



Europæisk cybersikkerhed i en forandret verden

Jonathan Kirdorf, Cyber og Informationssikkerhed,
Cyber og Robusthed i Sundhedssektoren
Digital Sundhed Danmark





Digital Sundhed Danmark - Helt kort

Digital Sundhed Danmark er sat i verden for at understøtte sundhedsreformen gennem data, digitale løsninger og fælles infrastruktur.



Understøtte
omstilling til det
nære
sundhedsvæsen



Understøtte
sammen-
hængende
patientforløb



Udvikle og udbrede
brugervenlige
digitale løsninger og
infrastruktur



Styrke det
innovative
sundhedsvæsen



Sikre
sundhedsdata i
verdensklasse



Sikre et robust
beredskab
indenfor
cybersikkerhed

Data er ikke et mål i sig selv. Data skal skabe nærhed, sammenhæng og bedre behandling.



Europæisk cybersikkerhed i en forandret verden

Hvorfor ser vi i disse år en bølge af regulering med fokus på sikkerhed og robusthed?

Hvad er det for nogle grundlæggende problemer, som EU forsøger at imødekomme?

Hvor bevæger vi os hen?



Videre til reguleringsjunglen



Fra cybersikkerhed til digital suverænitet

En bølge af regulering

Cybersecurity act (CSA), Cyber resilience act (CRA), Cyber solidarity act, Network and information Security directive 2 (NIS2), Critical Entities Resilience directive (CER), European Cybersecurity Competence Center (ECCC), Data governance act, Data act, AI-act, European Health Data Space (EHDS), Regulation on electronic identification and trust services 2 (eIDAS2), Chips Act, Health action plan, Digital omnibus, Cloud and AI Development Act, CSA2, Quantum Europe Strategy & Data Union Strategy, Digital Services Act,

Hvad er det vi ser

- De mange EU-initiativer er ikke tilfældige enkeltstående reguleringer. De er forskellige dele af et større projekt.
- Det afspejler en udvikling i EU's syn på cybersikkerhed: fra robuste organisationer, over sikre teknologier, til kontrol over kritiske leverandørkæder.



Første fase: Robuste organisationer

*”To effectively protect Europeans, the European Union needs to continue to reduce vulnerabilities, including for the **critical infrastructures that are essential for the functioning of our societies and economy.**”*

- Proposal for a CER-directive , Context of the proposal

NIS2 og CER

- Samfundets robusthed starter hos de organisationer, der leverer kritiske tjenester.
 - Risikovurdering, Konsekvenser for samfundet, Mindstekrav, Ledelsesansvar
 - Kan hospitaler fortsætte driften
 - Kan energisektoren levere strøm
 - Kan myndighederne håndtere kriser?
- Målet er robusthed i **samfundskritiske funktioner**, ikke bare i netværk eller systemer



Anden fase: Sikre teknologier

“Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union’s economy, but also on democracy as well as consumer safety and health”

-Cyber Resilience Act

CRA og AI Act

Robusthed kræver, at de teknologier organisationerne anvender, er sikre og troværdige igennem deres levetid.

- Security by Design, Produktsikkerhed, Sårbarhedshåndtering bliver krav
- Er softwaren sikker?
- Er de produkter vi omgiver os med sikre
- Kan vi stole på de teknologier vi bygger vores samfund på?
- Fra sikre organisationer til sikre teknologier



Tredje fase: Robuste leverandørkæder

"We cannot afford to depend on others for the technologies that keep our hospitals running, our energy grids stable and our services secure"

-Ursula von der Leyen

Tech Sovereignty Package, CSA2 og CADA

- Nu handler det ikke kun om sikkerhed, men også om kontrol.
 - Leverandører, forsyningskæder, tredjelandsrisici
- Cloud og AI er gået fra at være it løsninger til strategiske kapaciteter
 - Hvem kontrollerer infrastrukturen, hvis jurisdiktion er den underlagt?
 - Hvad gør vi, hvis de kapaciteter vi er afhængige af kontrolleres af andre?
- Fra sikre teknologier til robuste leverandørkæder



Hvorfor sker det nu?

Covid-19

- Sårbare forsyningskæder

Ukraine

- Cyber som geopolitisk værktøj

AI

- Koncentrationen af teknologisk magt

Geopolitik

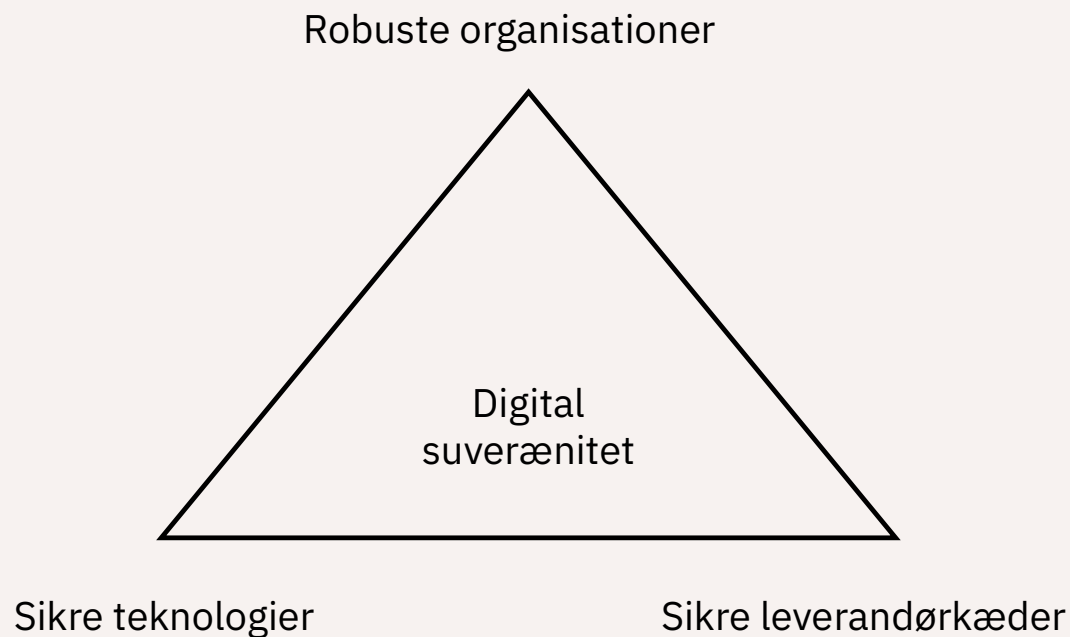
- Gjorde teknologisk kontrol til et sikkerhedspolitisk spørgsmål

EU reagerer ikke kun på cybertrusler.

EU reagerer på en verden, hvor teknologi, økonomi og sikkerhedspolitik i stigende grad hænger sammen.

Det har skabt et ønske om større robusthed og større handlefrihed

Digital suverænitet er summen af udviklingen – ikke én regulering





Hvad kan man gøre for at holde sig opdateret

SundCERTs Kvartalsvise statusmøder
-Trusselbilledet for sundhedssektoren
-Teknik og best practices

Cyberkompasset
-Løbende opdateringer på EU-regulering inden for cyber- og
robusthedsområdet der påvirker sundhedssektoren
-Hjælp til at "oversætte" EU-regulering til sundhedssektorens
kontekst

SundCERTAdmin@sundhedsdata.dk



Tak for ordet



Følg med på LinkedIn for seneste nyt