

MODERNE TRUSLER OG MODERNE LØSNINGER.

Gert Læssøe Mikkelsen

Head of Security Lab, Alexandra Instituttet A/S



ALEXANDRA
INSTITUTTET

Alexandra Instituttet er en **non-profit** virksomhed, der arbejder med **anvendt forskning, udvikling og innovation** inden for it



Vi er sat i verden for at skabe **værdi, vækst og velfærd** i det danske samfund.

VEJEN TIL HELVEDE ER BROLAGT MED IOT

- Virker min SmartBrandalarm, hvis der er ild i min WiFi router?

- Virk



artphone



MODERNE TRUSLER, KENDTE LØSNINGER

- Virker vores internet, hvis jeg putter denne dims på nettet?
 - Blev store dele af internettet DDoS'et og lagt ned af en enkelt person? [Brian Krebs]
- IoT giver nye udfordringer
- IoT kræver nye løsninger – fx på sw update.
- Men:
 - Telnet
 - default passwords
- “We're building a world-sized robot, and we don't even realize it.” [Bruce Schneier]



**Moderne virksomheder
er SW-virksomheder**

**Nogen ved det bare
ikke endnu**



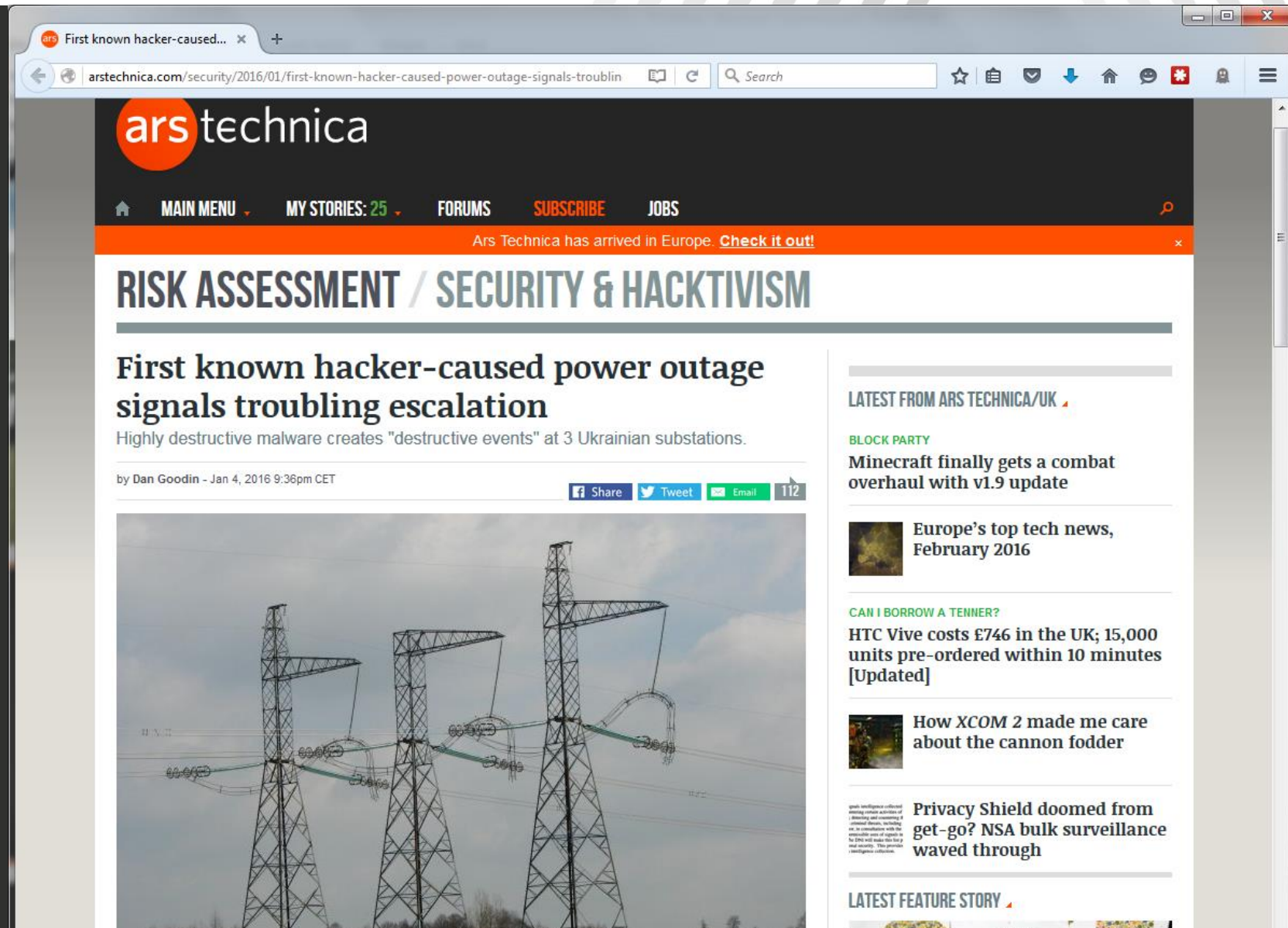
DK VIRKSOMHEDER ER KENDT FOR KVALITET

- Danske virksomheder er kendt produkter af høj kvalitet – det skal de også være kendte for i fremtiden
- Dette er muligt, hvis vi tager sikkerheden seriøst!
- Det er op til os.

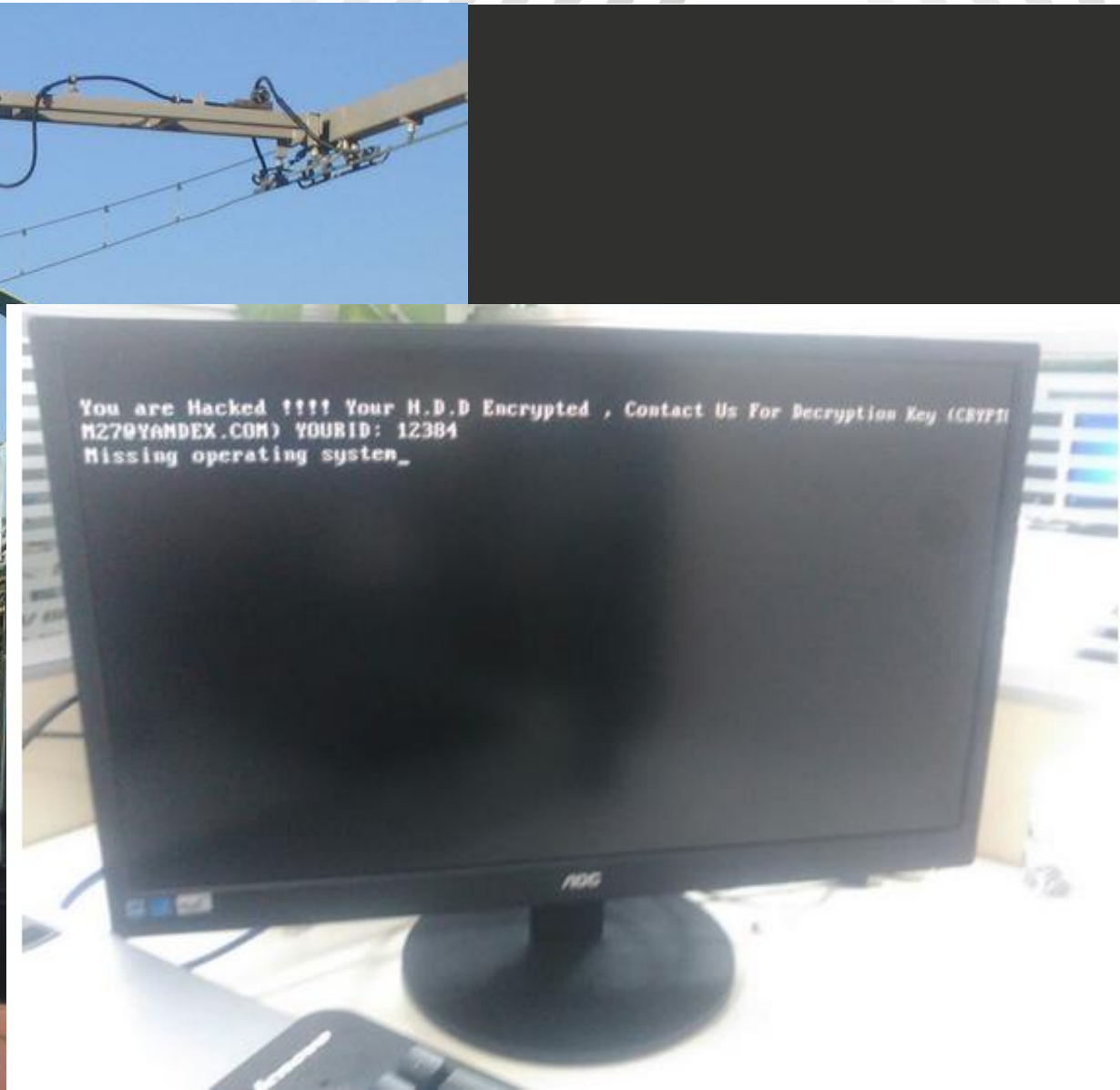
DEN FYSISKE VERDEN PÅ NETTET

- Estland 2007
- Ukraine 2015
- Ukraine 2016

- Finland 2016
 - Uden varme pga. DNS nedbrud



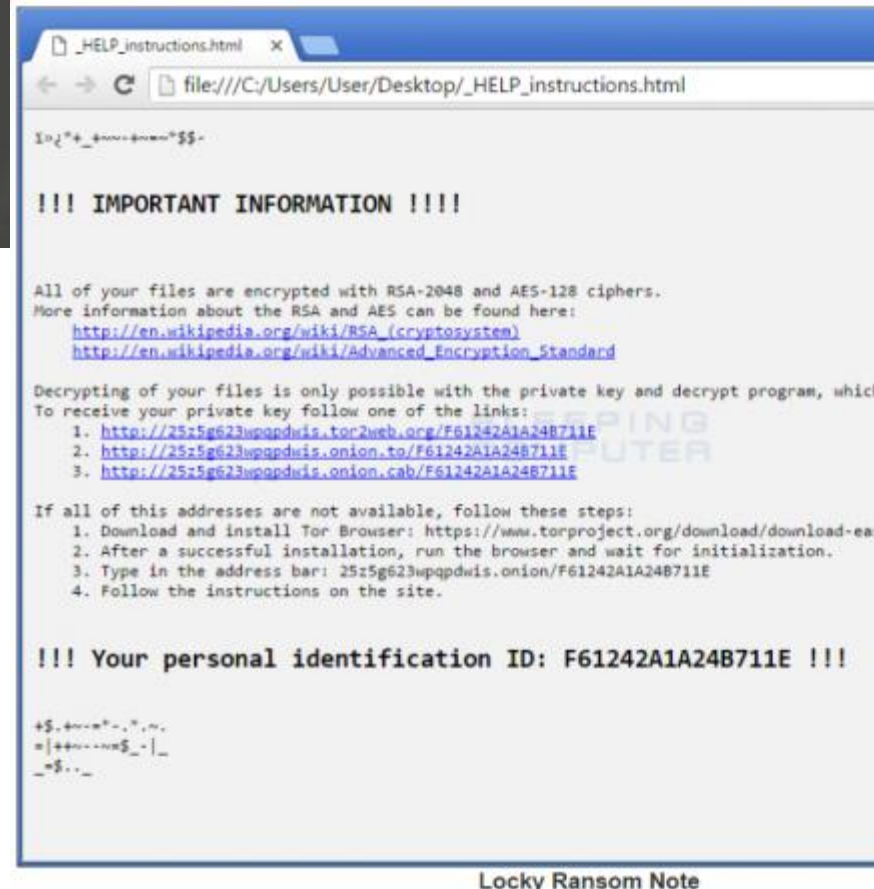
SAN FRANCISCO 2016



CYBERTRUSLEN MOD DANMARK

- Ifølge Center for Cybersikkerhed
 - Truslen fra cyberspionage mod danske myndigheder og private virksomheder er MEGET HØJ
 - Truslen fra cyberkriminalitet mod danske myndigheder og private virksomheder er MEGET HØJ.
 - Truslen fra cyberaktivisme mod danske myndigheder og private virksomheder er MIDDEL.
 - Truslen fra cyberterror mod myndigheder og private virksomheder er LAV.

[CFCS jan 2016]



Locky Ransom Note

DATA IS THE NEW OIL

- DATA
 - "Det 21. århundredes olie"
 - Både forretningsmæssigt, men også det der vil drive samfundsudviklingen – på godt og ondt
 - Interessekonflikter
 - Virksomheder vs. Individet
 - Samfundet vs. Individet
 - Individet vs. Individet

Big data is like teenage sex:
everyone talks about it,
nobody really knows how to do it,
everyone thinks everyone else is
doing it, so everyone claims they
are doing it...

(Dan Ariely)



EU PERSONDATAFORORDNING - GDPR

- Kommer politikerne og ødelægger den gode stemming?
- Begrænsninger i hvad man må med persondata
 - Krav til sikring af data
 - Krav til anonymisering
 - Krav til pseudonymisering
 - Krav til samtykke (men ikke altid!) – hvordan?
 - Hårdere straf
- “Mere fair konkurrence for dem der gør det godt!”
- “Spændende at se hvordan det i praksis bliver.”



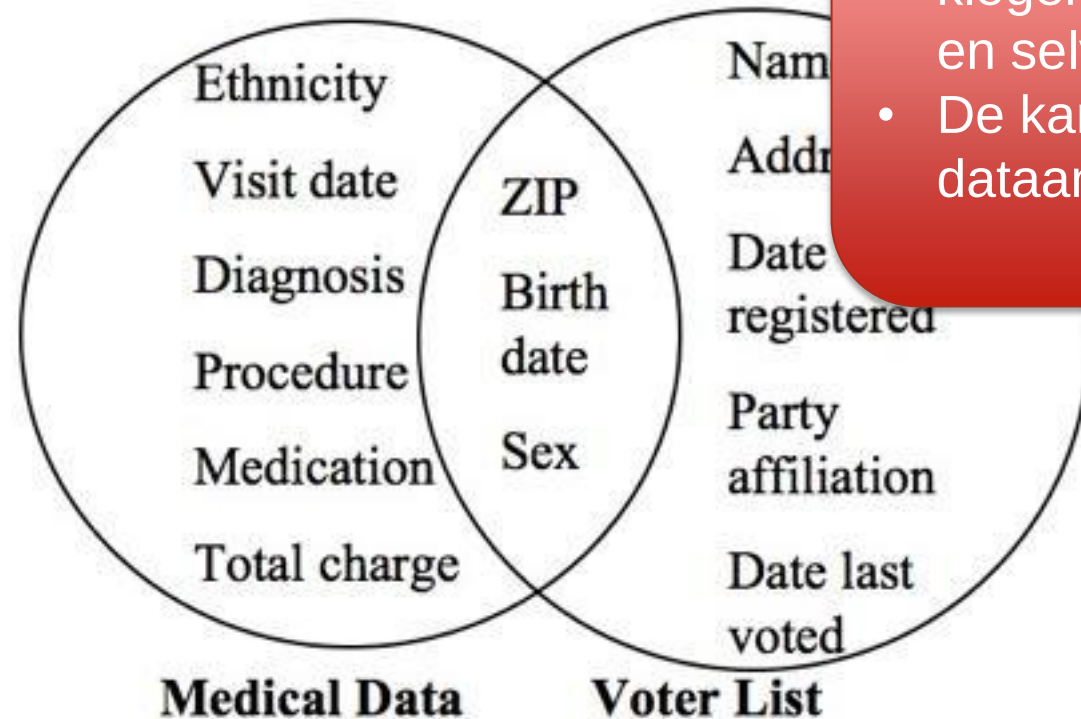
EU PERSONDATAFORORDNING - GDPR

- Er det er trussel mod danske virksomheder?
- Ja og nej, men kom i gang, I har 18 måneder.
 - Lever I op til persondataloven?
 - Hvad har I af persondata?
 - Hvor har I persondata?
 - Hvorfor har I persondata?
 - Datatilsynets 12 spørgsmål.
- Data beskyttelse via design (privacy by design)
 - Anonymisering
 - Pseudonymisering
 - Kryptering af data
 - ...



SÅ ANONYMISERE VI BARE DATA!

- Guvernøren for Massachusetts
helbredsdata lækket



HUSK:

- Der findes sikkert klogere personer end en selv
- De kan bruge dataanalyse etc.



- seudonomiserede og
iserede et dataset og
offentliggjorde det
- Det blev linket til IMDB
- Afslørede ekstra data om brugerne.

DIFFERENTIAL PRIVACY

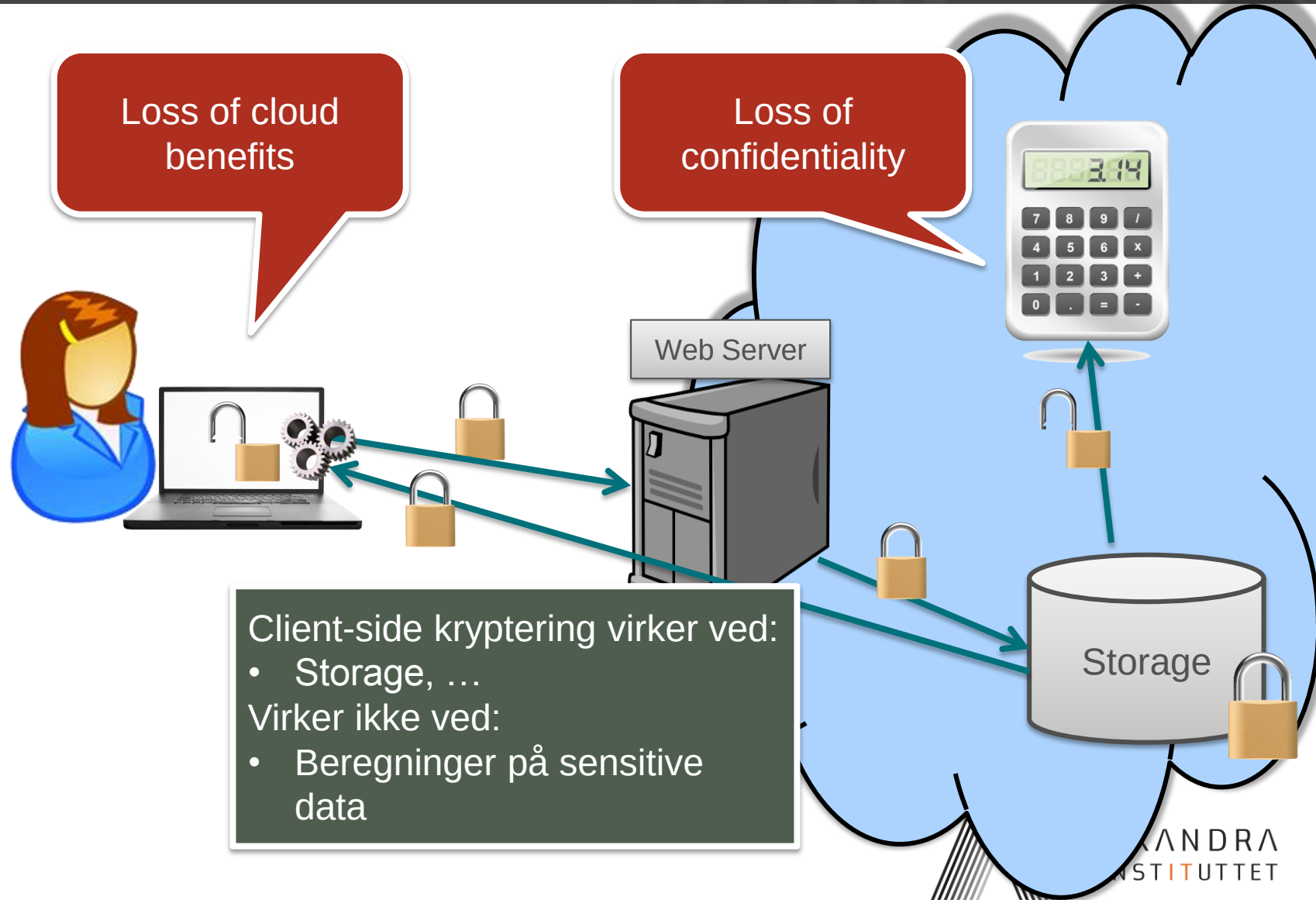
- Stærk definition af anonymisering
- Matematisk defineret
- Ide 1:
 - Tilføje støj - formaliseret.
- Ide 2:
 - Dataset A, og B
 - Hr. Jensen er i A, men ikke i B
 - Alle analyser på anonymiseret(A) og anonymiseret(B) giver (næste) ens resultat.
 - (næsten) er kvantificeret matematisk.



KRYPTERING – AVANCERET

- Nye metoder der tillader beregninger på krypteret data

- Fully Homomorphic Encryption FHE
- Secure Multiparty Computation MPC
- Beregninger på krypterede data
 - Fra flere kilder
 - I flere organisationer



MPC EKSEMPLER

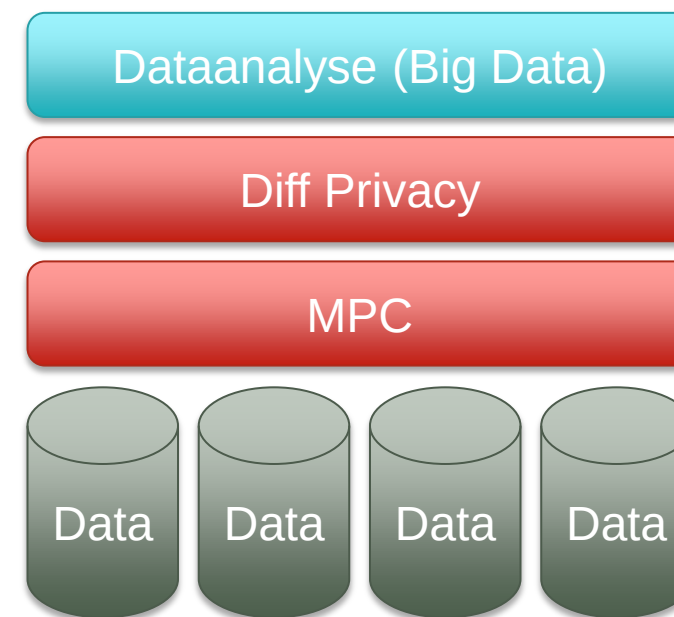
- Funktion beregnet på data fra flere parter.
 - Hver part kryptere egne data
 - De laver sammen en beregning på de krypterede data
 - Kryptered svar kan dekrypteres.
- Alexandra Institutet – Generelle løsninger
- Sepior – Nøglehåndtering i cloudløsninger
- Partisia – Konkrete løsninger, auktioner og surveys
- Projektet Big Data by Security
 - Benchmarking af bankkunder
 - Lån på auktion
 - Confidential benchmarking

Konference i marts



SODA PROJEKTET

- EU Forskningsprojekt 2017-2020
 - Alexandra,
 - Aarhus Universitet,
 - Philips,
 - Technische Universiteit Eindhoven,
 - Goettingen Universitet.
- Big Data sammen med Differential Privacy
- Sikker dataanalyse af sundhedsdata
- Både ny teori, implementationer og prototype.



DON'T TRY TO FIX THE USER!

- Vi har i 20 år givet brugerne teknologi, hvor de kan:
 - sende og modtage emails
 - Tilslutte ting til deres computer (fx USB)
 - Klikke på links og komme rundt på internettet
- Vi har i 20 år advaret brugerene mod:
 - emails
 - at tilslutte ting til deres computer (fx USB)
 - Klikke på links
- Nu må de da snart lære det
- **eller måske burde vi lære det!**

Tak for opmærksomheden!



ALEXANDRA
INSTITUTTET