Hånden under hospitalerne: **Stabil, sikker og effektiv IT**

Forretningsudvalget den 7. maj 2024

Mette Harbo, direktør, Center for IT og Medicoteknologi
Anna Olga Aaskilde Laursen, enhedschef, Center for IT og Medicoteknologi

De fem digitale brændpunkter
(og fire ordens-discipliner)

- Mere værdi af eksisterende IT-systemer
- Mere behandling i hjemmet
- Bedre brug af AI og data
- Styrket digitalisering af diagnostikken
- Cyber- og informationssikkerhed

- Oprydning & konsolidering
- Organisering
- Leverandørstyring
- Økonomistyring

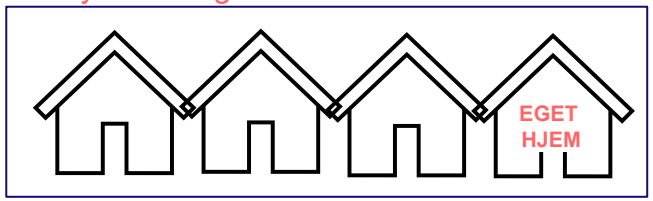
REGION

CYBERSIKKERHED

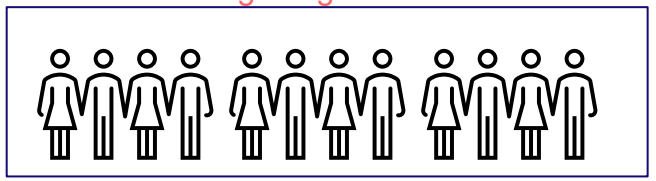
- Handler om at håndtere trusler fra cyberangreb,
- hvor en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester
- med det formål at genere forretningen eller stjæle data.

ANGREBSFLADER

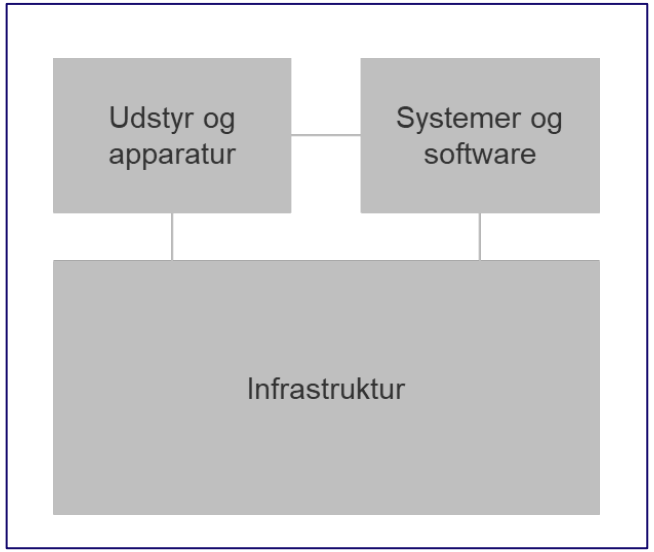
Den fysiske angrebsflade



Den menneskelige angrebsflade



Den digitale angrebsflade



REGION HOVEDSTADEN

- 90+ lokationer
- 700+ bygninger

- 45.000+ medarbejdere
- Studerende
- Vikarer
- Forskere
- Eksterne konsulenter

- 1500+ systemer og software
- Både central og decentral systemforvaltning
- 150.000+ stk. medicoteknisk apparatur
- 80.000+ PC'er, mobiltelefoner, tablets
- 2 primære datacentre
- 700+ fysiske servere
- 5000+ virtuelle servere
- … og meget mere

EKSTREMT HØJ KOMPLEKSITET
BÅDE TEKNISK OG ORGANISATORISK

REGION

FORSVARSDISCIPLINER

Forudse — Ved vi hvilke trusler, der kan ramme os og hvor vi er sårbare?

Forebygge — Har vi gjort tilstrækkeligt for at forhindre at vi bliver ramt?

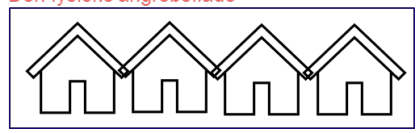
Opdage — Hvor hurtigt kan vi opdage og inddæmme et angreb?

Håndtere — Hvordan er vi gearet til at håndtere og reducere impact af et cyberanbreb?

KAPABILITETER

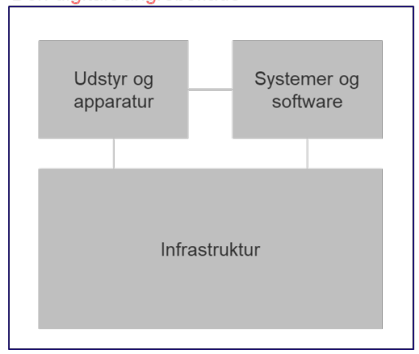
- **Trusselsvurderinger**
- **Varslingstjenester (leverandører, DCIS, CFCS)**
- **Modenhedsanalyser**
- **Tilsyn og revision**
- **Risikovurderinger**
- **Tekniske sikkerhedstest (eks. penetrationstest)**

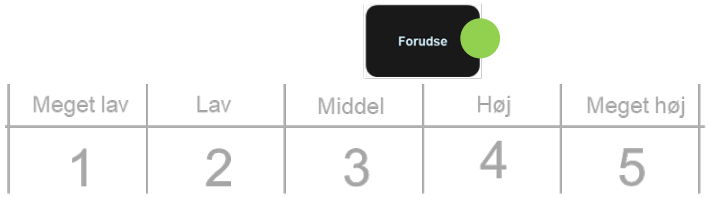
Den fysiske angrebsflade



Den menneskelige angrebsflade

Den digitale angrebsflade





FORSVARSDISCIPLINER

Forudse	Ved vi hvilke trusler, der kan ramme os og hvor vi er sårbare?
Forebygge	Har vi gjort tilstrækkeligt for at forhindre at vi bliver ramt?
Opdage	Hvor hurtigt kan vi opdage og inddæmme et angreb?
Håndtere	Hvordan er vi gearet til at håndtere og reducere impact af et cyberanbreb?

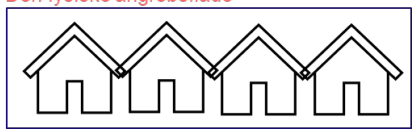
KAPABILITETER

- **Retningslinjer og politikker**
- **Sikkerhedskultur**
- **Core infrastruktur (eks. antivirus, firewalls, geoblokering)**
- **Cloudsetup**
- **Systemer**
- **Udstyr**
- **Patch Management**
- **Brugerstyring**

Forebygge

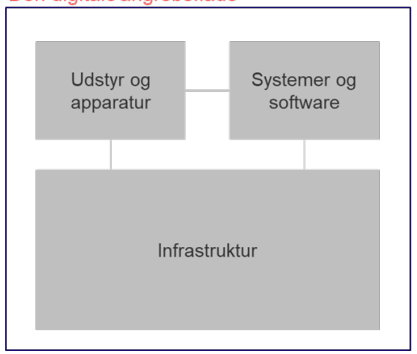
Meget lav	Lav	Middel	Høj	Meget høj
1	2	3	4	5

Den fysiske angrebsflade



Den menneskelige angrebsflade

Den digitale angrebsflade



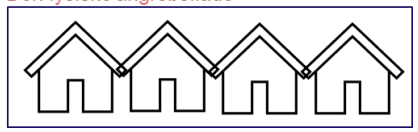
FORSVARSDISCIPLINER

Forudse	Ved vi hvilke trusler, der kan ramme os og hvor vi er sårbare?
Forebygge	Har vi gjort tilstrækkeligt for at forhindre og reducere impact?
Opdage	Hvor hurtigt kan vi opdage og inddæmme et angreb?
Håndtere	Hvordan er vi gearet til at håndtere et aktivt cyberanbreb?

KAPABILITETER

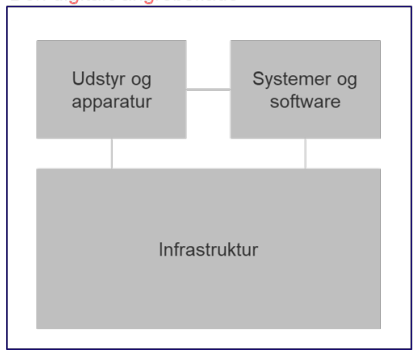
- **Lokalt Security Operation Center (24/7)**
- **Ekstern analysekapacitet**
- **Videnssdeling i sektoren (MISP)**
- **Overvågning og monitorering**
- **Sårbarhedsscanninger**

Den fysiske angrebsflade



Den menneskelige angrebsflade

Den digitale angrebsflade



Opdage

Meget lav	Lav	Middel	Høj	Meget høj
1	2	3	4	5

FORSVARSDISCIPLINER

Forudse — Ved vi hvilke trusler, der kan ramme os og hvor vi er sårbare?

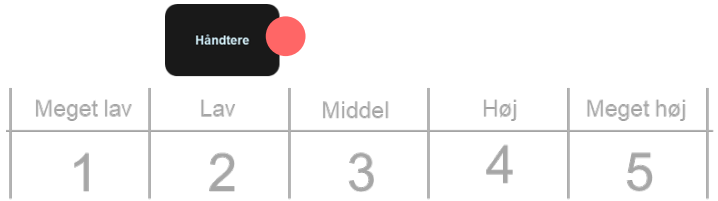
Forebygge — Har vi gjort tilstrækkeligt for at forhindre og reducere impact?

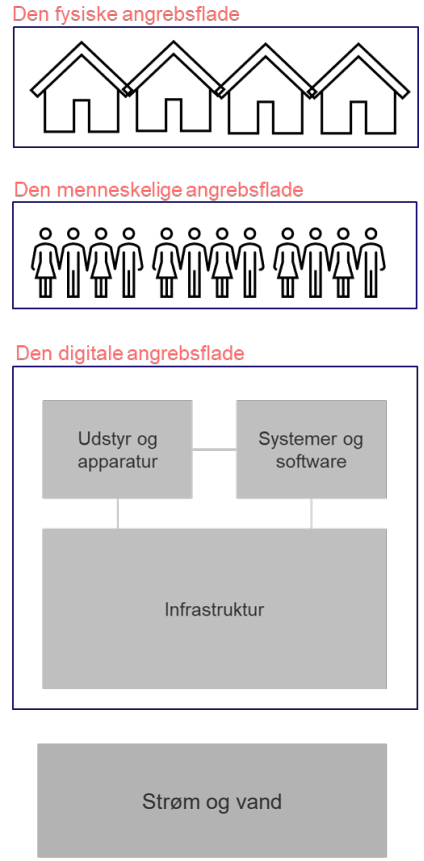
Opdage — Hvor hurtigt kan vi opdage og inddæmme et angreb?

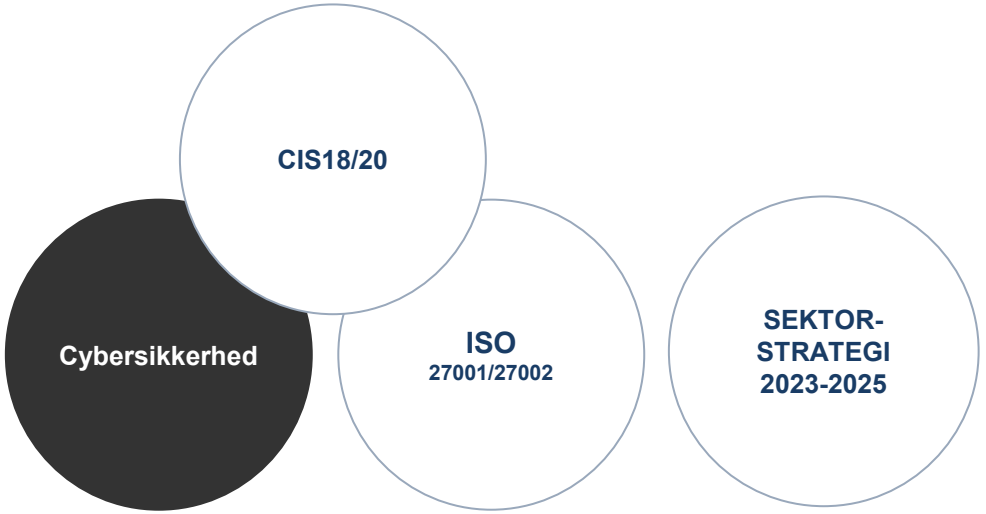
Håndtere — Hvordan er vi gearet til at håndtere et aktivt cyberanbreb?

KAPABILITETER

- IT-beredskab
- Lokale nødberedskaber
- Nødplaner for systemer
- Redundans
- Netværkssegmentering
- Backup og restore
- Forsyningsberedskab
- Regionalt kriseberedskab

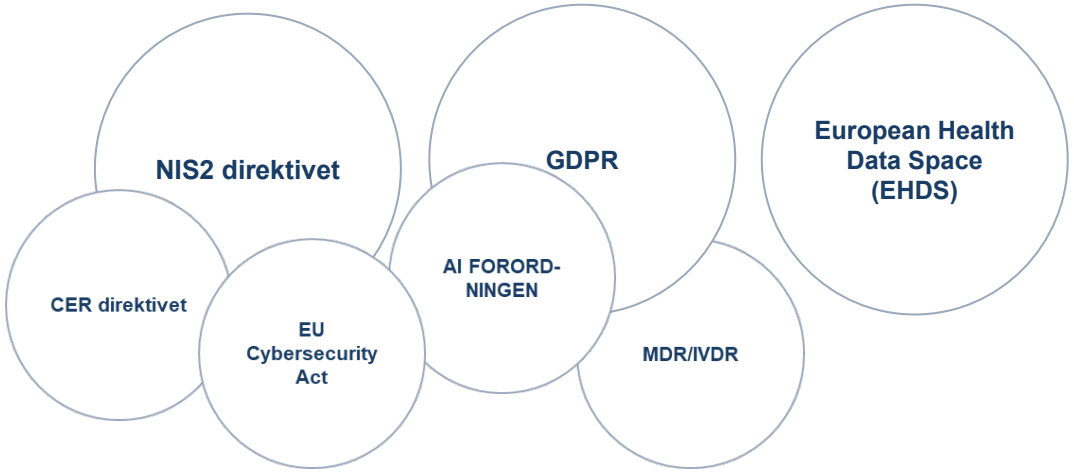






SAMLET STRATEGI FOR CYBER- OG INFORMATIONSSIKKERHED I REGION HOVEDSTADEN

Fremlægges for primo juni 2024



- Digital Agilitet
- Sikkerhedskultur
- Regulering & Governance
- Cyberværn
- Resiliens

Transformation af regionens IT-infrastruktur

Stor variation og volumen i platforme og teknologier

- Fokus på standarder - udfasning af legacy

Teknologiske udløbsdatoer er nær

- Nye krav til kompetencer og investeringer

Manglende eksekveringskraft

- Kapacitet og kapabilitet er udfordret

Understøttelse af cyber nødvendigt

- Netværkssegmentering, medicoudstyr og backup