, således at vurderingerne over tid bliver metodisk ensartede. Vejledningerne vil desuden være obligatoriske at følge for sårbarheds – og risikovurderinger af fælles, prioriterede, kritiske systemer. DCIS har desuden til opgave at udarbejde den samlede sårbarheds- og risikovurdering for hele sektoren.

Vi tror stadig på opgaven



Indhold

For at skabe mest mulig værdi på tværs af sektoren og for de lokale aktører skal der i initiativet arbejdes med at forbedre metoden for indmeldelse af de lokale risikovurderinger til brug i udarbejdelsen af sektorens samlede risikovurdering. Fokus for metoden vil være samarbejde og vidensdeling mellem sektorens aktører for at berige et fælles overblik på tværs.

De enkelte aktører udarbejder og opdaterer egne risikovurderinger. Sundhedssektorens trusselsbillede, der publiceres årligt af DCIS, kan anvendes i dette arbejde. Trusselsbilledet giver et grundlæggende overblik over aktuelle trusler og et indblik i trusselstendenser mod sundhedssektoren. Aktørenes sårbarheds- og risikovurderinger af den it-infrastruktur, der igennem initiativ 1.1 'Identifikation af sundhedssektorens samfundsvigtige funktioner og kritisk it-infrastruktur' identificeres som kritisk, skal som minimum være en del af aktørens samlede risikovurdering og dermed indgå i det samlede billede for sektoren.

Det er et komplekst domæne!



Metoden... Det ser enkelt ud, men lad dig ikke narre!


$$R = S \times K$$

$R = S$ (Sårbarheder og trusler) x K
(konsekvensvurdering- ikke at forveksle
med en DPIA)

Konsekvenser for
forretningen?


Konsekvenser for
den registrerede?

For samfundet
(NIS)

Spis elefanten i små bidder

INITIATIV 1.2.

Bedre overblik over sundhedssektorens sårbarheder og risici

Det er nødvendigt løbende at vedligeholde lokale og tværgående vurderinger af sårbarheder og risici. Det er de enkelte aktørers ansvar at udarbejde og opdatere egne sårbarheds – og risikovurderinger samt sikre ledelsesforankring. DCIS udarbejder i 2019 i samarbejde med sektorens aktører vejledninger til at understøtte arbejdet, således at . Vejledningerne vil desuden være obligatoriske at følge for sårbarheds – og risikovurderinger af fælles, prioriterede, kritiske systemer. DCIS har desuden til opgave at udarbejde den samlede sårbarheds- og risikovurdering for hele sektoren.

Trusselsbilledet i sundhedssektoren – Hvordan hjælper det dig?

TLP-CLEAR

SUNDHEDSDATA-STYRELSEN

Top 5 cybertrusler i 2023

Ransomware
Ransomware udgør en **MEGET HØJ** trussel mod sundhedssektoren. Det vurderes, at der er en **MEGET HØJ** hyppighed af ransomware-angreb og at cyberkriminelle, gennem en række angrebsvektorer, vil forsøge at ramme sundhedssektoren. Angreb mod store som små aktører vil have **KATASTROFALE** konsekvenser, hvis it-systemer gøres utilgængelige og brud på fortroligheden.

Phishing
Phishing udgør en **MEGET HØJ** trussel mod sundhedssektoren. Det vurderes, at der er **MEGET HØJ** hyppighed af phishing-angreb, da det er et af de mest benyttede værktøjer til at opnå adgang til organisationer, og særligt sundhedssektoren er et mål for cyberkriminelle. Phishing-angreb mod sundhedssektoren vil have **ALVORLIGE** konsekvenser, da systemer kan gøres utilgængelige og personfølsomme patientoplysninger kan blive lækket og solgt på The Dark Web.

Supply-chain
Supply-chain udgør en **MEGET HØJ** trussel mod sundhedssektoren. Det vurderes, at der er en **MEGET HØJ** hyppighed af supply-chain-angreb, og cyberkriminelle vil forsøge at udnytte sektorens mange leverandører af it-systemer og infrastruktur i angreb mod sektoren. Et angreb mod forsyningskæden vurderes at kunne have **ALVORLIGE** konsekvenser, hvis it-understøttelsen af sundhedsydelserne kompromitteres.

Cyberaktivisme
Cyberaktivisme udgør en **MEGET HØJ** trussel mod sundhedssektoren. Det vurderes, at der **MEGET HØJ** hyppighed af bl.a. DDoS-angreb. Trods den meget høje hyppighed har cyberaktivisme **MODERATE** konsekvenser for sundhedssektoren, da driften kan fortsættes, men forstyrrelserne skaber utryghed og kan tage fokus fra andre igangværende angreb. Normalt ville **MEGET HØJ** hyppighed og **MODERATE** konsekvenser vurderes som **HØJ** trussel, men der er en erkendt trussel for cyberaktivisme, og cyberkriminelle har både kapacitet, hensigt, planlægning og mulighed for iværksættelse af angreb, der potentielt kan skade tilliden til sundhedssektoren.

Malware
Malware udgør en **MEGET HØJ** trussel mod sundhedssektoren. Det vurderes, at der er **MEGET HØJ** hyppighed af brugen af malware, og de cyberkriminelle bliver bedre og bedre til at inficere systemer. Inficering af systemer med malware i sundhedssektoren vil have **ALVORLIGE** konsekvenser for patientbehandlingen, og systemer kan gøres utilgængelige.

TLP-CLEAR 6 / 52



TLP-CLEAR

Sundhedssektoren

Trusselsbillede 2023

CISSund - Sundhedssektorens decentrale cybersikkerhedscenter

Ransomware

Ransomware kan udgøre en alvorlig trussel mod sundhedssektoren, hvis den får adgang til patientoplysninger og andre vigtige data. Ransomware-angreb kan gøres utilgængelige og brud på fortroligheden.

Første skridt i et angreb er at få adgang til systemer, der har værdi for organisationen, og derfor skal der sættes fokus på at sikre systemer og data mod angreb. Dette kan gøres ved at opdatere systemer og software, anvende sikkerhedsopsætning og sikre, at systemer er beskyttet mod malware.

Heretter påbegynder angribere deres angreb ved at udføre følgende handlinger og scripts:

- Lock – låse adgang til systemer
- Encrypt – kryptere data
- Delete – slette data
- Steal – stjæle data

De konkrete metoder til at angribe systemer er beskrevet senere i rapporten.

Når aktivitet er bemærket, er det vigtigt at isolere den ramte organisation og informere myndighederne om angrebet.

- Offentliggørelse af angrebet
- Delvis eller fuld offentliggørelse af angrebet
- DDoS-angreb

Trusler pga. invasi af 2022

Ransomware-angreb mod sundhedssektoren udsættes data og i værste selvom angriber stadig har adgang til data.

Angrebsvektorer

De cyberkriminelle i sundhedssektoren anvender en række metoder og opmærksom på følgende:

- Phishing (se Phishing)
- Supply-chain (se Supply-chain)
- Fjernadgang (se Fjernadgang)
- Drive-by
- Udnyttelse af sårbarheder

Nogle teknikker giver cyberkriminelle adgang til systemer, som herefter kan bruges til at indlede et angreb.

Fjernadgang
Cyberkriminelle udnytter fjernadgangssystemer (RDP). De udnytter oftest følgende metoder:

- Cyberkriminelle udnytter fjernadgangssystemer (RDP).
- Cyberkriminelle udnytter oplysninger på offentlige netværk.
- Cyberkriminelle udnytter sårbarheder i systemer.

Drive-by
Et drive-by-angreb består af en forbindelse med almindelige brugere, der installerer malware i stedet for at angribe organisationen.

Udnyttelse af sårbarheder
Udnyttelse af sårbarheder i systemer og software kan give cyberkriminelle adgang til systemer og data. Angriberen udnytter sårbarheder til at installere ransomware og andre skadelige programvarer på systemer.

Ransomware

Ransomware-angreb er en alvorlig trussel mod sundhedssektoren, da det kan resultere i tab af patientoplysninger og andre vigtige data. Ransomware-angreb kan gøres utilgængelige og brud på fortroligheden.

Den eneste måde at undgå et ransomware-angreb er at sikre, at systemer er beskyttet mod malware. Dette kan gøres ved at opdatere systemer og software, anvende sikkerhedsopsætning og sikre, at systemer er beskyttet mod malware.

På trods af stigende opmærksomhed og støtte fra myndighederne fortsat vil der være mange mennesker, der bliver ramt af ransomware-angreb.

Cyberkriminelle
De cyberkriminelle i sundhedssektoren anvender en række metoder og opmærksom på følgende:

- Phishing (se Phishing)
- Supply-chain (se Supply-chain)
- Fjernadgang (se Fjernadgang)
- Drive-by
- Udnyttelse af sårbarheder

Der er flere cybersikkerhedsgrupper, der arbejder på at hjælpe organisationer med at beskytte sig mod ransomware-angreb. Disse grupper kan hjælpe organisationer med at identificere sårbarheder i systemer og software, og de kan også hjælpe organisationer med at opdatere systemer og software.

De fleste ransomware-angreb mod sundhedssektoren er udført af cyberkriminelle, der har adgang til systemer og data. Derfor er det vigtigt at sikre, at systemer er beskyttet mod malware.

Oversigt over angreb

Angreb mod sundhedssektoren er blevet mere hyppigt i 2023. Dette skyldes blandt andet den stigende anvendelse af cloud-tjenester og den stigende mængde data, der gemmes i cloud.

Angrebene er blevet mere avancerede og målrettede. Dette skyldes blandt andet den stigende anvendelse af AI og machine learning til at analysere data og identificere sårbarheder i systemer og software.

Angrebene har haft alvorlige konsekvenser for sundhedssektoren, da det kan resultere i tab af patientoplysninger og andre vigtige data. Angrebene kan også resultere i økonomiske tab og skade på organisationens omdømme.

Angrebene er blevet mere hyppigt i 2023. Dette skyldes blandt andet den stigende anvendelse af cloud-tjenester og den stigende mængde data, der gemmes i cloud.

Angrebene er blevet mere avancerede og målrettede. Dette skyldes blandt andet den stigende anvendelse af AI og machine learning til at analysere data og identificere sårbarheder i systemer og software.

Angrebene har haft alvorlige konsekvenser for sundhedssektoren, da det kan resultere i tab af patientoplysninger og andre vigtige data. Angrebene kan også resultere i økonomiske tab og skade på organisationens omdømme.

Mitigerende foranstaltninger

For at reducere risikoen for et ransomware-angreb er det vigtigt at implementere følgende foranstaltninger:

- Udarbejd en sikkerhedsplan og en beredskabsplan.
- Have en sikkerhedskop af vigtige data.
- Krypter vigtige data.
- Benyt sikkerhedsopsætning til at beskytte systemer mod malware.
- Deaktiver ikke nødvendige funktioner i systemer.
- Vedligehold systemer og software.
- Begræns adgang til systemer og data.
- Begræns brug af offentlige netværk.
- Segmenter netværket.
- Overvåg systemer og data.
- Vidensdeling om angreb og sårbarheder.
- Uddan og træning af medarbejdere.
- Betal ikke ransomsomme.

Conti cyberangreb
Det nationale sundhedsdataregister er blevet ramt af et cyberangreb. Angrebet resulterede i, at data blev låst og organisationen blev tvunget til at betale en ransomsomme for at få adgang til data.

Hospital Hørsholm
I januar 2018 blev Hospital Hørsholm ramt af et cyberangreb. Angrebet resulterede i, at data blev låst og organisationen blev tvunget til at betale en ransomsomme for at få adgang til data.

Wannacry, 2017
Wannacry er et ransomware-angreb, der blev udført i 2017. Angrebet resulterede i, at millioner af mennesker blev ramt og tvunget til at betale en ransomsomme for at få adgang til deres data.

<https://www.dsb.dk>

TLP-CLEAR

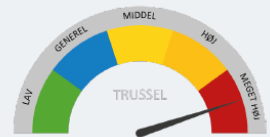
SUNDHEDSDATA-STYRELSEN

Trusselsvurdering - Ransomware

Sundhedssektoren er særligt sårbar over for ransomware, og et ransomware-angreb kan forstyrre kritiske operationer, forhindre sundhedsfaglig personale i at tilgå patientdata og patientjournaler og dermed give en forstyrrelse af patientbehandlingen og de generelle sundhedsydelser, som dagligt bruges. Et angreb kan ydermere resultere i tab og/eller tyveri af følsomme patientoplysninger, som kan bruges til identitetstyveri eller andre skadelige formål, såsom dataleak. Der er for set store angreb mod sundhedssektoren i udlandet, som har haft særligt økonomiske konsekvenser, men også konsekvenser for den enkelte borger.

Sammenholdt med den **MEGET HØJE** hyppighed af ransomware-angreb og den **KATASTROFALE** konsekvens, det ville have, vurderes det, at ransomware-angreb udgør en **MEGET HØJ** trussel mod sundhedssektoren. Der er en specifik trussel for ransomware-angreb og cyberkriminelle har både kapacitet, hensigt, planlægning og mulig iværksættelse.

TRUSSELSVURDERING



TRUSSEL

LAV GENEJEL MIDDLE HØJ MEGET HØJ

19 / 52

TLP-CLEAR

Vi starter med en sammenlignelig mapning

– *taxonomy of operational cyber security risk v.2*

1. Action of people	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent 1.1.1 Mistakes 1.1.2 Errors 1.1.3 Omissions 1.2 Deliberate 1.2.1 Fraud 1.2.2 Sabotage 1.2.3 Theft 1.2.5 Vandalism 1.3 Inaction 1.3.1 Skills 1.3.2 Knowledge 1.3.3 Guidance 1.3.4 Availability	2.1 Hardware 2.1.1 Capacity 2.1.2 Performance 2.1.3 Maintenance 2.1.4 Obsolescence 2.2 Software 2.2.1 Compatibility 2.2.2 Configuration management 2.2.3 Change control 2.2.4 Security settings 2.2.5 Coding practices 2.2.6 Testing 2.3 Systems 2.3.1 Design 2.3.2 Specifications 2.3.3 Integration 2.3.4 Complexity	3.1 Process design or execution 3.1.1 Process flow 3.1.2 Process documentation 3.1.3 Roles and responsibilities 3.1.4 Notifications and alerts 3.1.5 Information flow 3.1.6 Escalation of issues 3.1.7 Service level agreements 3.1.8 Task hand-off 3.2 Process controls 3.2.1 Status monitoring 3.2.2 Metrics 3.2.3 Periodic review 3.2.4 Process ownership 3.3 Supporting processes 3.3.1 Staffing 3.3.2 Funding 3.3.3 Training and development 3.3.4 Procurement	4.1 Disaster 4.1.1 Weather event 4.1.2 Fire 4.1.3 Flood 4.1.4 Earthquake 4.1.5 Unrest 4.1.6 Pandemic 4.2 Legal issues 4.2.1 Regulatory compliance 4.2.2 Legislation 4.2.3 Litigation 4.3 Business issues 4.3.1 Supplier failure 4.3.2 Market conditions 4.3.3 Economic conditions 4.4 Service dependencies 4.4.1 Utilities 4.4.2 Emergency services 4.4.3 Fuel 4.4.4 Transportation
Niveau 1.	1. Action of people		
Niveau 2.	1.1 Inadvertent		
Niveau 3.	1.1.1 Mistakes		

1	A	B	C	D	E	F	G	H	I	J	K	L
2	År og aktør		System		Trusselskatalog og risikobeskrivelse				Risikoindeks			Uddybning
3	År*	Aktør*	Tjeneste*	Net- og informationssystem*	Niveau 1 (x)*	Niveau 2 (x.x)*	Niveau 3 (x.x.x)	Beskrivelse af risiko*	Sandynlighed*	Konsekvens*	Risikoscore*	Kommentar
3	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn					lav	høj	8	Kommentar til risikoen
4	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn					Meget høj	Mellem	15	Kommentar til risikoen
5	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn					Lav	Lav	4	Kommentar til risikoen
6	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
7	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
8	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
9	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
10	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
11	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
12	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
13	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
14	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
15	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
16	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
17	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
18	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
19	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
20	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
21	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
22	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
23	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
24	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
25	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
26	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
27	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
28	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
29	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
30	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
31	2023	Indsæt aktør	Indsæt tjeneste	Indsæt systemnavn								Kommentar til risikoen
32												

Overblikket



Med hvad så med den ensartede metode?

- ▶ Der er lavet en afgræsning i målgruppen, som betyder at,
 - Der arbejdes videre på 4. år i en arbejdsgruppe på tværs af aktører underlagt NIS (1) i sundhedssektoren
 - Vi er blevet enige om metodefrihed
 - Fokus er på at skabe fælles referencetabeller, der giver sammenligningen resultater.

- ▶ Gevinsterne er bl.a.,
 - Understøttelse af det lokale arbejde
 - Indsatser og prioriteringer kan ske på et oplyst grundlag
 - Et samlet kvalificeret risikobillede.

Kontakt

E-mail

DCISSUND@sundhedsdata.dk

Mere information

[Cyber- og informationssikkerhed i sundhedsvæsenet](#)



**SUNDHEDSDATA-
STYRELSEN**