Spor 3

Sikkerhed

Hvordan arbejder Sundhedsdata-styrelsens med Sundhedsdata og sikkerhed

Søren Bank Greenfield, Afdelingschef, Cyber- og Informationssikkerhed, og Ole Fisker, Technical Security Analyst, Sundhedsdatastyrelsen

Hvordan arbejder Sundhedsdatastyrelsens med Sundhedsdata og sikkerhed

Få svar på spørgsmål som:

- Hvordan samarbejder sundhedssektoren omkring arbejdet med cyber- og informationssikkerhed?
- Hvilke værktøjer bruger DCIS sund og sektoren til at samarbejdet?
- Hvilke samarbejdsformer har vist sig at være gode?
- Hvad er næste skridt for samarbejdet?

Hvordan arbejder Sundhedsdatastyrelsen med sundhedsdata og sikkerhed?

DEIC konference 2022
12:00-12:30

SUNDHEDSDATA-STYRELSEN

Om os

Søren Bank Greenfield, chef for Cyber- og Informationssikkerheds afdeling.

- Faglig baggrund som operationel sikkerhedschef, CISO og med viden indenfor brugervendt infrastruktur, identitetsstyring og cybersikkerhed. Har før været i KBH amt, Glostrup hospital og Regionh (CIMT).

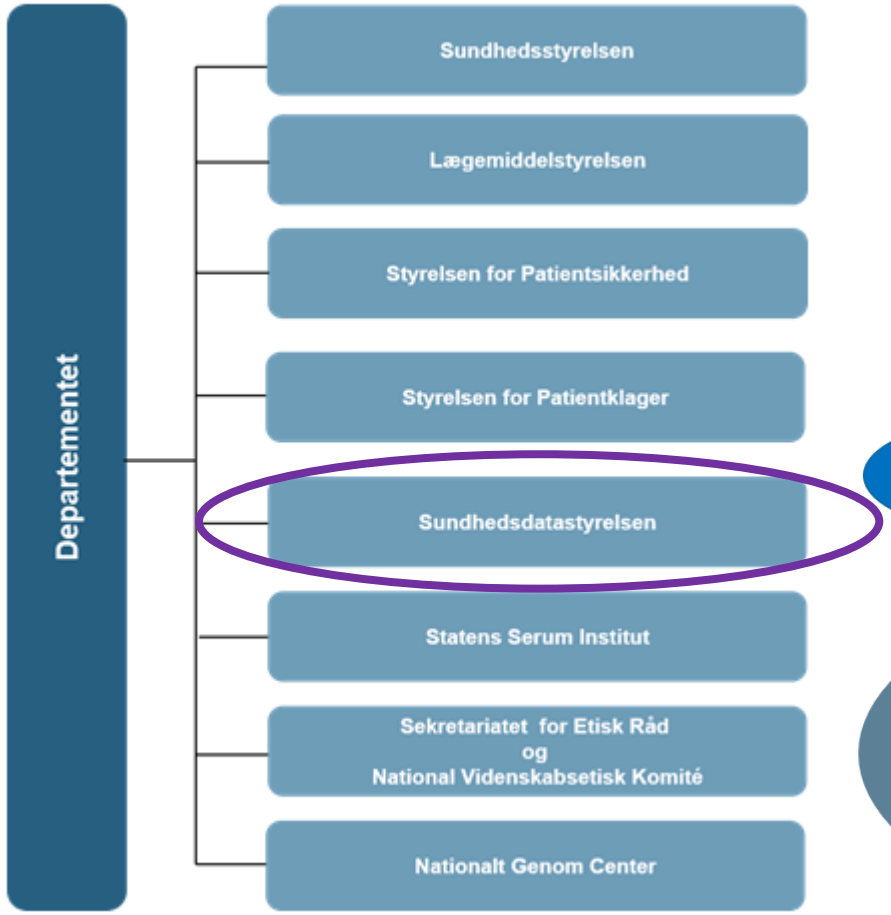
Ole Fisker, teknisk sikkerhedsanalytiker, etisk hacker og app-udvikler.

- Baggrund som sikkerhed specialist, programmør, infrastruktur arkitekt og tekniker. Har før været i politiet, DSV og Regionh (CIMT).

SUNDHEDSDATA-
STYRELSEN

Sundhedsministeriet

Afdelingen har til opgave at facilitere og koordinere den fælles indsat for at **styrke og øge** kapabiliteten og kapaciteten indenfor Cyber- og Informationssikkerhed i Sundhedsdatastyrelsen, **Sundhedsministeriet** og **på tværs af sundhedsvæsenet.**



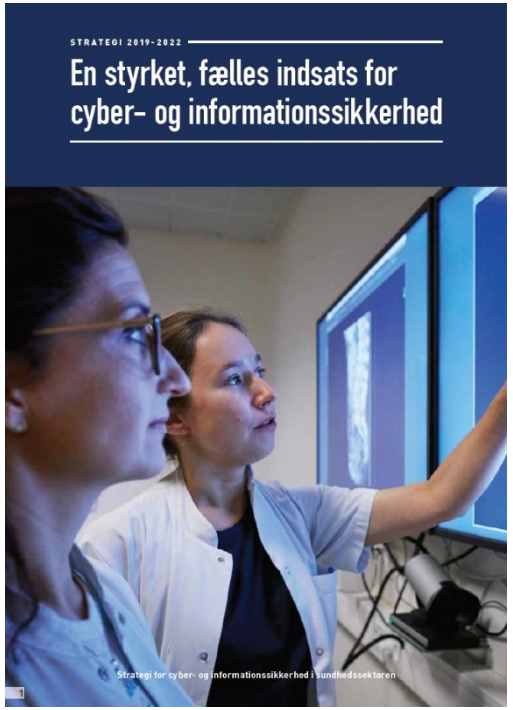
SUNDHEDSDATA-STYRELSEN

Strategi "siden"

Den nationale strategi for cyber- og informationssikkerhed fra maj 2022-2024

Primære fokusområder
- Hver sektor skal lave en strategi
- Oprette en DecentralCyber- og InformationsSikkerhedsenhed

Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022



Yderligere fokus
- Mere fokus på operative kapaciteter
- Mere fokus på samarbejde på tværs
- Flere faste krav til cybersikkerheden

Ny strategi 1/1 2023
- Videreføre alt det gode
- Fokus på de mindre aktører
- Fokus på at udnytte potentialer bedst muligt

https://digst.dk/strategier/cyber-og-informationssikkerhed/

https://sundhedsdatastyrelsen.dk/da/strategier-og-projekter/cyberstrategi

SUNDHEDSDATA-STYRELSEN

Strategiens udmøntning

Styregruppe

Sundhedsdatastyrelsen

Sundheds- og Ældreministeriet, Danske Regioner, Region Midt, Region Nord, Region Hovedstaden, KL, Digitaliseringsstyrelsen, Center for Cybersikkerhed, MedCom, Sundhed.dk, PLO, Sundhedsstyrelsen

Programledelse

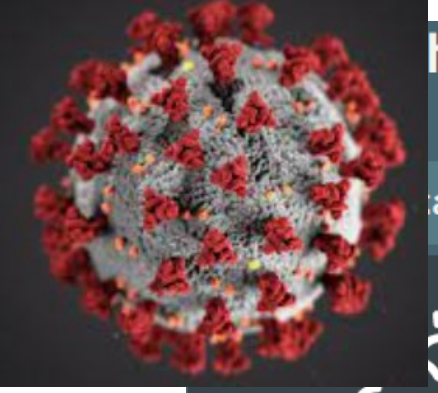
DCIS

Sekretariat

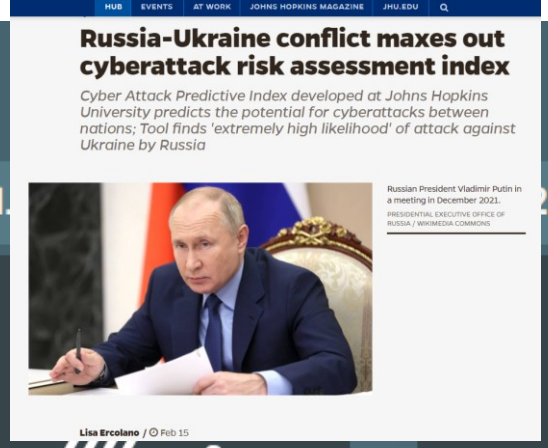
Hovedinitiativerne

1. Forudse hændelser	2. Forebygge hændelser	3. Opdage hændelser	4. Håndtere hændelser	5. Styring og effekt
1.1 Identifikation af kritiske forretningsprocesser og it-systemer på tværs af sektorens aktører 1.2 Bedre overblik over sundheds-sektorens sårbarheder og risici 1.3 Effektiv koordination af varsler 1.4 Klarhed over den enkelte aktørs rolle og ansvar 1.5 Deltagelse i relevante internationale fora om cyber- og informationssikkerhed på sundhedsområdet	2.1 Sikkerhed starter med medarbejderne 2.2 Styrket teknisk sikkerhed i sektorens løsninger og it-infrastruktur 2.3 Håndtering af sikkerheden i ældre it-systemer og –udstyr 2.4 Øget sikkerhed i online medicinsk udstyr 2.5 Skærpede sikkerhedskrav til it-leverandører 2.6 Udbygning af sektorens sikkerhedsarkitektur	3.1 Løbende tests af sikkerheden i sundhedssektorens systemer og udstyr 3.2 Etablering af overvågnings- og analysefunktioner 3.3 Effektiv håndtering af mistanke om hændelser	4.1 Hændelseshåndtering 4.2 Tværgående samarbejde om fælles it- og cyberberedskab 4.3 Beredskabsøvelser for fælles systemer og forsyningskæder	5A løbende opdatering af porteføljeoverblik 5B Årshjul cyklus 5C Forslag til kommende års review 5D Databaseret effektmåling 5E Løbende dialog med private aktører

SUNDHEDSDATA-STYRELSEN



hændelser i sundhedssektoren



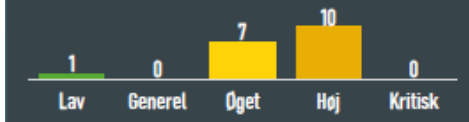
al 2021

Generel

Udvalgte varsler

- Kritisk sårbarhed i FortiWeb OS
- Aktiv udnyttelse af ProxyShell sårbarheder
- Sårbarheder i Atlassain Confluence
- Sårbarheder i Palo Alto produkter

Antal udsendte varsler



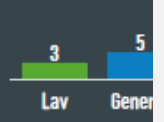
4. Kvartal 2021

Øget

Udvalgte varsler

- Kritisk sårbarhed i Apache Log4j kodebibliotek
- Citrix ADC, Citrix Gateway og Citrix SD-WAN WANOP
- Zero-day i Windows installer (MSI)
- Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products

Antal udsendte varsler



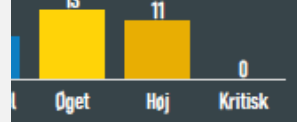
1.

Øget

Udvalgte varsler

- Destruktive cyberangreb observeret mod ukrainske organisationer
- Zero-day fix til apple enheder
- Zero-day i Google Chrome browser
- Øget fokus på kritisk infrastruktur
- 2 Zero-days i Mozilla Firefox
- Sårbarhed i Infusionspumper

Antal udsendte varsler



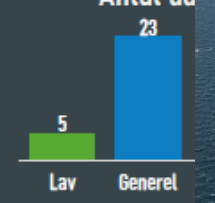
2. Kvartal 2022

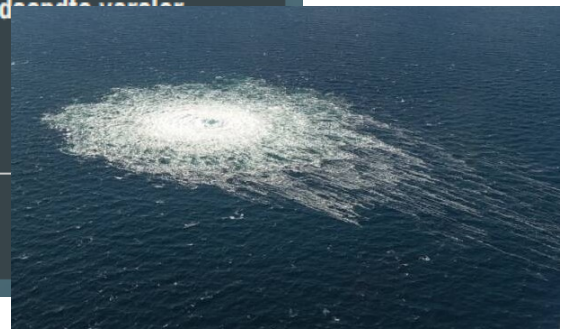
Generel

Udvalgte varsler

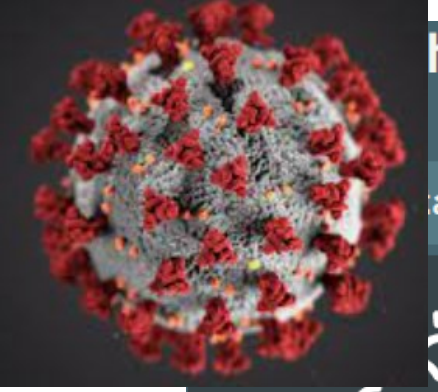
- Kritiske sårbarheder i VMware
- Kritisk opdatering til Zyxel firewlls og VPN
- TLSstorm sårbarhed i Avaya og Aruba
- Hackere udnytter kritisk fejl i Zyxel firewalls og VPN'er
- Alvorlige sårbarheder i SonicWall SSLVPN SMA 1000-serien

Antal ud





SUNDHEDSDATA-STYRELSEN



hændelser i

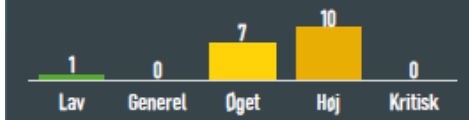
al 2021

Generel

Udvalgte varsler

- Kritisk sårbarhed i FortiWeb OS
- Aktiv udnyttelse af ProxyShell sårbarheder
- Sårbarheder i Atlassain Confluence
- Sårbarheder i Palo Alto produkter

Antal udsendte varsler



SOCRadar

BlueBleed

1
Bucket

2TB
Sensitive Data

111
Countries

65,000
Entities

133,000
Project Files

548,000
Users

Source: SOCRadar

ut
dex
ins
en
gainst

dimir Putin in
er 2021.
OFFICE OF
MONS

2. Kvartal 2022

Generel

Udvalgte varsler

Kritiske sårbarheder i VMware

Kritisk opdatering til Zyxel firewlls og VPN

TLSstorm sårbarhed i Avaya og Aruba

Hackere udnytter kritisk fejl i Zyxel firewalls og VPN'er

Alvorlige sårbarheder i SonicWall SSLVPN SMA 1000-serien

Antal ud

SUNDHEDSDATA-
STYRELSEN

Sundhedssektorens samarbejde omkring cyber- og informationssikkerhed

SUNDHEDSDATA-
STYRELSEN

Ansvar for cybersikkerhed

Spionage og nationens frihed

Som national efterretnings- og sikkerhedsmyndighed har PET til opgave at identificere, forebygge og imødegå trusler mod friheden, demokratiet og sikkerheden i det danske samfund. Det gælder såvel trusler i Danmark som trusler, der er rettet mod danskere og danske interesser i udlandet.

Kriminel efterforskning

Rigspolitiet NC3
@Rigspoliti_NC3

Nationalt Cyber Crime Center (NC3) er Rigspolitiets center for cyberkriminalitet. For tips eller anmeldelser ring 114 eller besøg politi.dk

CENTER FOR CYBERSIKKERHED

Forebyggelse af cyberangreb

Som national it-sikkerhedsmyndighed og kompetencecenter for cybersikkerhed varetager centeret en række forebyggende opgaver. Arbejdet indebærer information til samt vejledning og rådgivning af danske myndigheder og virksomheder i at styrke cybersikkerheden og imødegå cyberangreb.

Netsikkerhedstjenesten

Omdrejningspunktet for netsikkerhedstjenestens arbejde er ikke almindelige cybertrusler og simple angreb – dem skal myndighederne og virksomhederne i første omgang selv skal forholde sig til.

Netsikkerhe… …ftest udfø… …eller cyberangreb, der i øvrigt kan påvir… …grad.

SUNDHEDSDATA-STYRELSEN

REGION NORDJYLLAND – i gode hænder

medcom

KL

PRAKTISERENDE LÆGERS ORGANISATION

midt regionmidtjylland

Region Hovedstaden

FAS

REGION SJÆLLAND – vi er til for dig

Region Syddanmark

DI

MEDICO INDUSTRIEN

Cyber kriminalitet
Collateral damage
Industri spionage

Forskellen på "cyberangreb"

Rekognoscering

Angrebs forsøg
(fx forsøgt udnyttelse
af sårbarhed)

Angreb udført
(angriber har adgang)

Angreb gennemført
(data exfiltreret)

DCIS værktøjer

CYCOGNITO

Rekognoscering

Blueliv.

CTI LEAGUE

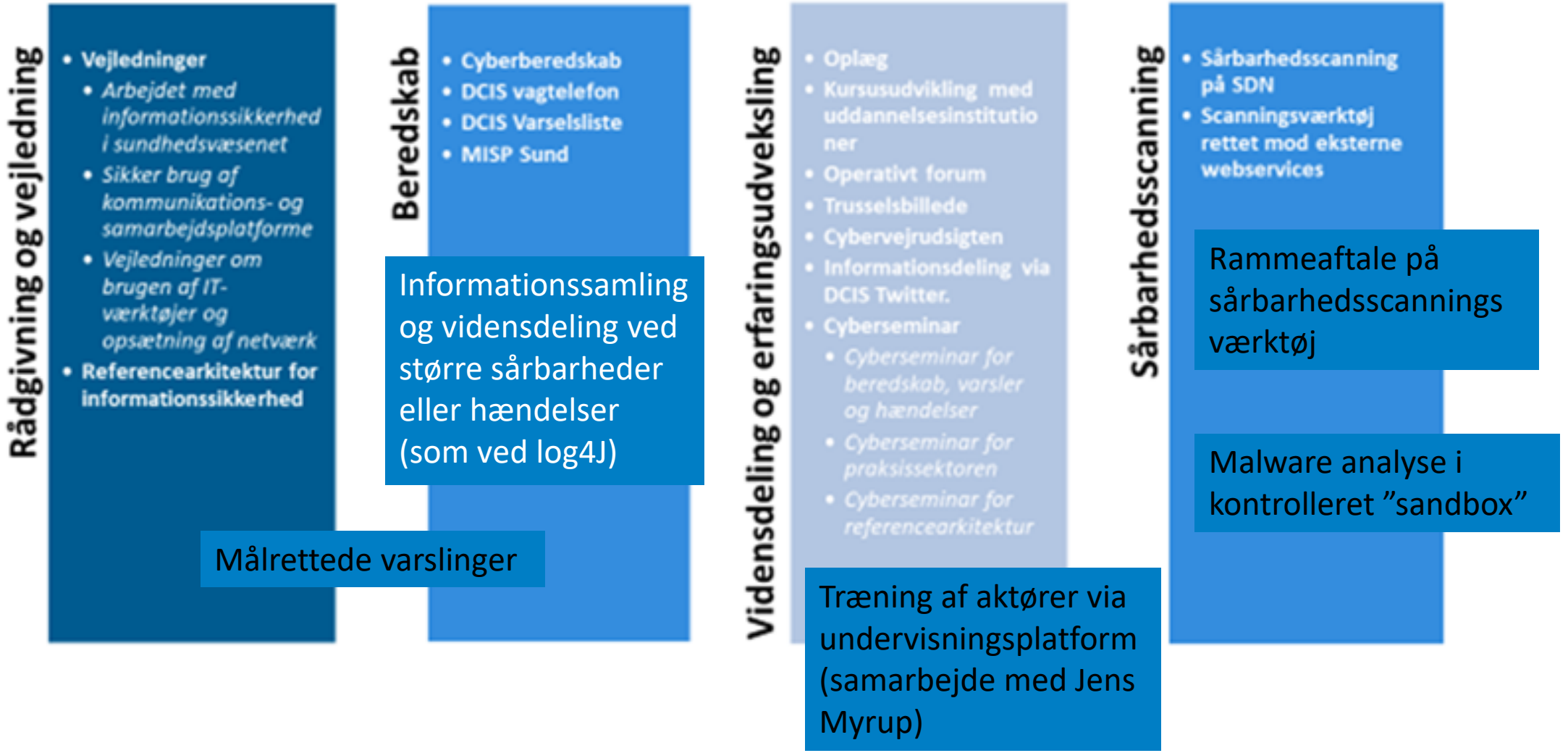
FE CENTER FOR CYBERSIKKERHED

HelseCERT

Angreb gennemført
(data exfiltreret)

SUNDHEDSDATA-STYRELSEN

DCIS produkter og services.



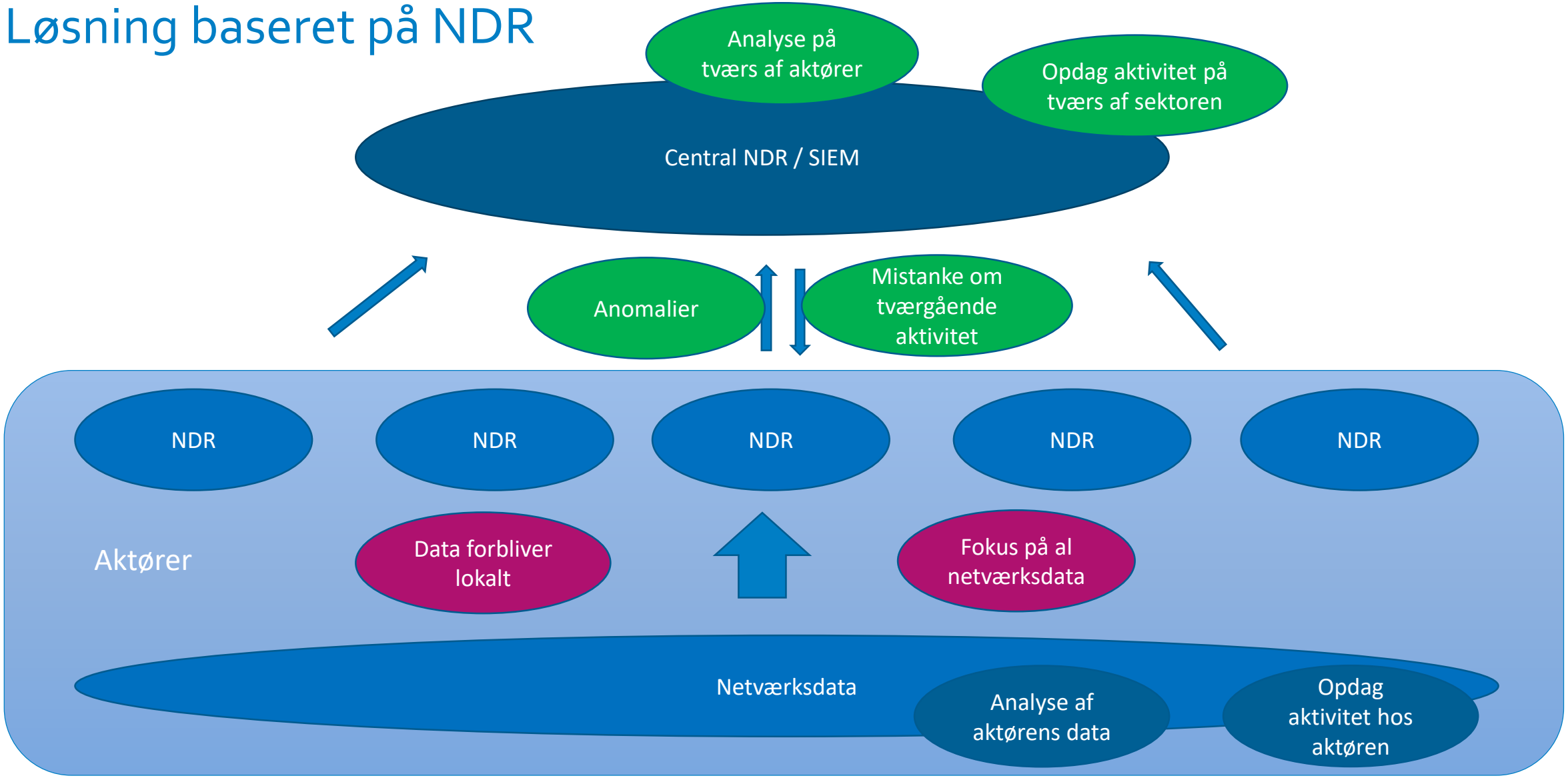
Aktivitets informations fra overvågning- og analyseplatform

Samlet indsats for at opdage tværgående og koordinerede hackerangreb

3.2 Etablering af funktioner til overvågning og analyse af aktivitet på sundhedssektorens it-systemer og -infrastruktur

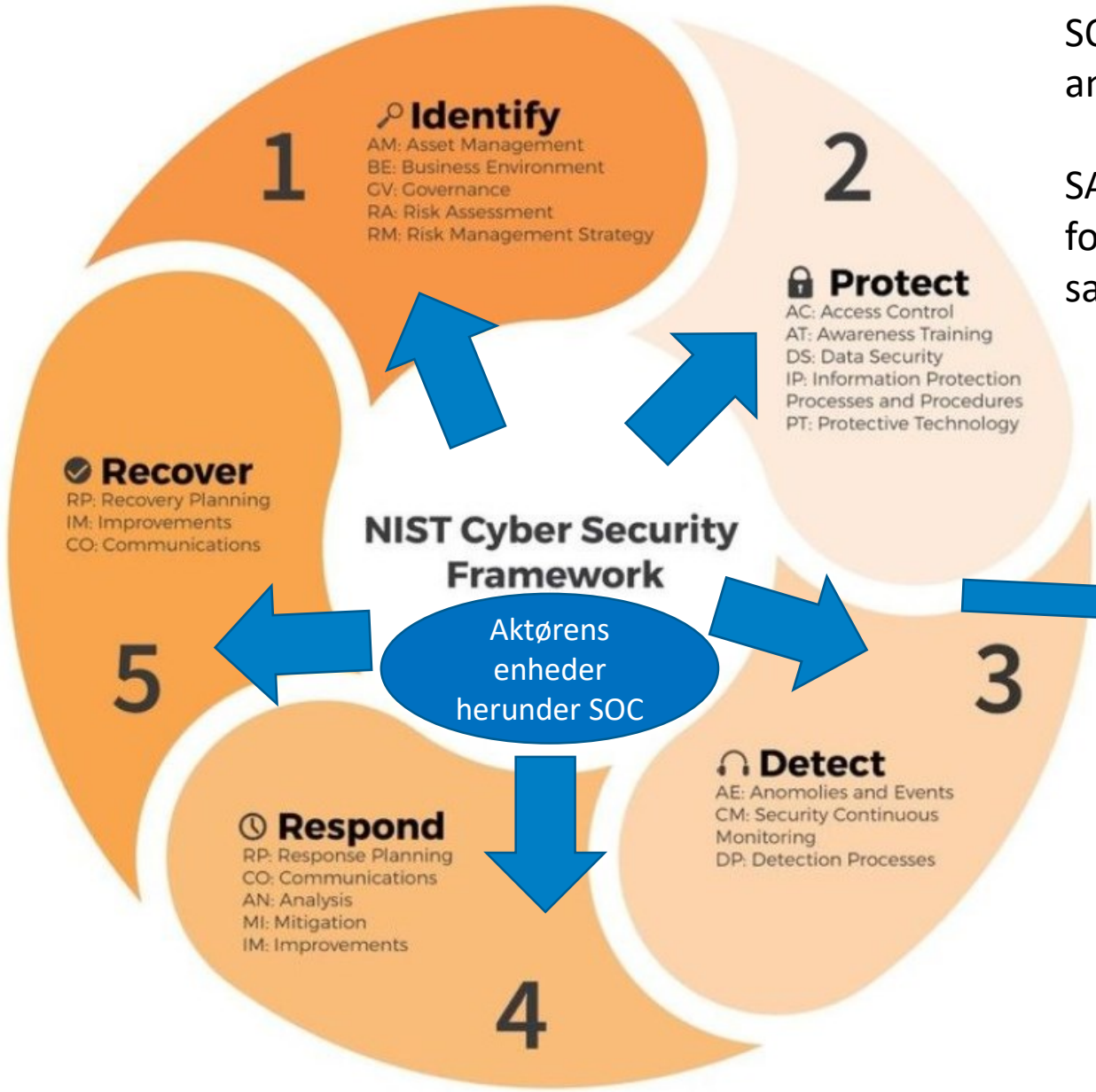
SUNDHEDSDATA-STYRELSEN

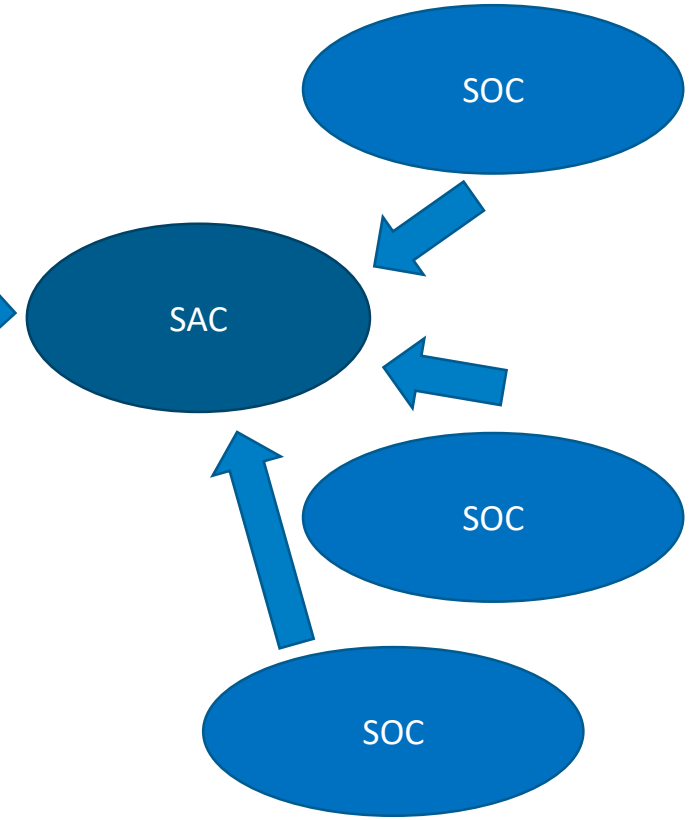
Løsning baseret på NDR



SOC = Security operations center med ansvar og focus på lokal aktivitet

SAC = Security analysis center med fokus på tværgående aktivitet og samarbejde på tværs af sektorer

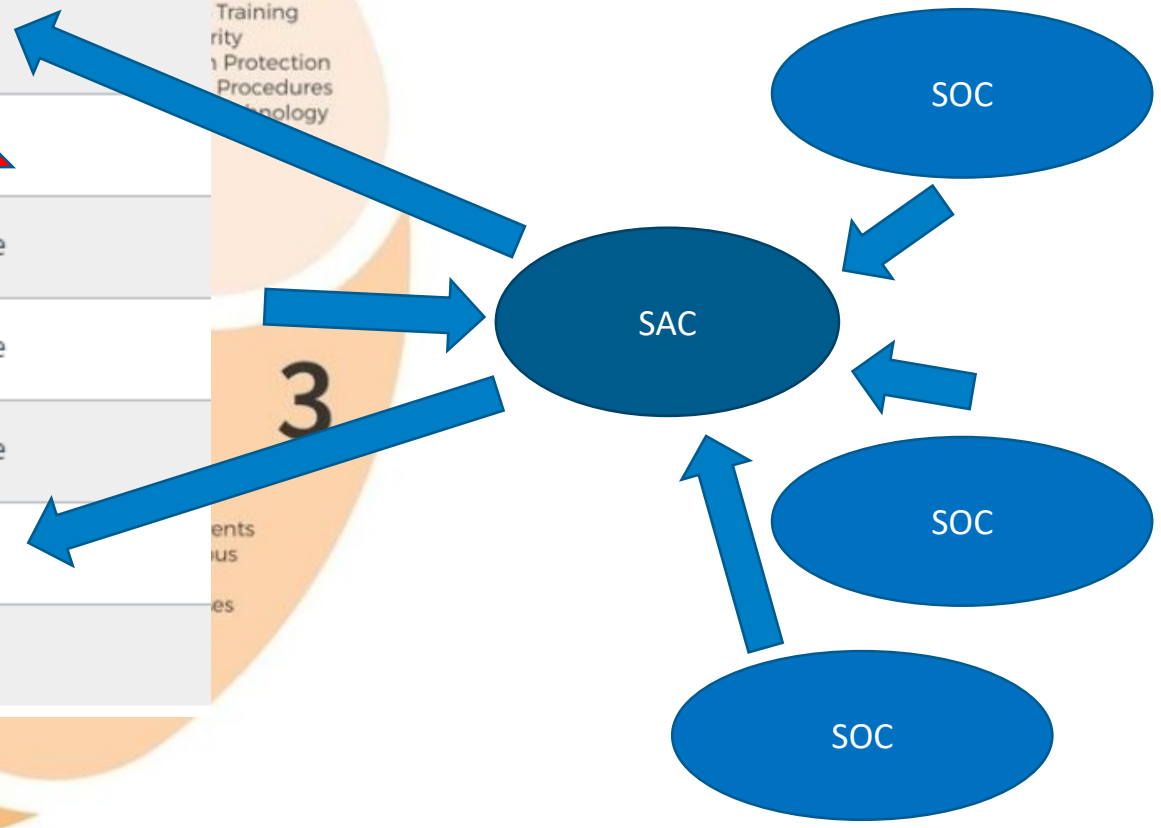




SOC = Security operations center med ansvar og focus på lokal aktivitet

SAC = Security analysis center med fokus på tværgående aktivitet og samarbejde på tværs af sektorer

Impact	Urgency	Priority
Search	Search	Search
1 - High	1 - High	1 - Critical
2 - Medium	1 - High	2 - High
1 - High	2 - Medium	2 - High
3 - Low	1 - High	3 - Mode
2 - Medium	2 - Medium	3 - Mode
1 - High	3 - Low	3 - Mode
3 - Low	2 - Medium	4 - Low
2 - Medium	3 - Low	4 - Low



International

norskhelsenett

H-ISAC HEALTH - ISAC

DCIS-SUND – Sundhedsdatastyrelsen

Triagering
Analysering
Vidensdeling

National

MISP Threat Sharing

ENERGI CERT

TELEDCIS

SØFARTSSTYRELSEN

FINANSTILSYNET

CENTER FOR CYBERSIKKERHED

SAC

Operativt samarbejde og tværgående aktivitet

Sektor

MISP Threat Sharing

SOC

SOC

SOC

SOC

Mulighed for automatisk beskyttelse ud fra IOC'er og IOB'er" i firewall

Operative SOC'er
Hos aktører

SUNDHEDSDATA-STYRELSEN

SUNDHEDSSTYRELSEN

STATENS SERUM INSTITUT

NATIONALT GENOM CENTER

LÆGEMIDDELSTYRELSEN

SUNDHEDS- OG ÆLDREMINISTERIET

STYRELSEN FOR PATIENTKLAGER

STYRELSEN FOR PATIENTSIKKERHED

PRAKTISERENDE LÆGERS ORGANISATION 3436

apotek 468

FAS 1000

KL 98

REGION NORDJYLLAND

Region Hovedstaden

midt regionmidtjylland

REGION SJÆLLAND

Region Syddanmark

Andre private aktører Ca. 2000

DANSKE REGIONER

PL

TANDLÆGE FORENINGEN 1923

SUNDHED DANMARK 27

850

MEDICO INDUSTRIEN

sundhed.dk

medcom

Demo på hvordan vi arbejder ☺

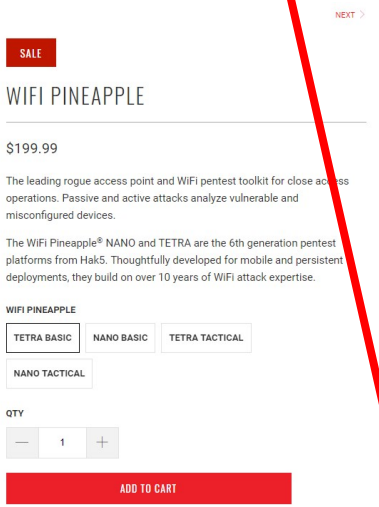
SUNDHEDSDATA-
STYRELSEN

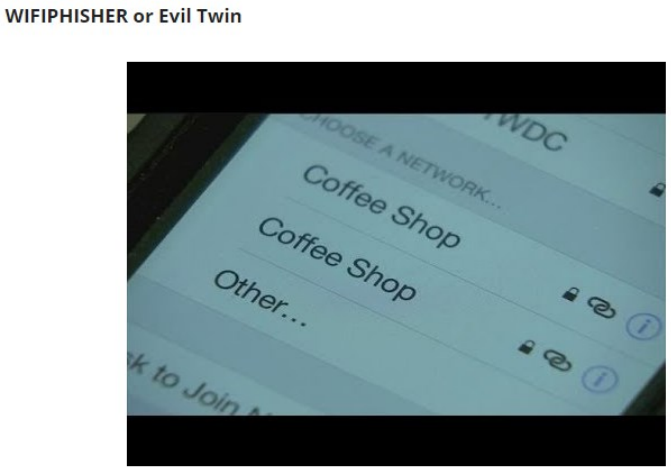
Offentlige Wifi set fra en hacker

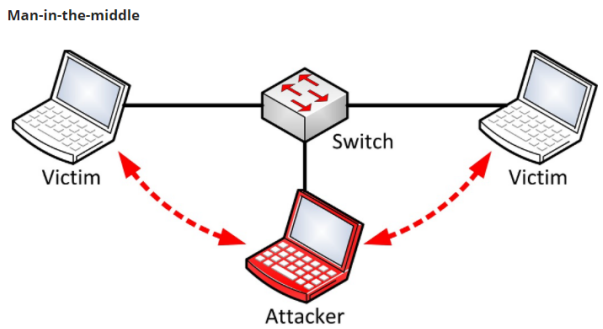
Liste ☺

Din telefon fortæller hele tiden alle de netværk den kender

Hacking







https://e-channelnews.com/top-5-most-dangerous-public-wifi-attacks/

Spørgsmål?

Søren Bank Greenfield

SBGR@sundhedsdata.dk

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk

Kontakt

DCIS Sund

DCISSUND@sundhedsdata.dk

DCISSund på Twitter
@dcissund

DCISSund information
https://sundhedsdatastyrelsen.dk/informationssikkerhed