Skyte fra hofta eller systematisk risikostyring?

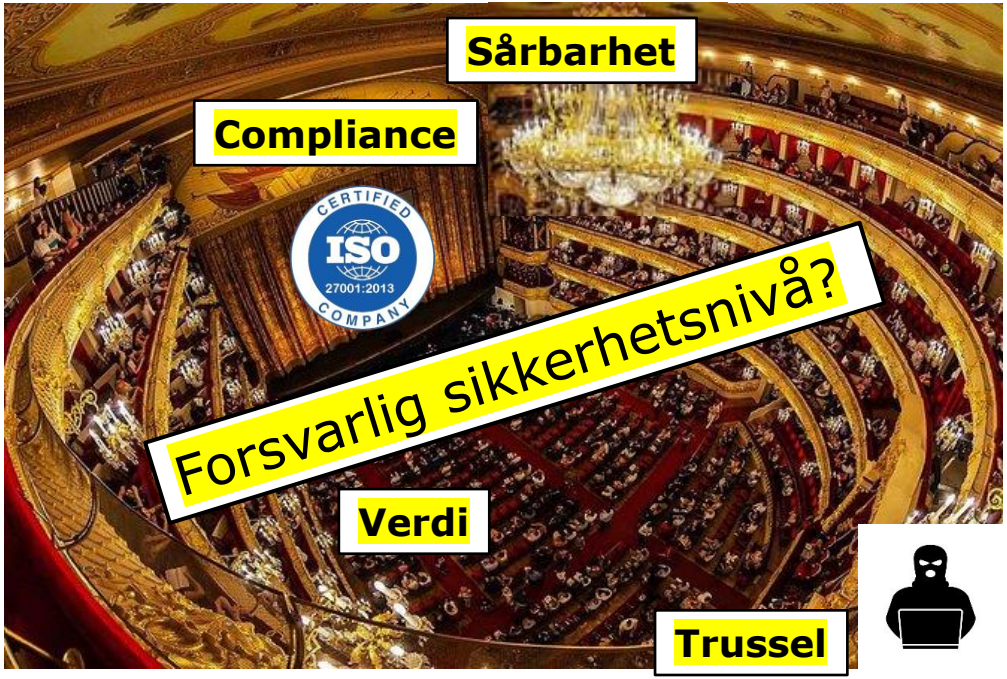
Simen Bakke, Politiets IT-enhet

Senior informasjonssikkerhetsrådgiver

Sikkerhetsfestivalen

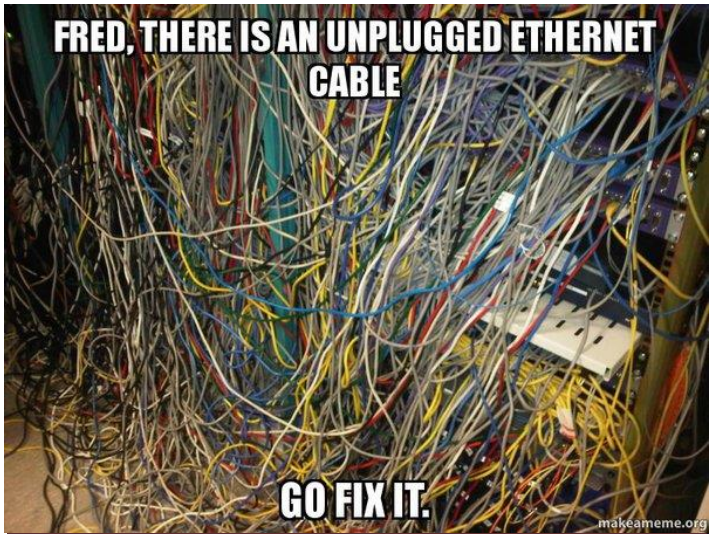
Lillehammer, 29.8.2023

Hvorfor er risikostyring og -vurderinger viktig?



Så, hva mener vi med risiko?

- *Risiko* omhandler **fremtidige** *uønskede* hendelser
  - Innebærer **usikkerhet** (noen ganger betydelig!)
- Som *kan* medføre **konsekvenser**
  - Enten **tilsiktet handling (trussel)**
  - Eller en **utilsiktet hendelse («uhell»)**
- I *konteksten* **informasjons-/cybersikkerhet**
  - Påvirker **konfidensialitet**, **integritet** og **tilgjengelighet**

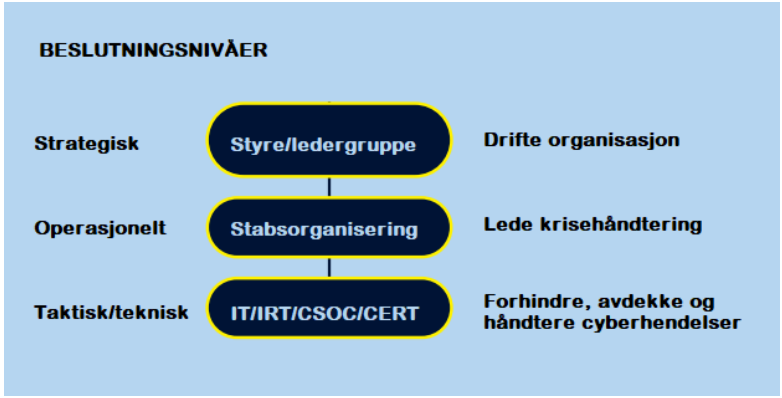


Risikostyring og -vurderinger

Risikovurderinger: Enkeltstående vurderinger

Risikostyring: Kontinuerlig og systematisk

- **Metodisk** og **systematisk** fremgangsmåte
- For å gi presis og relevant **beslutningsstøtte**
- Kan benyttes både **i og utenfor hendelser**
- Til **sentrale interessenter** i organisasjonen
- For å tilegne risiko- og **situasjonsforståelse**
- Slik at **risikoreduserende tiltak** kan iverksettes



Forskjellen på «å skyte fra hofta» og risikostyring

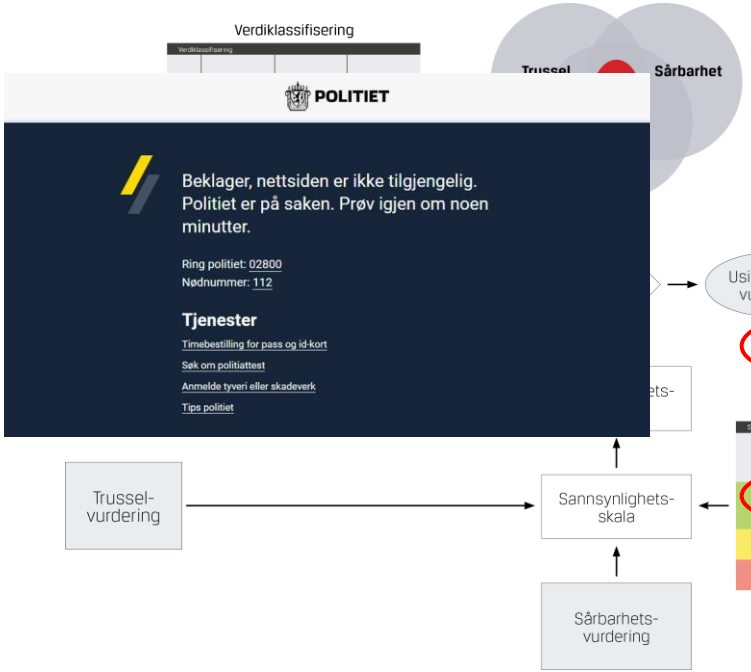
Å «skyte fra hofta»:

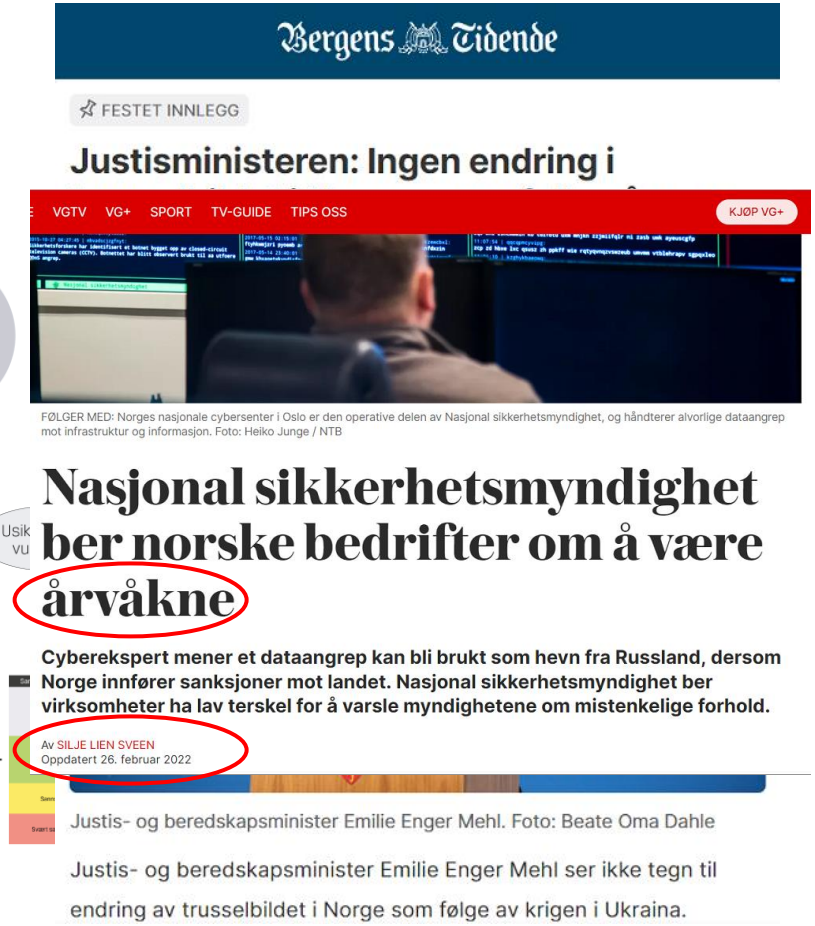
- **Mangelfullt** faktagrunnlag
- **Subjektive** vurderinger av risiko
- **Ingen** vurdering av usikkerhet
- Uklart **hvem som beslutter** hva og når
- **Ikke basert på** eksplisitte kriterier
- **Fravær** av risikoreduserende tiltak

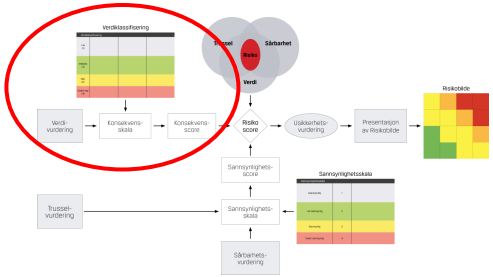
Systematisk risikostyring:

- Basert på **dokumentert** faktagrunnlag
- **Vurderinger** av risiko (V, T, S) og **usikkerhet** (!)
- Tydeliggjorte **kriterier** for vurderingene
- **Klare** mandater og ansvarsforhold
- **Beslutninger** med dokumentert **risikoaksept**
- **Plan** for implementering av **tiltak**

Rammeverk for risikostyring

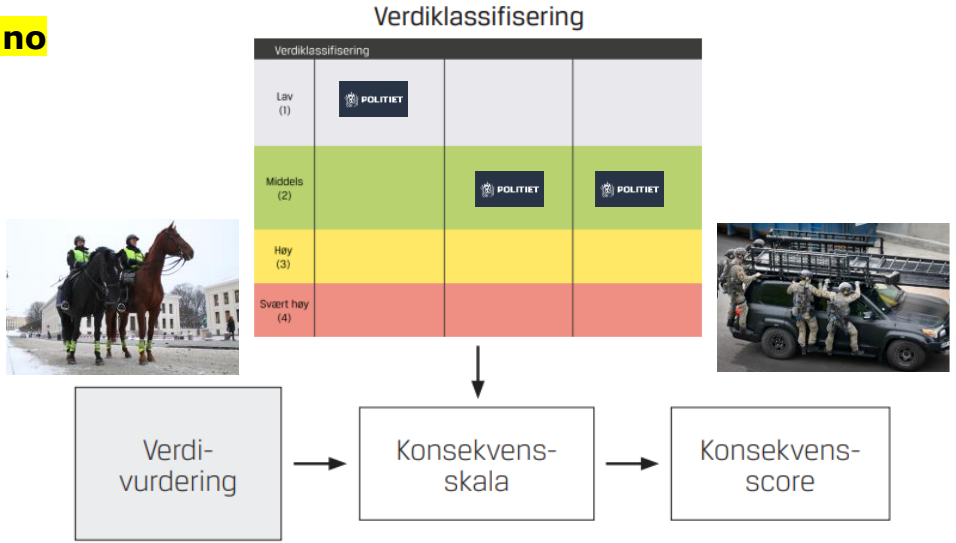


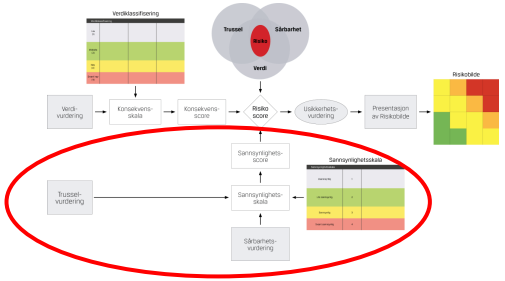




Verdi- og konsekvensvurdering

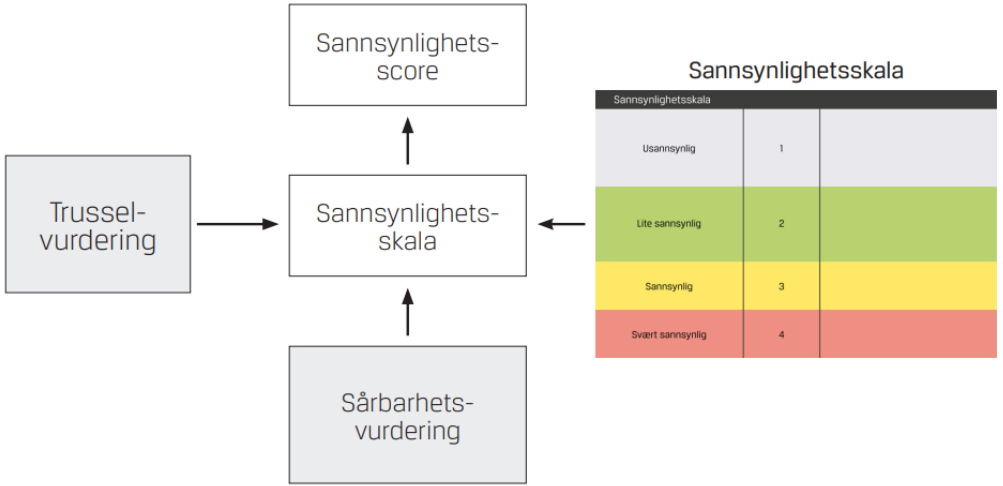
- Vurdering av **skadepotensialet** til verdien (K, I, T)
- Verdiklasser utløser **sikrings-** og **behandlingskrav**
- Eksempel: **Tjenestenektangrep** mot **Politiet.no**

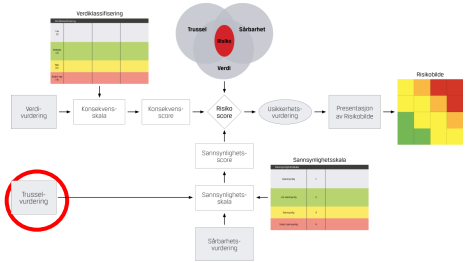




Trussel, sårbarhet og sannsynlighet

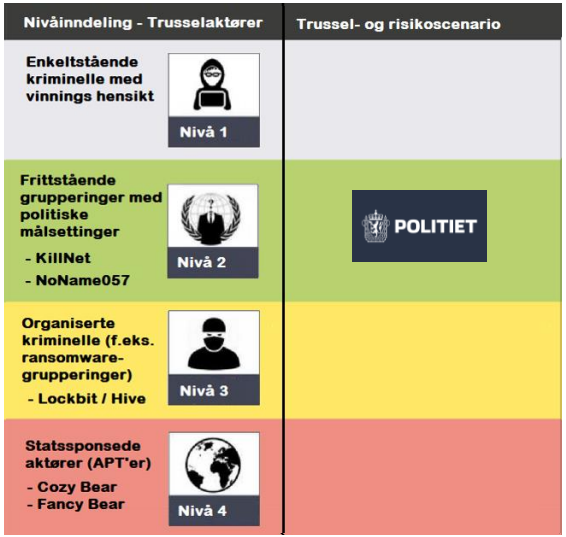
- 1: **Trusselvurdering** – trusselaktører og -scenarioer
- 2: **Sårbarhetsvurdering** – sårbarhetsanalyse og kontroll
- 3: Definere **sannsynlighet** for valgt scenario

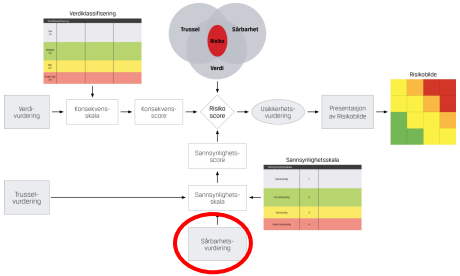




Definere trusselnivå

- Hvilke aktører har **intensjon** (vilje)?
- Hvilke aktører har **kapasitet** (evne)?
- Eksempel: **Tjenestenektangrep** mot **Politiet.no**





Definere sårbarhetsnivå

- Hvor god **kontroll** har vi på **sårbarhetstilstanden**?
- Hvor **sårbare** er vi i lys av definert **trusselaktør** og **-scenario**?
- Eksempel: **Tjenestenektangrep** mot **Politiet.no**

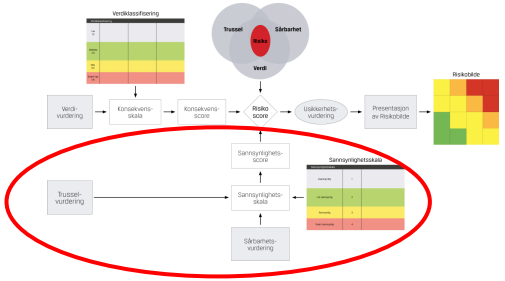
OWASP TOP10

NIST

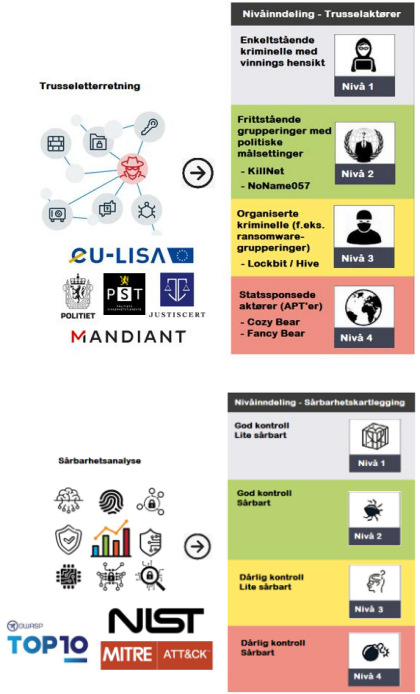
MITRE ATT&CK

Sårbarhetsanalyse

Nivåinndeling - Sårbarhetskartlegging		System/plattform/tjeneste/app
God kontroll Lite sårbart	Nivå 1	
God kontroll Sårbart	Nivå 2	POLITIET
Dårlig kontroll Lite sårbart	Nivå 3	
Dårlig kontroll Sårbart	Nivå 4	

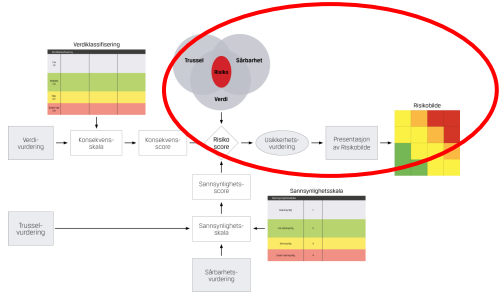


Definere sannsynlighetsnivå

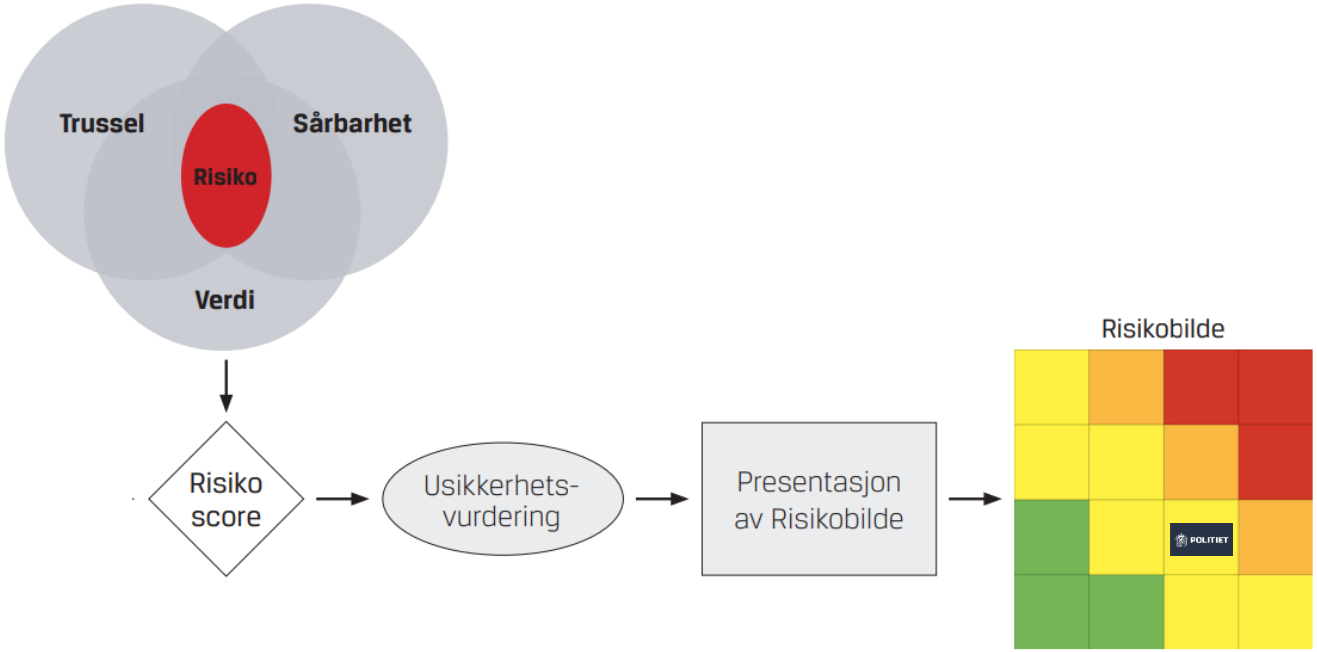


Sannsynlighetsskala		
Usannsynlig	1	
Lite sannsynlig	2	
Sannsynlig	3	POLITIET
Svært sannsynlig	4	

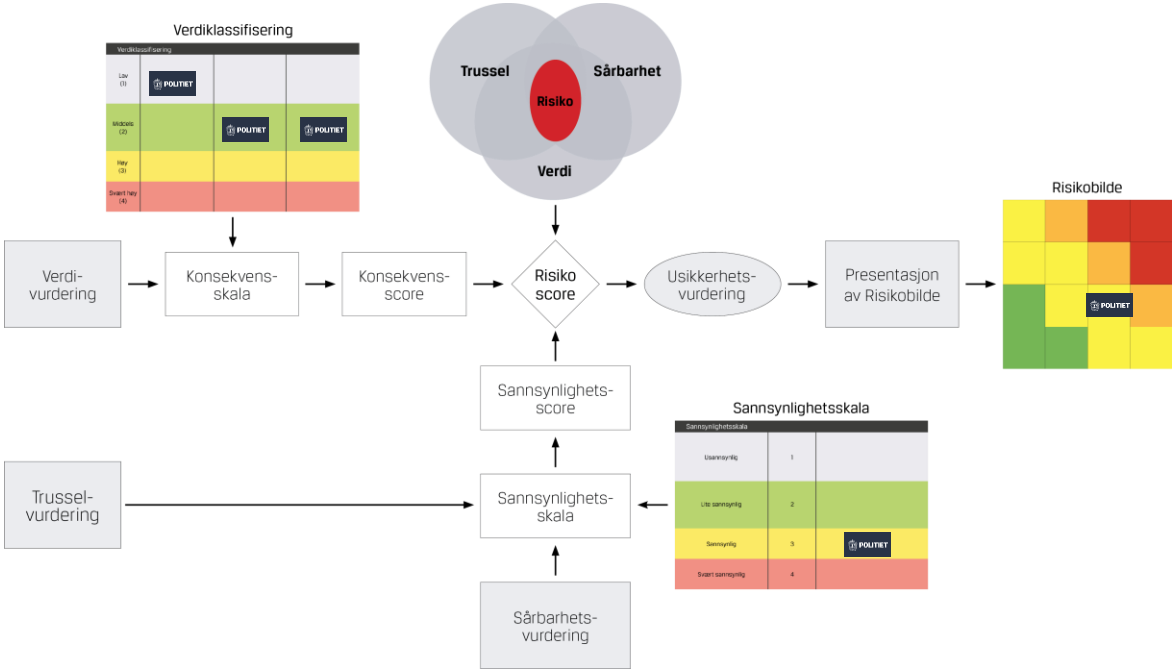
27.08.2023 Side 11



Risiko og usikkerhetsvurdering



Rammeverk for risikostyring



Trussel- og risikoscenarioer:

- R1: Russiske «hacktivister» utfører tjenestenektangrep mot Politiet.no slik at websiden blir utilgjengelig i **kortere tid** (0 – 2t)
- R2: Russiske «hacktivister» utfører tjenestenektangrep mot Politiet.no slik at websiden blir utilgjengelig i **lengre tid** (2t +)

- Men hva er egentlig **trusselaktørens mål**?
  - **Konsekvensene** av tjenestenektangrep:
    - For den enkelte virksomhet?
    - For alle berørte virksomheter?
    - For staten eller samfunnet?
    - Som del av en påvirkningsoperasjon?

- Alle **virksomheter** kan være en **liten brikke** i et større spill!
- Klarer vi å se hva som **egentlig** foregår ute på det store **spillbrettet**?


DN

Innlegg

Innlegg: Tjenestenektangrep kan være del av en påvirkningsoperasjon

Tjenestenektangrep mot sentrale norske samfunnsinstitusjoner bør ikke kun betraktes som it-tekniske hendelser – det er også en del av et pågående stormaktsspill mellom stater.

1 MIN | PUBLISERT: 07.07.22 – 16.43 | OPPDATERT: ETT ÅR SIDEN

Manipulerte bilder av utenriksministeren Anniken Huitfeldt og Natos generalsekretær Jens Stoltenberg ble lagt ut som del av cyberoperasjonen til den russiske tilknyttede grupperingen Killnet. Skjermdump hentet fra Telegram. (Foto: Beate Oma Dahle/NTB)

Flere sentrale norske samfunnsinstitusjoner som Arbeidstilsynet, Altinn,