Nasjonalt cybersikkerhetssenter

NORMEN 3. Februar 2021

NASJONAL
SIKKERHETSMYNDIGHET

Harald Næss,
John Bothner

Innhold

- Kort om Nasjonalt cybersikkerhetssenter
- Situasjonsbilde - cyberområdet
- Helhetlig Digitalt Risikobilde 2020
- NSM Grunnprinsipper for IKT-sikkerhet
- Litt om SKY

NCSC - Nasjonalt cybersikkerhetssenter

- NCSC skal bidra til å beskytte grunnleggende nasjonale funksjoner, offentlig forvaltning og næringsliv mot digitale angrep.
- NCSC legger til rette for samarbeid i offentlig sektor og med næringsliv, akademia og internasjonale partnere.
- Senteret er en del av NSM og skal være en driver for digital sikkerhet i Norge.

NASJONALT
CYBERSIKKERHETSSENTER

Utvikling og tilgjengeliggjøring av tiltak og anbefalinger. Rådgiving

Nasjonal responsfunksjon med deteksjon og hendelseshåndtering

Nasjonale tekniske sikkerhetstjenester

Samlet nasjonal kompetanse der ulike aktører samarbeider basert på felles risikobilde og situasjonsforståelse i felles lokaler og over nett

Varslingssystem for digital infrastruktur (VDI)

- Samarbeid mellom private og offentlige virksomheter og de hemmelige tjenestene
- Deltagelse i VDI er frivillig, basert på samarbeidsavtale
- Operativ (24x7) drift i over 20 år
- Har inspirert andre nasjonale CERTs, NATO NCIRC, m.fl.
- Open-source og egenutviklet teknologi
- I kontinuerlig utvikling for å møte IKT-risikobildet

Det digitale risikobildet

Digitale hendelser mot norske mål

- Viktige samfunnsfunksjoner utsatt
- Spenner bredt i omfang og alvorlighetsgrad

Operasjoner blir mer komplekse og sofistikerte

- Hendelseshåndtering er tid- og ressurskrevende
- Aktører har mye ressurser

COVID-19 har forsterket digitale sårbarheter

- COVID-19 tematikk utnyttes i svindel- og phishingforsøk
- Vist viktigheten av forebygging og tiltak – i forkant

Anvendte angreps-metoder:

- Kartlegging og forberedelser skjer ofte i lang tid på forhånd
- Det benyttes skadevare som er tilgjengelig på Internett
- E-post og passord benyttes ofte som inngangsvektor
- Uvitende tredjeparter benyttes som plattform for angrep
- Utdaterte systemer som er eksponert mot Internett er sårbare
- Løsepengevirus og DDoS trusler er motivert av økonomisk vinning
- Svindel ofte relatert til falske nettsider

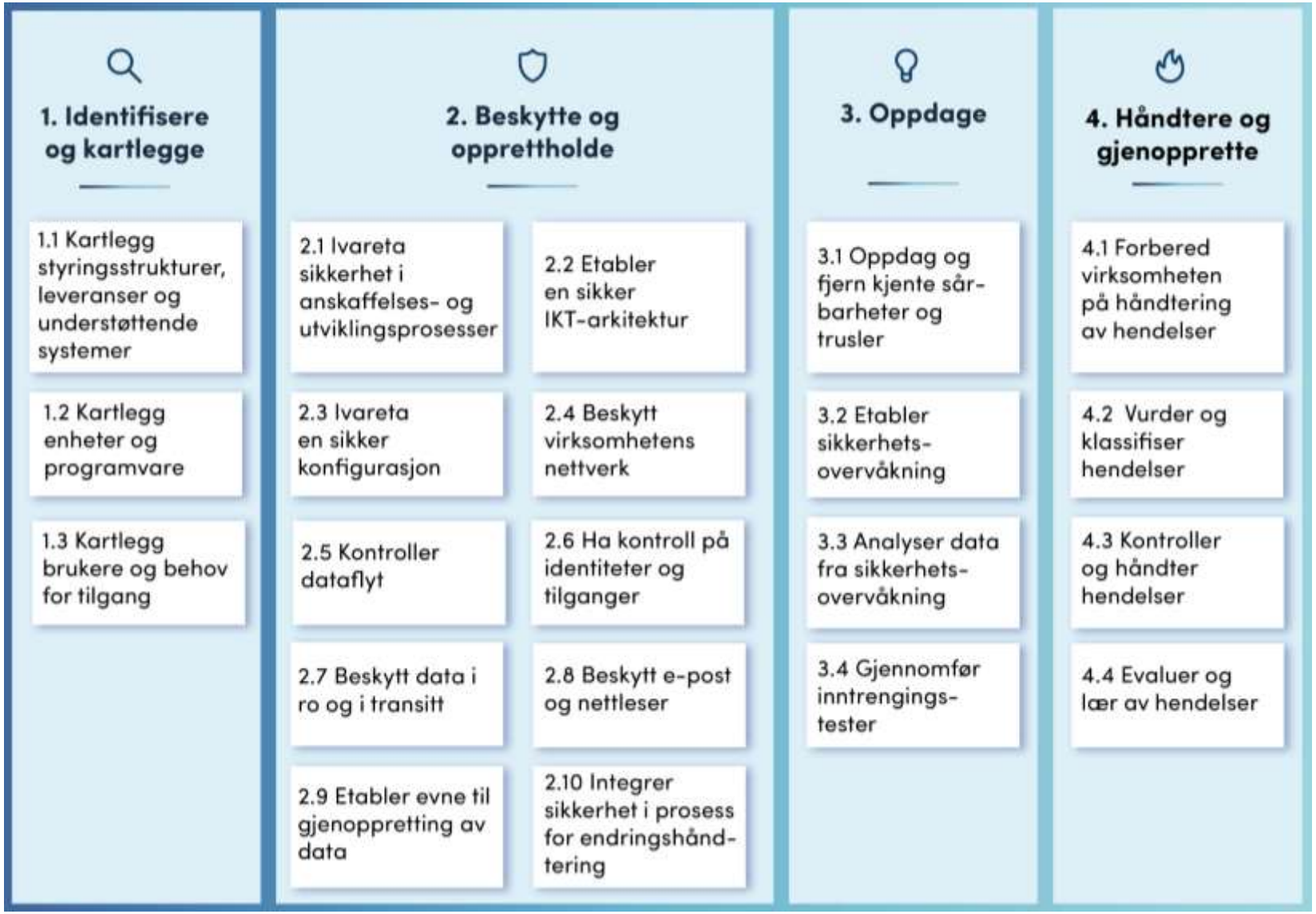
NSM Grunnprinsipper – John tar det herfra ☺

Generelt om grunnprinsippene

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner

NSMs grunnprinsipper for IKT-sikkerhet



Målgrupper for dokumentet

- Generelt: virksomheter i Norge
  - Offentlig og privat virksomhet
  - Herunder kritisk infrastruktur
    - Viktig ifm. Corona!

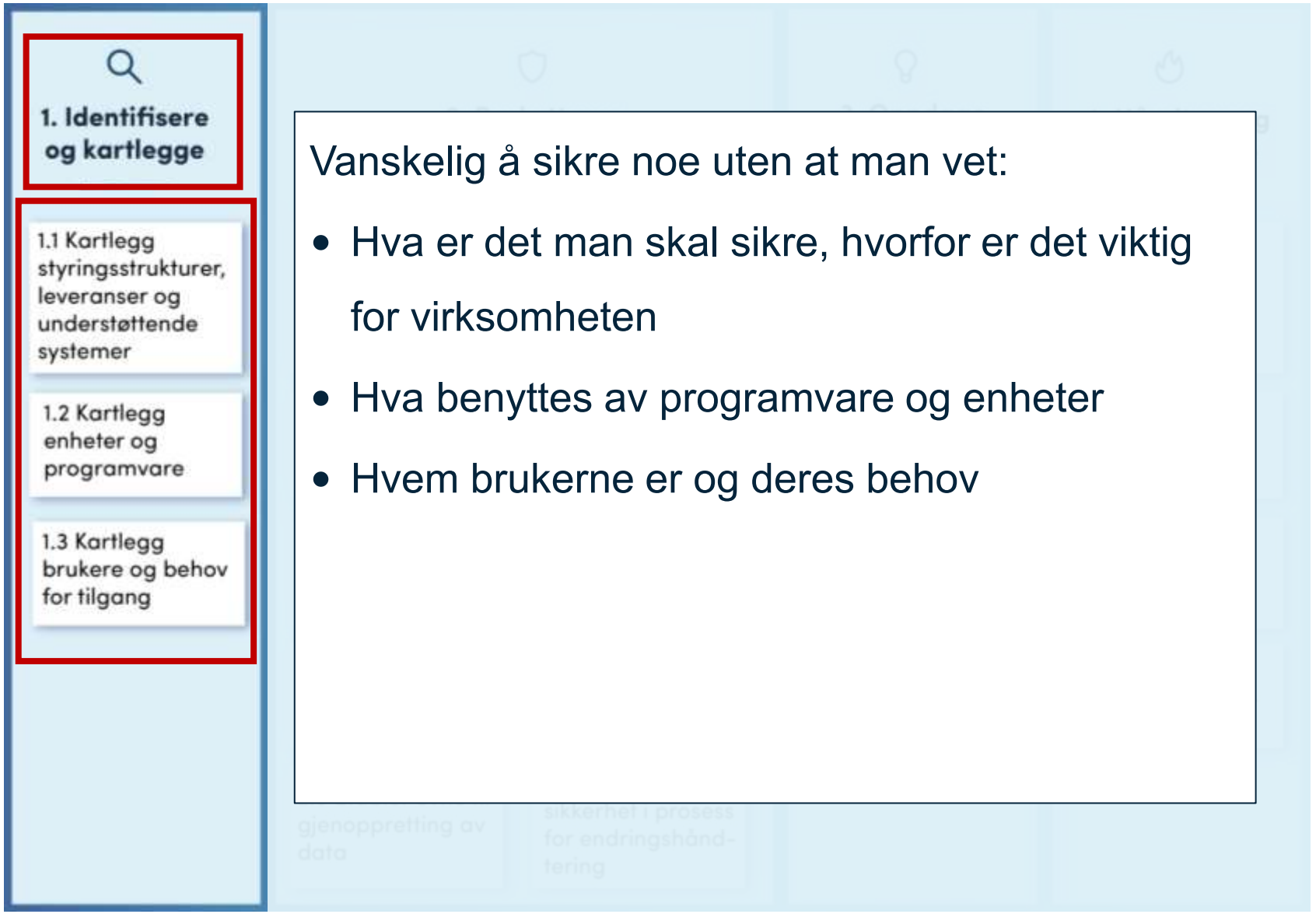
- Roller i virksomheten
  - IT-ledere, Sikkerhetsledere, IT-arkitekter, Driftsledelse

- Antagelse: virksomhet med en IT-avdeling

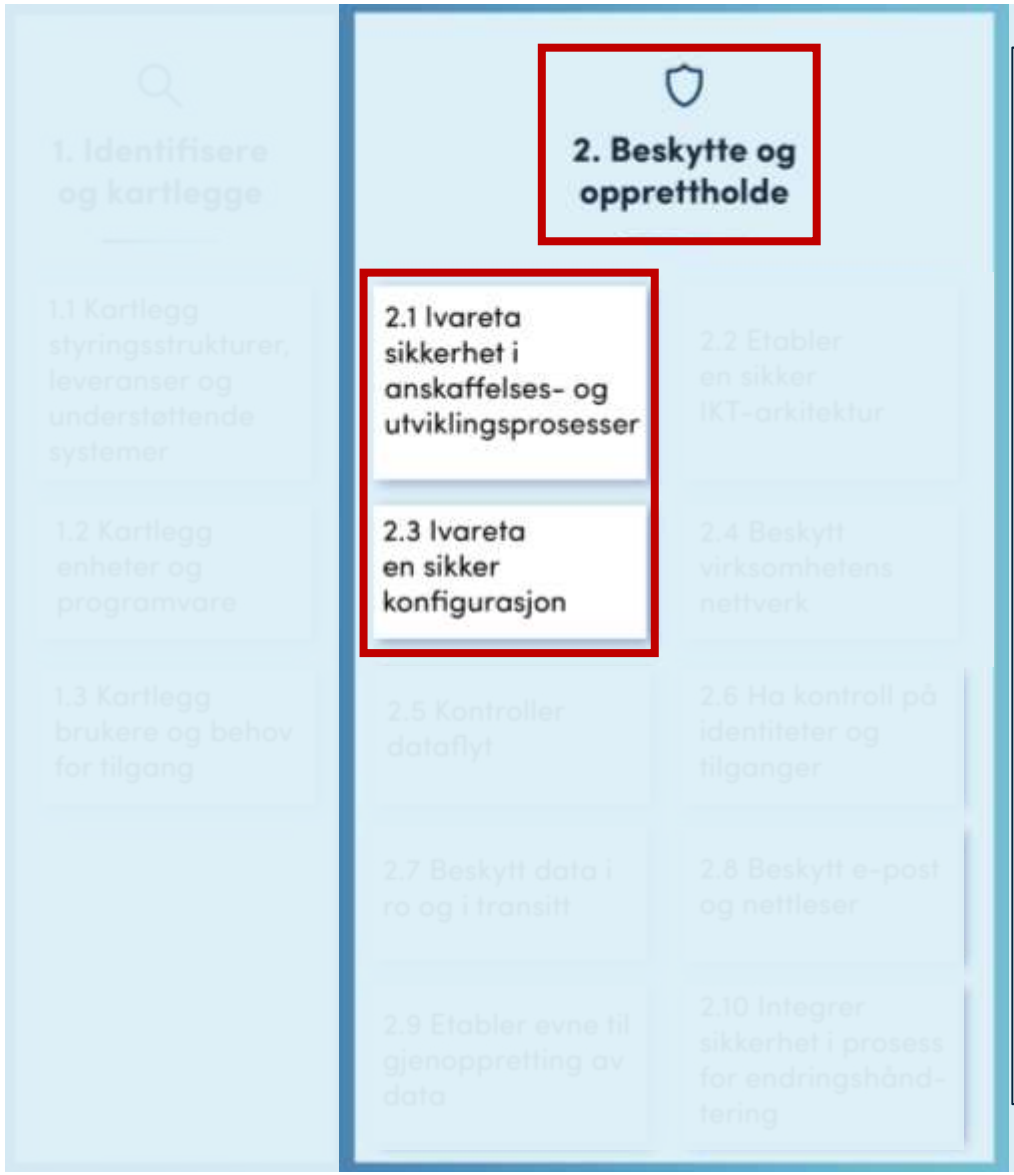
Kritisk infrastruktur

Kraftforsyning	Telekom
Vann og avløp	Forsvar
Helse	Forsynings-sikkerhet
Finansielle tjenester	Transport
Satellittbaserte tjenester	Viktig offentlig administrasjon

Kategori 1 – Identifisere og kartlegge

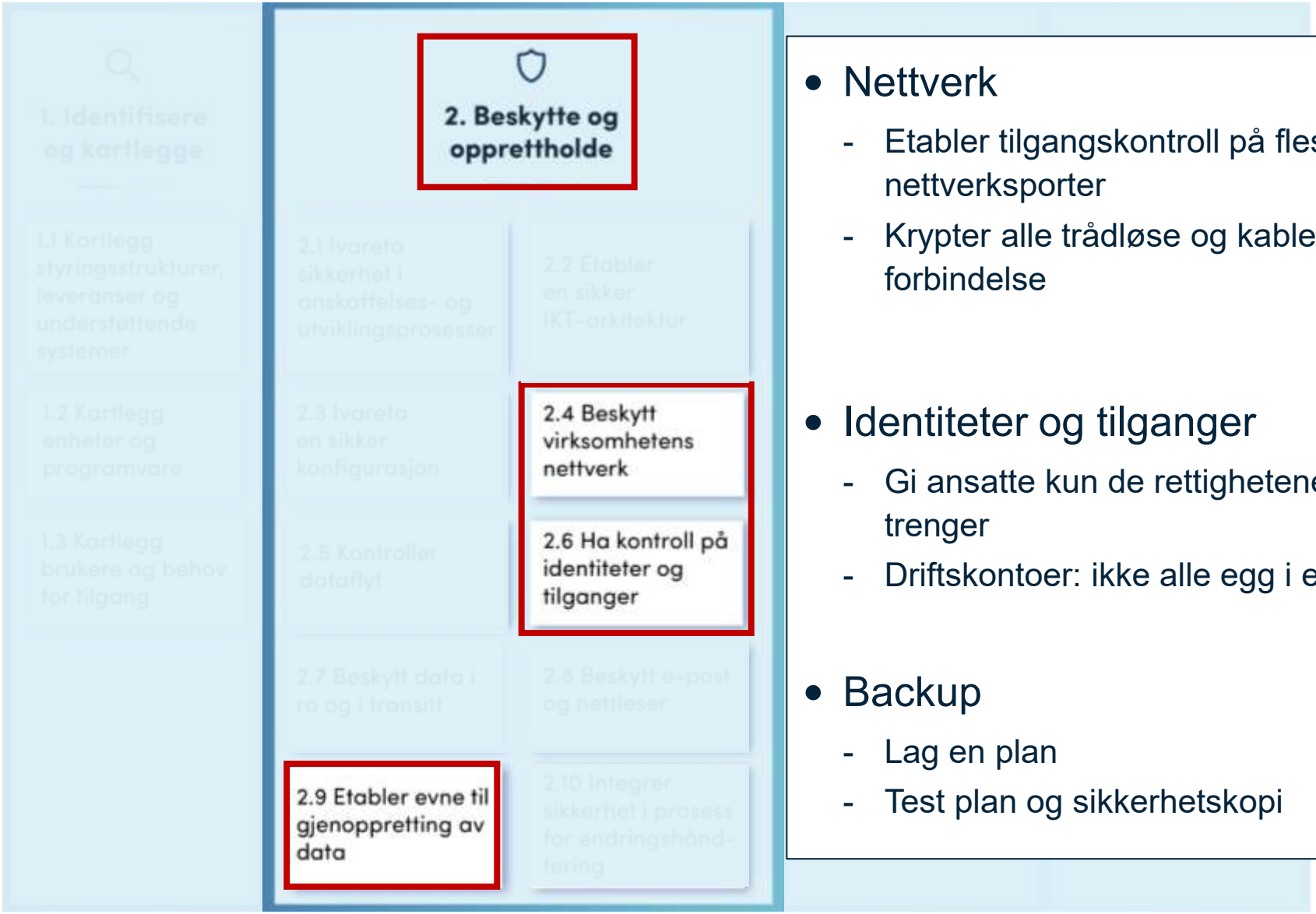


Kategori 2 – Beskytte og opprettholde



- Sikkert kjøp
  - Sikkerhet angår ikke bare sikkerhetsprodukter!
  - Fas ut eldre IKT-produkter
  - Virtualisering og “sky”
- Sikkerhetskonfigurasjon
  - sentralt styrt regime for sikkerhetsoppdatering
  - klienter slik at kun kjent programvare kjører på dem

Kategori 2 – Beskytte og opprettholde (forts.)



- Nettverk
  - Etabler tilgangskontroll på flest mulige nettverksporter
  - Krypter alle trådløse og kablede forbindelse
- Identiteter og tilganger
  - Gi ansatte kun de rettighetene de trenger
  - Driftskontoer: ikke alle egg i en kurv …
- Backup
  - Lag en plan
  - Test plan og sikkerhetskopi

Kategori 3 – Oppdage

- Oppdage trusler og sårbarheter
  - Jevnlig sårbarhetskartlegging, helst automatiserte verktøy
- Etabler sikkerhetsovervåkning
  - Beslutt hvilke data som er sikkerhetsrelevant
  - Verifiser at innsamling fungerer
  - Analyser data fra sikkerhetsovervåkning
- Inntrengningstester

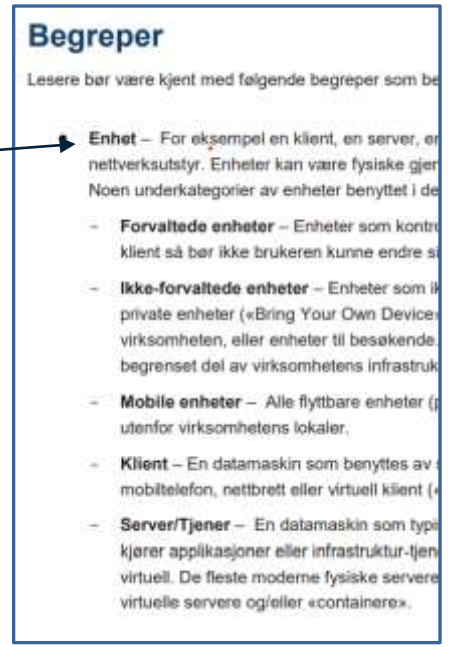
Kategori 4 - Håndtere og gjenopprette

- Forbered virksomheten på håndtering av hendelser
  - Plan!
  - Øve!
- Håndter hendelser når de inntreffer
- Lær av hendelsen

Hvordan bruke grunnprinsippene og sky/virtualisering

- Grunnprinsippene gjelder
  - For alle programmer, tjenester og enheter
  - Uansett hvem som kjører og drifter det

- Begreper i grunnprinsippene
  - *«Enhet»* kan gjelde både *fysiske OG virtuelle* klienter, servere og nettverk
  - *«Enhet» k*an gjelde både lokalt hos virksomheten OG hos en sky-leverandør



- Gjør praktiske vurderinger i sikkerhetsarbeidet, f.eks.
  - IaaS: maler/templates, ikke enkelt (virtuelle) enheter.
  - SaaS: fokuser på virksomhetens bruk (f.eks. tilgangskontrollen)

GRUNNPRINSIPPER FOR IKT-SIKKERHET

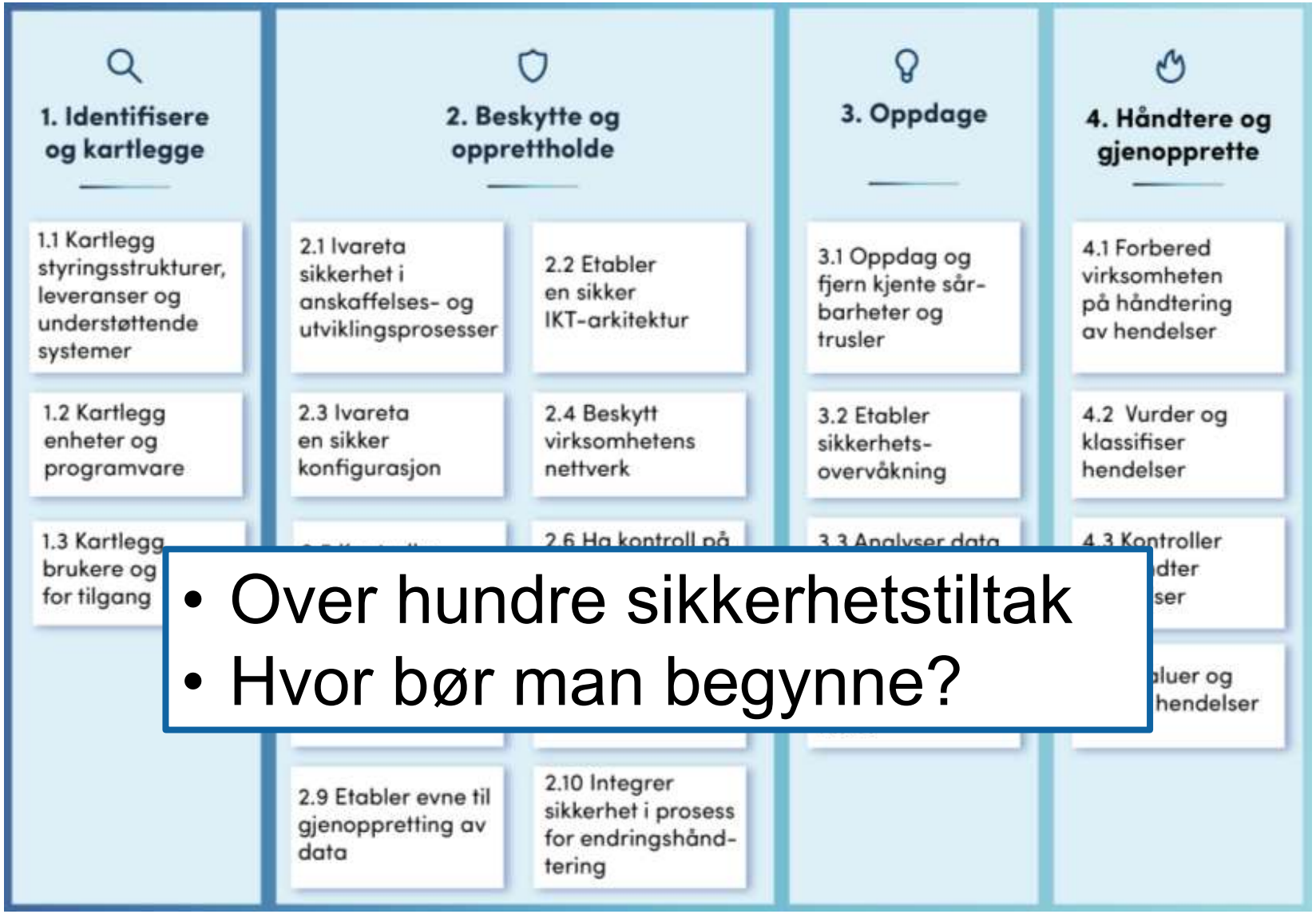
Viktige sikkerhetstiltak

John Bothner

Denne delen av presentasjonen kan sees i sin helhet på
https://www.youtube.com/watch?v=rSyJeYiZTdk

NASJONAL
SIKKERHETSMYNDIGHET

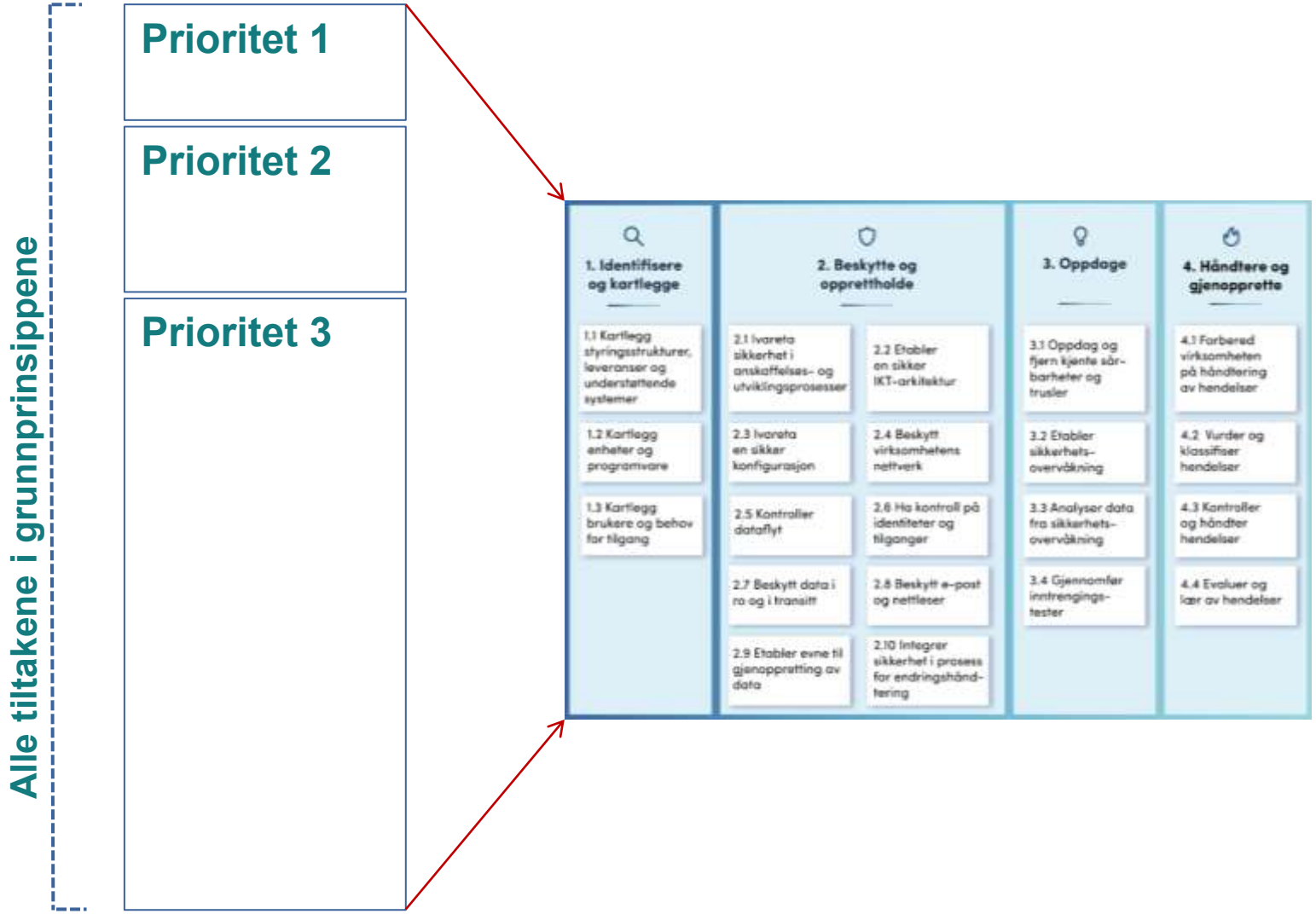
NSMs grunnprinsipper for IKT-sikkerhet



Prioritering av sikkerhetstiltak

Anbefalt rekkefølge ved implementering av tiltakene i grunnprinsippene:

1. Prioritetsgruppe 1
2. Prioritetsgruppe 2
3. Prioritetsgruppe 3



Se regneark på www.nsm.no

	A	B	C	D	E	F	G	H	I	J	K
1	**NSMs grunnprinsipper for IKT-sikkerhet v2.0**										
2											
3	**Nr.**	**Kategori**	**GP. ID**	**Grunnprinsipp**	**Spesifisering**	**Tiltak ID**	**Tiltaksoverskrift**	**Tiltaksbeskrivelse**	**Prioritet**	**A**	**B**
4	1	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.1	Identifiser virksomhetens strategi og prioriterte mål	**Identifiser virksomhetens strategi og prioriterte mål**, samt regelverk, bransjenormer og avtaler som kan ha innvirkning på sikring av informasjonssystemer.	3	A.18.1.1	A.18.
5	2	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.2	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.	**Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.** Dette inkluderer normalt **a)** policyer fra ledelsen, **b)** ledelsesstruktur med veldefinert ansvar og ansvarslinjer, **c)** prosesser for risikostyring (se 1.1.3) **d)** fastsatte toleransegrenser for risiko (se 1.1.4), **e)** tilføring av tilstrekkelige ressurser og fagkompetanse for å støtte ledelsen i arbeidet. **f)** Etabler strukturer og prosesser for sikkerhetsstyring dersom dette mangler. Sørg for at det tilpasses virksomheten og er en inkludert del av virksomhetsstyringen. Se «Utdypende informasjon» for ytterligere informasjon.	3	A.5.1.1	A.6.
								Identifiser virksomhetens prosesser for risikostyring knyttet til IKT. Dette inkluderer normalt **a)**			

Tiltak ID

Prioritetegruppe nr

Prioritet 1: tiltak som stopper mest

Formålet med disse 15 tiltakene er:

- Hjelpe virksomheter å komme i gang
- Peke på tiltak som er kritisk for de fleste virksomhetene
  - Basert på NSMs observasjoner i norske virksomheter
  - Basert på flere tiår med utvikling av sikkerhetstiltak
  - Andre lands myndigheter har råd som er grovt sett tilsvarende

15 viktige tiltak (Gruppe 1): **Tiltak 1-5**

1. **1.2.3** Kartlegg enheter i bruk i virksomheten.
2. **1.2.4** Kartlegg programvare i bruk i virksomheten.
3. **2.1.2** Kjøp moderne og oppdatert maskin- og programvare.
4. **2.1.9** Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
5. **2.2.3** Del opp virksomhetens nettverk etter virksomhetens risikoprofil.

- Merknad til 1.2.3: Se tiltaket i sammenheng med 1.2.1 og 1.2.2.
- Merknad til 1.2.4: Se tiltaket i sammenheng med 1.2.1 og 1.2.2.
- Merknad til 2.1.2: Fokuser i første omgang på klientene.
- Merknad til 2.2.3: Bør sees i sammenheng med 2.5.1.

15 viktige tiltak (gruppe 1): **Tiltak 6-10**

6. **2.3.1** Etabler et sentralt styrt regime for sikkerhetsoppdatering.
7. **2.3.2** Konfigurer klienter slik at kun kjent programvare kjører på dem.
8. **2.3.3** Deaktiver unødvendig funksjonalitet.
9. **2.3.7** Endre alle standardpassord på IKT-produktene før produksjonssetting.
10. **2.6.4** Minimer rettigheter til sluttbrukere og spesialbrukere.

- Merknad til 2.3.2: Dette må tilpasses klient-operativsystem og applikasjoner.
- Merknad til 2.3.3: Fokuser i første omgang på klientene.
- Merknad til 2.3.7: Og vurder generelt passordkvaliteten i virksomheten, se 2.6.3.e.
- Merknad til 2.3.7: Og vurder å ta i bruk multi-faktor autentisering, se 2.6.7.

15 viktige tiltak (gruppe 1): **Tiltak 11-15**

11. **2.6.5** Minimer rettigheter på drifts-kontoer.
12. **2.9.1** Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.
13. **3.2.3** Avgjør hvilke deler av IKT-systemet som skal overvåkes.
14. **3.2.4** Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
15. **4.1.1** Etabler et planverk for hendelseshåndtering.

- Merknad til 2.9.1: Test sikkerhetskopier regelmessig ref. 2.9.3.
- Merknad til 3.2.3: Se tiltaket i sammenheng med bl.a. 3.2.4, 3.3.1 og 3.3.3.
- Merknad til 3.2.4: Se tiltaket i sammenheng med bl.a. 3.2.3, 3.3.1 og 3.3.3.
- Merknad til 4.1.1: Som minimum planlegg roller og ansvar ref 4.1.3. Og øv på dette, ref. 4.1.6.

Vanlige myter innen IKT-sikkerhet

NASJONAL SIKKERHETSMYNDIGHET

John Bothner
Senioringeniør NSM

Utvalgte myter innen (teknisk) IKT-sikkerhet

Vanlige misforståelser, dvs dette er feil:

- **Myte 1:** Det er trygt på innsiden av brannmuren
- **Myte 2:** Antiskadevare/antivirus holder mot skadevare
- **Myte 3:** Vi har ingen sårbarheter hvis vi er god på sikkerhetsoppdatering
- **Myte 4:** Kryptert data i skyen kan ikke leses av leverandøren

Myte 1: Det er trygt på innsiden av virksomhetens brannmur

- Angrep kan også komme fra innsiden, f.eks.
  - Kompromitterte mobile klienter
  - Eksterne tjenesteleverandører kan ha blitt kompromittert
  - Ansatte (inkl. IT-avdelingen) kan gjøre feil
  - Ansatte («insidere») kan med vilje kompromittere systemet

- Skillet mellom «innsiden» og «utsiden» viskes gradvis ut
  - Stadig mer mobilitet, inkludert bruk av hjemmekontor
  - Stadig mer bruk av eksterne tjenester

Myte 1: Tiltak

- Tilgangskontroll på flest mulige nettverksporter
  - Virtuelle, trådløse og kablede porter

- Som minimum ha en variant av soneinndeling
  - Vurder også nyere løsninger innen f.eks.
    - «Mikrosegmentering», «Zero Trust», eller «Software Defined Networking»

- Les prinsippene om nettverk, dataflyt og arkitektur (kategori 2)

Myte 2: Antivirus / antimalware er nok for å stoppe skadevare

- NB mange leverandører og produkter innen denne produktfamilien
- Antimalware stopper en del angrep men blir en sovepute for mange kunder
- Selv moderne antimalware fjerner ikke sårbarheter
- For eksempel sårbarheter innen
  - Manglende sikkerhetsherding
  - Manglende rettighetsstyring (masse kjempesårbarheter)
  - Manglende autentisering av nettverkstrafikk
  - For enkle passord
  - Manglende sikkerhetsoppdatering

Myte 2: Tiltak

- Fortsett med sikkerhetsarbeidet
- Fjern sårbarheter
  - På klienter, servere og nettverk

- Les prinsippene om å beskytte IKT-systemet (kategori 2)

Myte 3: Vi har ingen sårbarheter hvis vi er god på å sikkerhetsoppdatering

- CVS er ikke synonymt med sårbarhet
- Sårbarheter er så mye mer enn bare manglende sikkerhetsoppdatering (og zero-days)

Myte 3: Tiltak

- Fjern sårbarheter innen (som myte nr 2)
  - Klientkonfigurasjon
  - Serverkonfigurasjon
  - Nettverkskonfigurasjon
- Mer konkrete sårbarheter, eksempelvis:
  - Manglende sikkerhetsherding
  - Manglende rettighetsstyring (masse kjempesårbarheter)
  - Manglende autentisering av nettverkstrafikk
  - For enkle passord
  - OG: Manglende sikkerhetsoppdatering

Myte 4: Kryptert data i skyen kan ikke leses av leverandøren

- Dette er feil. Det er en vanlig misforståelse

- Senere i presentasjonen

Sky

og NSMs bekymringer

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
Senioringeniør NSM

Kjetil Nilsen
Kjetil Nilsen, direktør, Nasjonal sikkerhetsmyndighet

Innlegg

Bekymret over at tjenester settes ut

Vi er bekymret for datasikkerheten når virksomheter setter ut tjenestene. Datalagring og -prosessering utenfor landets grense særlig aktsomhet.

DN+ 1 min Publisert: 19.05.17 – 20.48 Oppdatert: 3 år siden

Nasjonal sikkerhetsmyndighet (NSM) er bekymret for at tjenesteutsetting gjøres uten at virksomheter vurderer sikke godt nok (Foto: Istockphoto/Getty Images)

Saken handler om: Nasjonal sikkerhetsmyndighet om datasikkerheten når tjenester settes bort

Tjenesteutsetting, eller «outsourcing», skal gi bedre driftstjenester forc

Nasjonal sikkerhetsmyndighet: Trygt å bruke utenlandske skytjenester

TEMAER: IT Konkurranseutsetting Sikkerhet Veiledning

Nasjonal sikkerhetsmyndighet, her ved sin direktør Kjetil Nilsen, har utarbeidet en v vurdering av IKT-sikkerheten ved tjenesteutsetting (foto: Cicilie Andersen).

PUBLISERT AV: LENNART HOVLAND 6. FEBRUAR 2019

SEND ARTIKKELEN PÅ E-POST SKRIV UT ARTIKKELEN

– Det er trygt å bruke utenlandske skytjenester. Det kan være be håndtere det selv in house. Alle virksomheter må imidlertid vær bevisst hva de tjenesteutsetter og hvilken risiko det innebærer. K kommer fra Nasjonal sikkerhetsmyndighet i en kommentar til A reportasje om en svenske rapport som skremte de offentlige innl vårt naboland.

Anbud365 bragte forleden nyheten om at da en «tung», offentlig eksp Sverige la fram sin rapport om sky-tjenester gikk alarmen i svenske of innkjøpsmiljø. Gruppen slo fast at ved bruk av utenlandske, f.eks. ame skytjenester, er det ingen garanti for at sikkerhetsbelagte opplysninge hendene på uvedkommende.

Det var en rapport fra eSam som vekket offentlige oppdragsgiver melder upphandling24.se. eSam er et samarbeid mellom 23 myndigh Kommuner och Landsting med formål å fremme og påskynde digitalis

HELHETLIG DIGITALT RISIKOBILDE 2020

NSM er bekymret for outsourcing og økende bruk av nettsky – men skytjenester kan også gi økt sikkerhet

– Skytjenester levert fra og med infrastruktur i Norge vil være en god start, ifølge sikkerhetsmyndighetene.

Innkjøp av skytjenester må vurderes opp mot behovet for nasjonal kontroll og beredskap, sier avdelingsdirektør Bente Hoff i NSM.

MARIUS JØRGENRUD SKYTJENESTER 25. SEP. 2020 - 07:47

Denne Ekstra-saken kan leses gratis av alle du deler den med.

Nasjonal sikkerhetsmyndighet (NSM) legger fredag fram sin årlige rapport om det digitale risikobildet for 2020. Det er en rapport hvor økende bruk av skytjenester og outsourcing til

Noen sikkerhetsmessige fordeler med "allmenn sky"

- Leverandørene er ofte gode på å automatisere IKT- drift og -sikkerhet.
- Leverandørene besitter ofte mye ekspertkompetanse
- De er gode på kapasitetsplanlegging mht datakomponenter, linjekapasitet og strøm.
- Fysisk sikkerhet er ofte god
- De leverer ofte mer stabile, tilgjengelig og oppgraderte tjenester enn virksomheten selv klarer
- God oppfølging av sikkerhetsstandarder/rammeverk, jevnlig sikkerhetsrevisjoner
- Men …

Noen utfordringer med «allmenn sky»

- *Kundens bruk* av er ofte ved “det gamle” sikkerhetsmessig (IaaS/SaaS eksempler)
- *Krever høy tillit* til leverandører og andre land (neste side)
- Samfunnsmessig mange egg i en kurv (*noen få store leverandører*)
- Hva med *krisespennet*? (tilgjengelighet)
- Leverandør/land kan teknisk sett lese kryptert kundedata
- Vil påloggingen til norske virksomheter styres fra utlandet? (Identity-as-a-service, krisespennet ...)

Kommersielle skytjenester krever av kunde

- Høy tillit til **skyleverandør** og kanskje **andre kunder** på samme infrastruktur
- Høy tillit til **landet** leverandøren har **datasentre**
- Høy tillit til **land(ene)** datasentre **driftes fra** (ulike lag kan driftes fra ulike land)
- Høy tillit til **landet** leverandøren har **hovedkontoret**
- Høy tillit til internasjonale **kommunikasjonslinjer** (hele krisespennet)

- Alt mht. konfidensialitet + integritet + tilgjengelighet
- I tillegg mange “vanlige” problemstillingene innen IKT-sikkerhet

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

Sky og sikkerhetsansvar

NSM og tjenesteutsetting (sky)

www.nsm.no/sky

Kryptering av kundedata i skyen

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
Senioringeniør NSM

Påstand: skyleverandører kan ikke lese kundekryptert data

Tillegspåstand: Og i alle fall ikke hvis man benytter kundegenerert nøkkel?

- Dette er en utbredt missforståelse og er feil.

- 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)

- Ref. VP Al Gore

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, kontainere**
- **3. V-maskin, v-nett, kontainere**
- **2. Hypervisor**
- **1. Fysiske servere m.m.**

Kontrollert av skyleverandør

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

Kundes datasenter (“on-prem” del)

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

Kontrollert av kunde

Kryptert data i skyen kan leses av leverandøren

- Skyleverandører tilbyr kryptering
  - Beskytter *ikke* mot alle ansatte hos skyleverandøren
- Teknisk mulig å lese data
  - Selv med kundegenerert nøkkel
  - Ikke spesielt krevende teknisk
- Kundenøkkel sendes fra kunde til sky, må pakkes ut i prosessor/minne
  - Kan da leses av f eks hypervisor
- Hypervisor driftes fra utlandet selv om lag 1 ofte i norge
- Tillegg: «alle» IT-produktene inneholder sårbarheter

Forenklet modell sky-plattformer

5. Applikasjon/Tjeneste

4. Gjeste-OS, kontainere

3. V-maskin, v-nett, kontainere

2. Hypervisor

1. Fysiske servere m.m.

Oppsummering om krypto

- Ikke ha noen illusjoner om at det er uoverstigelige tekniske hindre for å lese dine krypterte data
  - uansett hva du gjør av tekniske valg.

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

Tiltak

- *Problem*: skyleverandør og annen stat kan teknisk sett lese data om mine kunder/innbyggere, uansett type kryptering

- *Verdivurdering*: er dette et problem for «min» virksomhet, «min» tjeneste, «mine» brukere?

- Mange virksomheter:
  - Kanskje det ikke er så nøye?

- Noen virksomheter:
  - Må ha alle lag under nasjonal kontroll?
    - Fysisk plassering OG drift (av alle lag)

Se www.nsm.no/sky

Takk for oss!

NSMs nettsider:

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

eLæringskurs i grunnprinsippene

- Kommer i løpet av vinteren/våren
- Følg med på
- https://nsm.no/kurs-og-konferanser/nsm-kurssenter/