Skytjenester og sikkerhet sett fra NSM

2021-09-17-NIFS

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner

Agenda

1. Kort om NSM, NCSC og John
2. Noen av NSMs bekymringer
3. Betydning av fysisk plassering av datasenter
4. Kryptering av kundedata
5. (Hvordan styrke sikkerhet i skyen)
6. Avrunding

Illustrasjoner: egne/NSM, Wikipedia, colourbox.com, pixabay.com

Nasjonal cybersikkerhetssenter

- Nasjonalt Cybersikkerhetssenter er en del av NSM

- NSMs fokus: sikkerherhetslov + kristiske samfunnstjenester
  - Har også en plikt til å dele sin kompetanse med samfunnet for øvrig

- John: teknolog med mange år i NSM
  - Utvikling av sikkerhetstiltak
  - Medforfatter av “NSMs grunnprinsipper for IKT-sikkerhet”

Sky

Faglig intro

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

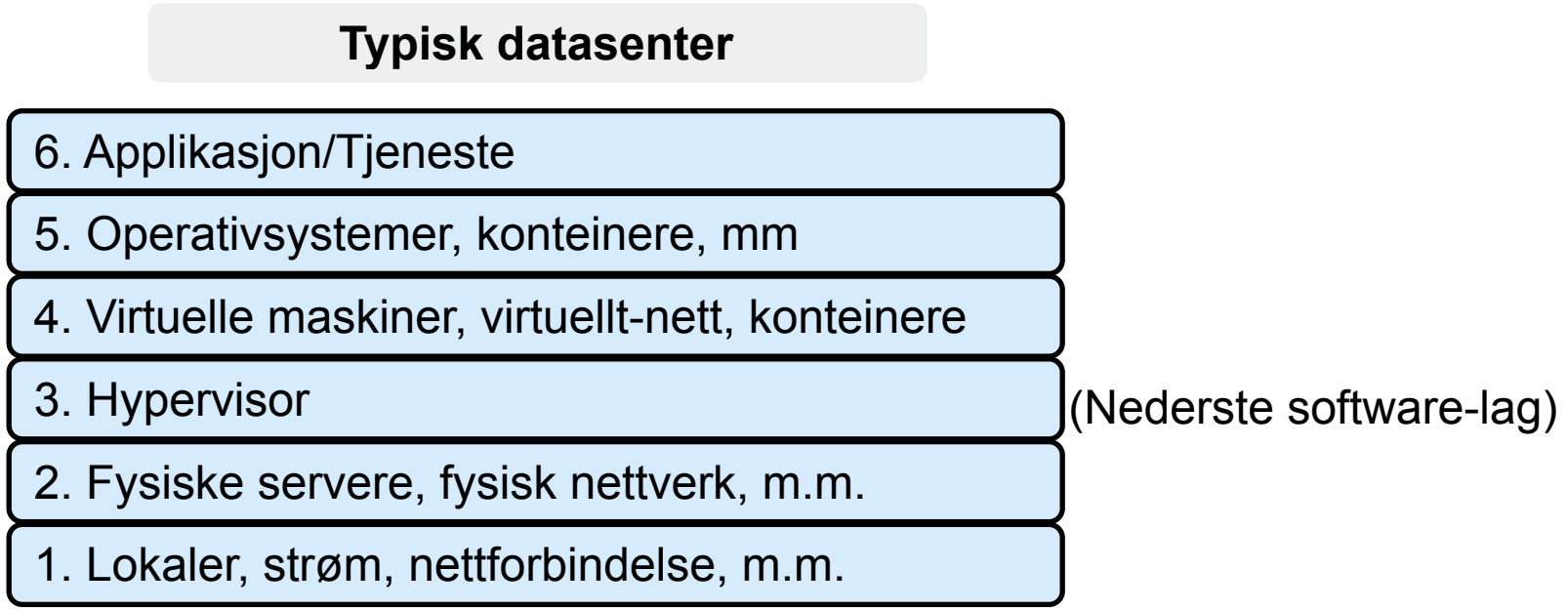
Vanlige myter innen IT-sikkerhet (teknisk fokus)

Vanlige missforståelser/myter:

1) Vi har ingen sårbarheter hvis vi/leverandøren er gode på å patche
2) Kryptert data i skyen kan ikke leses av leverandøren
3) Alt sikkerhetsansvar tar skyleverandøren seg av
4) Regionene til skyleverandørene er avgjørende mht jurisdiksjonen
5) Hvis sky-data er lagret i Norge, da har vi nasjonal kontroll
6) Det er trygt/tryggere på innsiden av brannmuren
7) Antiskadevare/antivirus holder mot skadevare

Litt spissformulert, men likevel dessverre vanlige oppfatninger ...?

Forenklet modell av typisk datasenter



Lag 4-6 er ofte driftet av kundene eller annen leverandør (kjøp av Iaas-tjeneste).
Den som drifter/utvikler lag 3 har teknisk tilgang til alt i lag 4-6.

Sky og sikkerhetsansvar, standard forenkling

	On-premise	Allmenn sky		
		IaaS	**PaaS**	**SaaS**
7. Klient-applikasjon		Virksomhetens/ kundens ansvar		
6. Applikasjon/Tjeneste				
5. OS, konteinere				
4. V-maskin, v-nett, konteinere			Leverandørens ansvar, kundens kontrollansvar	
3. Hypervisor				
2. Fysiske servere m.m.				
1. Lokaler, strøm, internett				

Sky og sikkerhetsansvar, flere modeller

	«On-premise»	Serverplass-leie	Allmenn sky			Privat sky
		Variabelt: med og uten drift	**IaaS**	**PaaS**	**SaaS** O365, Teams, G-suite, mm.	**A la «Azure Stack» og «AWS Outpost»**
7. Klient-applikasjon						
6. Applikasjon/Tjeneste						
5. OS, konteinere						
4. V-maskin, v-nett, konteinere						Variabelt?
3. Hypervisor						
2. Fysiske servere m.m.		Variabelt?				Variabelt?
1. Lokaler, strøm, internett						Variabelt?

Virksomhetens/ kundens ansvar

Leverandørens ansvar, kundens kontrollansvar

Streng tolkning: er f.eks. lag 3 styrt fra utlandet så er alle lagene i praksis utenfor norsk teknisk kontroll.

Sky og reell jurisdiksjon

	«On-premise»	Serverplass-leie	Allmenn sky			Privat sky
		Variabelt: med og uten drift	**IaaS**	**PaaS**	**SaaS** O365, Teams, G-suite, mm.	A la «Azure Stack» og «AWS Outpost»
7. Klient-applikasjon	**Helt under kun norsk lovgivning**		**Helt eller delvis under andre lands lovgivning. Andre land har teknisk adgang til data.** (Uansett kryptering) **(de 3-4 største leverandørene)**			
6. Applikasjon/Tjeneste						
5. OS, konteinere						
4. V-maskin, v-nett, konteinere						
3. Hypervisor						
2. Fysiske servere m.m.						
1. Lokaler, strøm, internett						

Streng tolkning: er f.eks. lag 3 styrt fra utlandet så er alle lagene i praksis utenfor norsk teknisk kontroll. Selv om servere fysisk sett er i Norge.

Færre eller flere sårbarheter med sky?

(Her moderne on-prem vs allmen sky)

- Lagene leverandør er ansvarlig for:
  - Lagene er mer oppdatert, sikrere konfigurert. Bedre tilgjengelig (men kun i fredstid)?
    - Monner det? Går angripere som oftest uansett til de øvre lagene?
  - Enklere å ta i bruk tilleggstjenester som MFA?
- Lagene kunden er ansvarlig for:
  - Kundene beholder mange sårbarheter som de alltid har hatt: nettverksårbarheter, tilgangskontroll, rettigheter, konfigurasjon, mm. ?
- Nye sårbarheter med sky: ny funksjonalitet + nye sammenkoblinger av ulike tjenester
- Ett samlet mål for angripere …

- *For tidlig å si hvordan det er og hvordan det utvikler seg?*

- **Avgjørende: hvordan kundene kommer til å <u>bruke</u> skytjenester**
  - Brukes tid som muligens vinnes ved tjenesteutsetting til å forbedre sikkerhets for øvrig?

Sky

og NSMs bekymringer

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

Positivt og negativt med kommersielle skytjenester

- Sky-leverandørene, gjør mye bra for sikkerheten:
  - Gode på automatisere drift og sikkerhetsarbeidet
    - Sentralisert drift
    - Standardisert: styrt av maler/templates (færre manuelle feil)
  - God kapasitet og stabilt med høy tilgjengelighet
  - Gode på sikkerhetsstandarder/rammeverk med jevnlig sikkerhetsrevisjoner
  - Mye annnet positivt sikkerhetsmessig
- Men:
  - *(neste side)*

Positivt og negativt med kommersielle skytjenest

- Skytjenester, mye positivt for sikkerhet:
  - (forrige side)
- Men gir også bekymringer:
  1) *Kundens bruk* av plattformen er ofte ved "det gamle" sikkerhetsmessig (både IaaS og SaaS eksempler)
  2) *Krever høy tillit* til leverandører og andre land
  3) Samfunnsmessig mange egg i en kurv (*noen få store leverandører*)
  4) Hva med *krisespennet*? (tilgjengelighet)
  5) Leverandør/land kan teknisk sett lese kryptert kundedata
  6) Vil påloggingen til norske virksomheter styres fra utlandet? (Identity-as-a-service, krisespennet ...)
  7) Manglende *monitorerings-evne* i annenmanns datasenter (på alle lag)

Flere sårbarheter i skyen

Sårbarhetene i skyen (kilde: US-GOV*)

1) Vanlig: feil konfigurering og svak arkitektur (mest av kunde)
   - lite oppfølging av «minste privilegium» og «forvar i dybden»
   - *lift and shift* bare viderefører gamle sårbarheter
2) Vanlig: svak aksess kontroll
   - svake passord og en-faktor autentisering
   - eldre autentiseringsprotokoller
3) Skjeldent: sårbarheter opp mot andre kunder («shared tenancy»)
   - sårbarheter i hypervisor
   - uheldig bruk av konteinere (f.eks. “serverless”)
4) Skjeldent: sårbarheter i leverandør kjeden
   - leverandørene benytter mange underleverandører innen HW og SW

* https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

Kommersielle skytjenester krever av kunde

- Høy tillit til **skyleverandør**
- Høy tillit til **landet** leverandøren har **datasentre**
- Høy tillit til **landet** datasentre **driftes fra**
- Høy tillit til **landet** leverandøren har **hovedkontoret**
- Høy tillit til internasjonale **kommunikasjonslinjer** (hele krisespennet)
- Høy tillit til **andre kunder** på samme infrastruktur

- Alt mht. konfidensialitet + integritet + tilgjengelighet

NSMs bekymring: en bekymring over to akser

Sikkert nok for en enkel virksomhet?

Sikkert nok akkumulert for hele nasjonen?

Illustrasjon: Colourbox.com

NSM er bekymret for …

Virksomhetsnivå:

- … at det er ikke er gjennomført gode **risikovurderinger**
- … at **beslutning** om tjenesteutsetting ikke er tatt av **øverste ledelse**
- … at øverste **ledelse ikke forstår** hva tjenesteutsettingen innebærer og/eller har for stor risikoappetitt

Akummulert for hele nasjonen:

- … økt **konsentrasjonsrisiko** («alle eggene i en kurv»)
- … **manglende nasjonal kontroll** på kritisk infrastruktur
- … at kritisk infrastruktur ukritisk tjenesteutsettes til **utland/risikoland**

Sikker sky og våre nasjonale verdier

- Hva må vi som nasjon tenke på?
  - **Krisespennet** (fred – krise – krig)
    - **Hvilke tjenester** *må* fungere i hele krisespennet? Hvilke kan vi klare oss uten?
    - **Kritikalitetsnivået** setter føringer.
  - **S-loven**: Vil alle kritiske tjenester bli fanget opp ? Verdikjeder, avhengighet til andre.
  - **Hvem blir Norge avhengig av**? Ok at andre kontrollerer våre nasjonale data/funksjoner vi er avhengig av?

- Regulert vs. uregulert
  - Selv om det er tillatt/lovlig, er det smart?

Illustrasjon: Colourbox.com

Misforståelser om fysisk plassering av datasenter

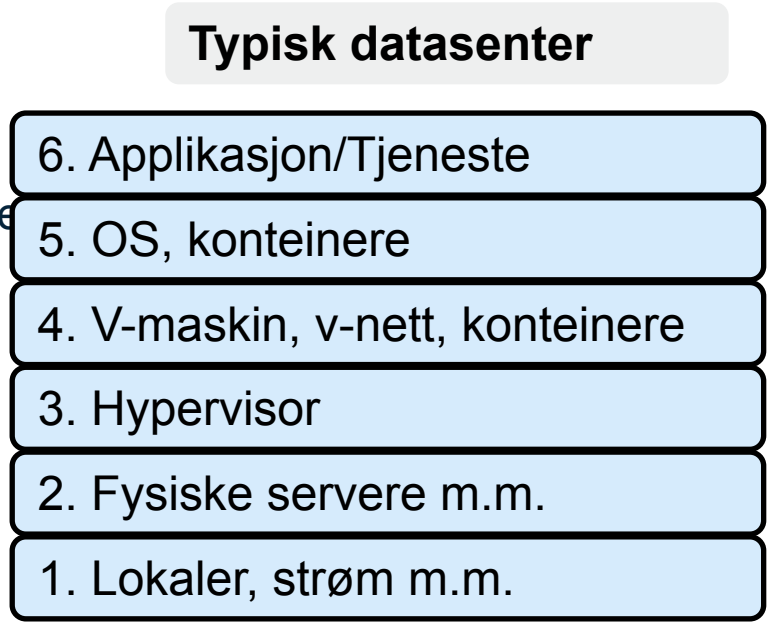
(Plassering i Norge har mindre betydning sikkerhetsmessig)

NASJONAL SIKKERHETSMYNDIGHET

John Bothner
NSM

Misforståelser om land og «regioner»

- Misforstått overfokus på hvor de fysiske maskinene er plassert (“regioner”)
- Ofte mange land å forholde seg til (forenkling, uten verdikjede-vurderinger):
  - Land A: plassering av de fysiske maskinene med alle lagene
  - Land B: leverandør(enes) hovedkontor
  - Land C: drifter hypervisorene
  - Land D: drifter de virtuelle maskiner og kontainere
  - Land E: drift av selve applikasjonen/tjenesten
  - Land F: et «security center» som bl.a. utfører sikkerhetsovervåkning
  - Land G: plassering av servere som kjører databaser med bruker identiteter (Identity as a service
  - Land H: drift av bruker identiteter (Identity as a Service)
  - Land I: supporttjenester som kan inkludere systemrettigheter
- Alle disse landene har de-fakto tilganger – jurisdiksjon (i og utenfor EU)



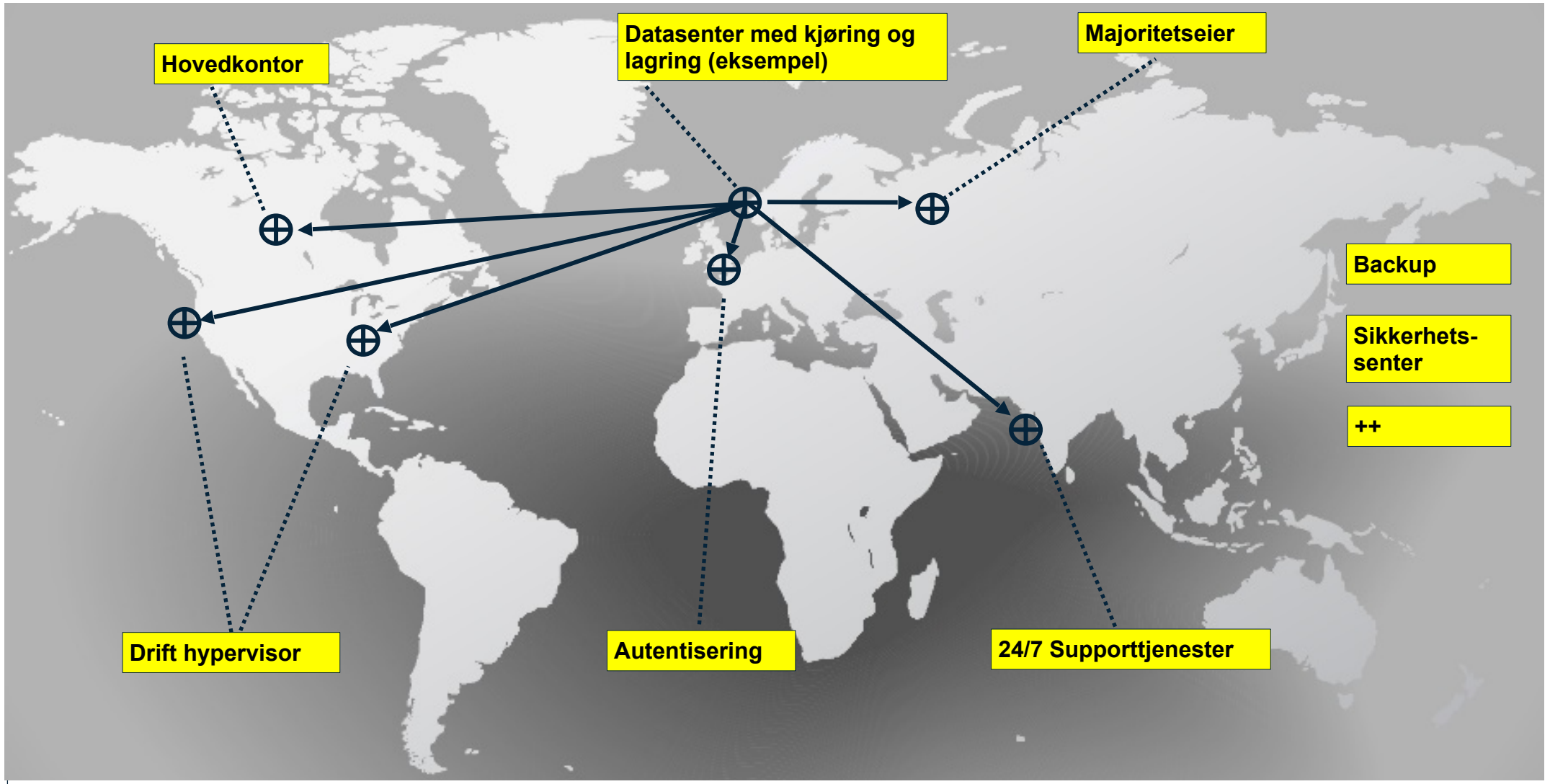
Sky og lag og land

Hvert lag (og hver celle) kan ha **ulik drift gjennomført fra ulike land**. Og ulike underleverandører.
Også store sky-leverandører kan ha fordelt dette på ulike land.
NB neppe 5x6=30 ulike land som i dette *eksemplet*, men i praksis 1-10 land som dette er fordelt på

	Generell Drift *	**Backup**	**Alt. HA site**	**Sikkerhets-Overvåkning**	**Bruker-DB: IAM**	**Utvikling**
6. Applikasjon/Tjeneste	Land?	Land?	Land?	Land?	Land?	Land?
5. OS, Konteiner	Land?	Land?	Land?	Land?	Land?	Land?
4. V-maskin/nett, konteinere	Land?	Land?	Land?	Land?	Land?	Land?
3. Hypervisor	Land?	Land?	Land?	Land?	Land?	Land?
2. Fysisk server, fys nett	Land?	Land?	Land?	Land?	Land?	Land?
1. Lokaler, strøm internett						

* For eksempel oppdateringer, sikkerhetskonfigurasjon, mm.

Land – lagring, drift, prosessering



Missforstått om “jurisdiksjon” og fysisk plassering

- Overfokus på den fysiske plasseringen til leverandørens servere
- Sikkerhetsmessig (mht. *konfidensialitet*) har fysisk plassering mindre betydning
  - Litt avhengig av hvilken type trussel man er bekymret for
  - Hvis vaktmesteren som sjekker at «lamper lyser grønt» er utro
- Mer interessant: hvilket land driftes/utvikles f.eks. hypervisorlaget fra?
  - Det landet har den reelle tekniske tilgangen til data
    - (Uansett hva slags kryptering som velges)
- I mange tilfeller mange land man nå forholde seg til mht. ulik drift
- Fysisk plassering kan derimot være viktig mht. *tilgjengelighet*

Det landet som drifter har kontroll på dine data,
eller som minimum dine metadata.
Er det i orden?

Kryptering av kundedata i skyen

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

NSM og anvendelse av krypto

- Statens ekspertorgan på bl.a. anvendelse av krypto

- Siden krigen i tett samarbeide med
  - Forskere i universitetsmiljøer
  - Produktutviklere i norsk industri
  - Brukere i ulike deler av staten (mil/siv)
  - Allierte nasjoner

- NSM fortsetter med fremtidige utfordringer f.eks.
  - Kvanteresistent krypto

Hvor er kryptering relevant? Ulike typer kryptering

- Kryptering av data under transport over f.eks. internett
  - Fagsjargong: "*data in transit*"
  - Hvor: Mellom kundens og skyleverandørens datasentre
  - Dette er standard og i bruk av tilnærmet alle (variabel kvalitet, vurder flere lag kryptering)

- Kryptering av data på disk hos leverandør *(hovedfokus i de neste sidene)*
  - Fagsjargong: "*data at rest*"
  - Hvor: Disker i skyleverandørens datasenter
  - Mange misforstår den sikkerhetsmessige effekten

Skyleverandører kan lese kundekryptert data på disk
- uansett hvordan man velger å kryptere

Svært mange tror det motsatte, det er feil.

- Dette gjelder også ved bruk av kundegenerert nøkkel

NSMs konklusjon først:

- Det er ingen store tekniske hinder for at skyleverandører kan lese lagret kundekrypter kundedata
- Uansett hvordan krypteringen utføres

En ubeleilig sannhet (An inconvenient truth)

Politiske, juridiske og forretningsmessige aspekter er ikke drøftet i denne delen av presentasjonen.
Fokus er på hva som er teknologisk mulig.

(Manglende symmetri er med vilje)

Sky og hvem som har reell kontroll

Skyleverandørs datasenter

- **5. Applikasjon/Tjeneste**
- **4. Gjeste-OS, konteinere**
- **3. V-maskin, v-nett, konteinere**
- **2. Hypervisor**
- **1. Fysiske servere m.m.**

- Kundens data
- Kryptonøkler (“data-at-rest”)

Kundes datasenter (“on-prem” del)

- **5. Applikasjon/Tjeneste**
- **4. Gjeste-OS, konteinere**
- **3. V-maskin, v-nett, konteinere**
- **2. Hypervisor**
- **1. Fysiske servere m.m.**

Kontrollert av skyleverandør

Kontrollert av kunde

Kryptert data i skyen kan leses av leverandøren

- Kundenøkkel sendes fra kunde til sky, pakkes gjerne ut i lag 3-5
- Den som drifter/utvikler hypervisor-laget er teknisk «gud».
- Nøkler som benyttes i lag 3-5 er lesbare fra hypervisor
- Da teknisk lett å lese data, selv med kundegenerert nøkkel
- Hypervisor driftes/utvikles oftest av noen utenfor EU (men spør!)

- Tillegg: «alle» IT-produktene i figuren inneholder sårbarheter

Forenklet modell sky-plattformer

Spesialtilfelle 1: “Data in use” type kryptering

- Kunden får dedikert plass (”enklave») i deler av prosessor og minne på server
  - For utpakking av kundegenerert nøkkel
  - Kryptografisk sikret
- Mest kjente eksempel: Intel SGX (aka. «Confidential Computing»)
- Gir bedre sikkerhet, men ...
- ... gir *ikke* full kundekontroll, som mange hadde håpet
  - Sikkerhetsforskere har påpekt sårbarheter
  - Andre sårbarheter kan/vil avdekkes i fremtiden
- Mister noen av fordelen med virtualisering og sky:
  - må ha kundededikert server uten sømløs flytting av virtuelle maskiner?

Spesialtilfelle 2: kun kryptert backup i sky, ikke prosessering i sky

- Antar man kun lagrer kryptert data sky, ikke prosesser det i leverandør-datasenter
  - Typisk anvendelse: sky-backup
  - Krypteringen/dekryptering foregår utelukkende i kundens on-prem datasenter
  - Leverandør får aldri tak i nøkkel !
  - Men kan kopiere kryptert data
- 20 år senere:
  - Krypto ikke lenger state-of-the-art
  - Krypterte kopier kan nå leses
  - Hypotetisk annen stat foretar data mining på norske innbyggere/kunder, 20 år gammel data
    - Har det en verdi? Er det greit?

Oppsummering om krypto

Kryptering er ingen reel barriere mot andre lands lovgivning.
Uansett tekniske valg.

- Slik avlesning av kryptert kundedata er teknisk mulig
- Det er ikke krevende teknisk sett
- Vanskelig, kanskje umulig, å detektere

Viktig for noen, uviktig for mange andre?

Risikoredusjon - missforståelser

- “Men, vi reduserer risiko uansett med kryptering?”
- Tja.

- Scenarier (data-at-rest):
  - Vurderer leverandør fra land X, bekymret for land X etterretning
    - Schrems 2 - scenariet
    - Kryptering gir uvesentlig risikoreduksjon, ref forrige plansjer
  - Vurderer leverandør fra land X, bekymret for land Y etterretning
    - Kryptering gir absolutt risikoreduksjon

Metadata ifm sky

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

Metadata skytjenester

- Metadata:
  - data som ikke direkte er i kundens dokumenter
  - data om transaksjonene, ikke selve innholdet
  - neppe kryptert

- Er det i orden at annet land har teknisk adgang til all denne informasjonen?

Metadata skytjenester, f eks SaaS-møteromstjenester

- Tjenester fra utlandet, underlagt annen lands lovgivning
- Påstand/Spekulasjon: neppe mye direkte «avlytting»
- Men hva med metadata om møtene:
  - Hvem møter hvem
  - Møte agenda
  - Sakspapirer, referater
  - Presentasjoner
- Er det i orden at annet land har lett teknisk adgang til all denne informasjonen?
  - Er dette et problem eller er er det ikke noe viktig norske virksomheter bruker disse tjenestene til?

Øke sikkerheten i sky leveransene

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

Råd for bedre sikkerhet ved kjøp og bruk av tjenester

Mange råd ...

Her følger noen forskjellige gode råd:

- NOR GOV – NSM
- UK GOV – NCSA
- US GOV – NSA
- CSA – Cloud Security Alliance

NSMs 5 råd ifm. tjenesteutsetting

5 overordnede råd ved tjenesteutsetting

www.nsm.no/sky

1) Ha oversikt/kontroll over hele livsløpet til tjenesteutsettingen
2) Ha riktig kompetanse (bestillerkompetanse)
3) Ha gode risikovurderinger (for å fatte riktig beslutning)
4) Sett krav til IKT-tjenesten og leverandøren
5) Sørg for høyt forankret beslutning

➔ Husk! Virksomheten må sørge for at sikkerhetsnivået opprettholdes eller forbedres i forbindelse med tjenesteutsetting.

NSMs “Ofte stilte spørsmål om sky og tjenesteutsetting»

- 25 spørsmål (med svar) ofte rettet til NSM
- Om sky og tjenesteutsetting

www.nsm.no/sky

US GOV - Mitigating cloud vulnerabilities

- USA myndigheters anbefalinger for å oppdage og fjerne *sårbarheter*
- Bra, kort og rett på poengene!
- Deler opp sårbarheter i 4 kategorier/grupper
  - feil konfigurering
  - svak aksess kontroll
  - sårbarheter opp mot andre kunder
  - leverandør kjede
- NB Fokus på US kunders behov

https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

UK GOV - Implementing the Cloud Security Principles

- Britiske myndigheters sikkerhetsanbefalinger
- 14 prinsipper for sky-sikkerhet, en fin sjekkliste for kunder

- https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

Hva kan man da gjøre?

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

Alternativer

- Virksomheten løse dette alene?
  - Velg allmenn/privat sky og akseptere at annet lands myndigheter teknisk sett kan lese virksomhetsdata
  - Varianter av «on prem», alle lag i Norge
- Eller, er dette for stort for en virksomhet å løse alene?
  - nasjonal samarbeid («nasjonal-sky»?)
  - nordisk/europeisk samarbeid (felles utvikling – men nasjonal drift?), GAIA-X?
- Desentraliserte datasentere – 5G Edge (Se «Risiko 2021» fra NSM)
- «Homomorfisk kryptering»
  - Store begrensninger og foreløpig ikke praktisk tilgjengelig
- NB «private cloud» har som oftest utenlandsk drift av hypervisorlaget (tenk konfidensialitet)
  - Men kan være bra mht tilgjengelighet

Avslutting

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
NSM

Oppsummering

1. Fordeler og ulemper med skytjenester
   - Tillitssak!
2. Vurder ulike tiltak for risikoreduksjon
3. Overfokus på den fysiske plassering av datasenter(ene)
   - Spør og hvem som drifter de ulike lagene
4. Leverandør (og annet land) kan lese data uansett type krypto

Takk for meg!

Mer informasjon om “sky” og sikkerhet:

- www.nsm.no/sky
- www.nsm.no/grunnprinsipper-ikt

Nytt eKurs!
«NSMs grunnprinsipper for IKT-sikkerhet».
Nå også som eLæringskurs!