GRUNNPRINSIPPER FOR IKT-SIKKERHET

2020-11

NASJONAL
SIKKERHETSMYNDIGHET

John Bothner
Senioringeniør NSM

Agenda

- Prioriterte sikkerhetstiltak
- Utvalgte “myter” innen IKT-sikkerhet

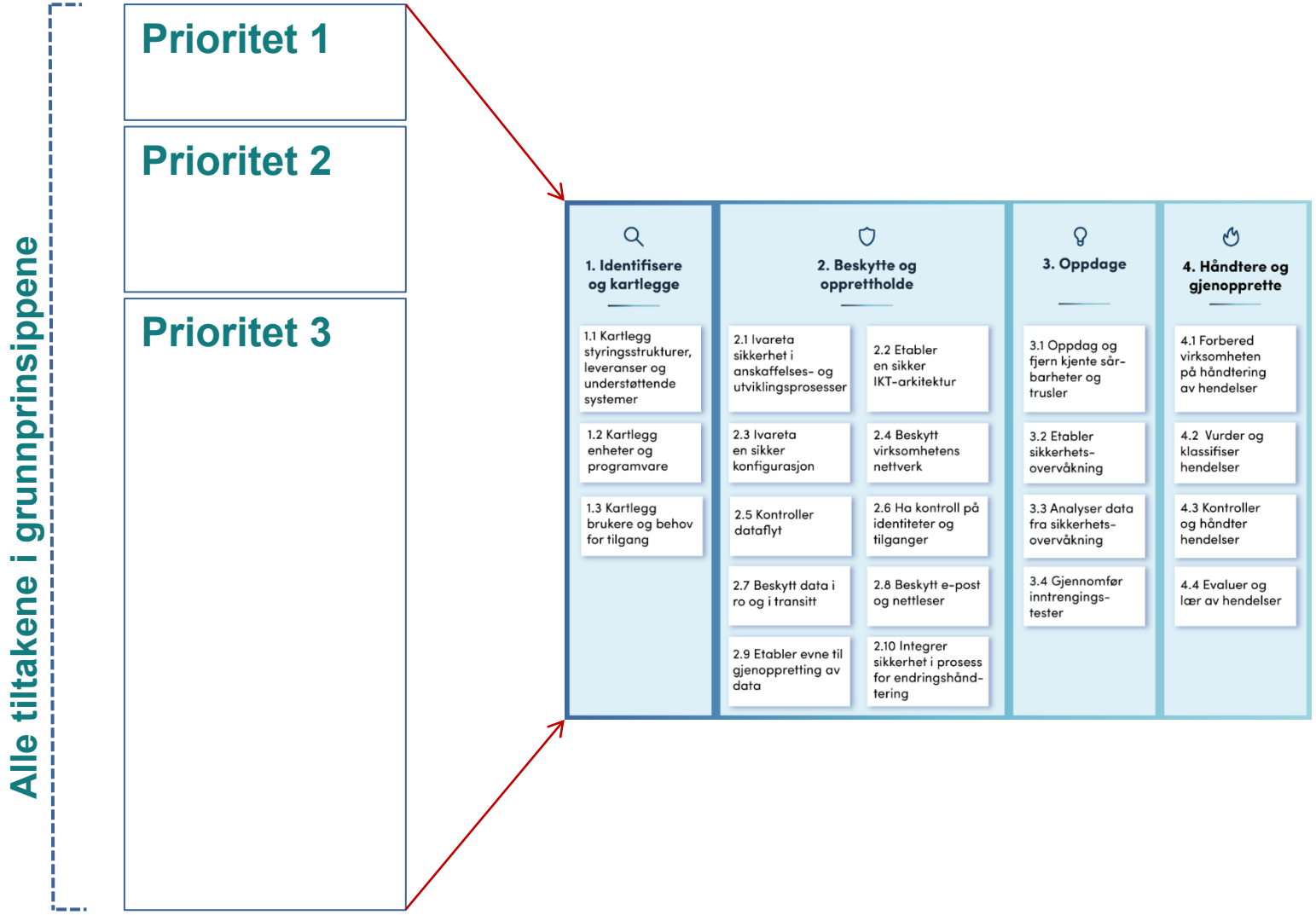
Viktige sikkerhetstiltak

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

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

Utvalgte myter innen (teknisk) IKT-sikkerhet

Vanlige misforståelser:

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

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: Kryptert data i skyen kan ikke leses av leverandøren

- Sky leverandører tilbyr kryptering
  - Beskytter godt mot flertall av driftere og mot dataangrep generelt
  - Beskytter *ikke* mot sky leverandøren som organisasjon
- Teknisk mulig å lese data
  - Selv med kundegenerert nøkkel
  - Ikke spesielt krevende teknisk
- NB Vi har ingen indikasjon på at dette har skjedd
- MEN: enkelte bør være klar over at dette er teknisk mulig

Forenklet modell sky-plattformer

5. Applikasjon/Tjeneste

4. Gjeste-OS, kontainere

3. V-maskin, v-nett, kontainere

2. Hypervisor

1. Fysiske servere m.m.

Myte 3: Tiltak

Verdivurdering

- De fleste virksomheter:
  - Kanskje det ikke er så nøye?
- Noen virksomheter:
  - Må ha alle lag under nasjonal kontroll?
    - Fysisk plassering OG drift

Se www.nsm.no/sky

Myte 4: Vi har ingen sårbarheter hvis vi er god på å patche

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

Myte 4: 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

Avslutning

Takk for meg!

Mer informasjon:

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