SINTEF

# MÅLING AV CYBERSIKKERHET KREVER GODE SKALAER – HVORDAN LYKKES?

Ketil Stølen

# Motivasjon

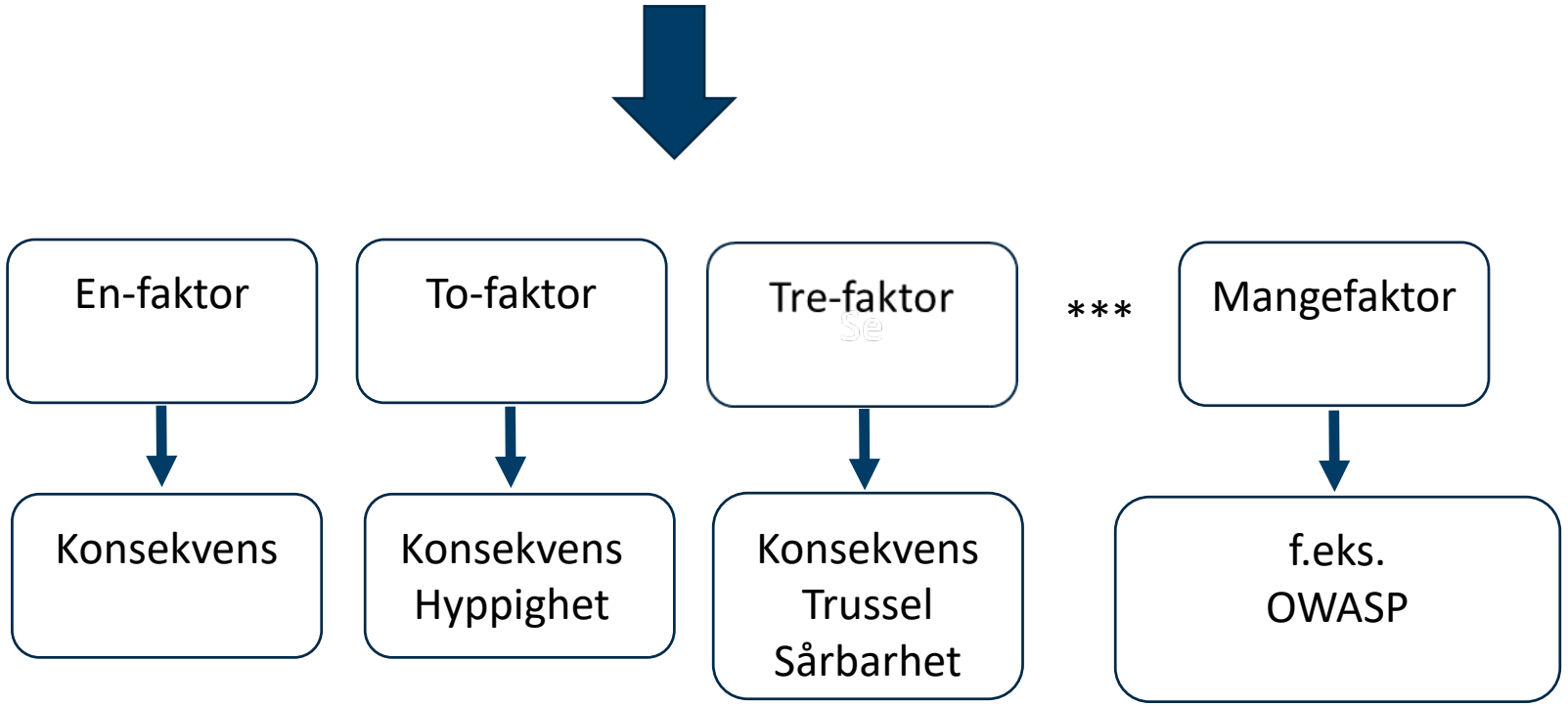
- Mål og estimater er viktige beslutningsgrunnlag for cybersikkerhet
- Det krever gode og velegnede skalaer

**MEN**

- Hva vil det si at en skala er god eller velegnet?
- Hvordan velge og/eller definere slike skalaer?

SIKKERHETSRISIKO er et mål på alvorlighet av et negativt eller skadelig potensielt scenario

**ISO/IEC 27005** — Information technology — Security techniques — **Information security risk management**



Uansett, hvilke og hvor mange faktorer:

**Gode og velegnede skalaer er en forutsetning for et godt resultat!**

# Er dette en god skala?

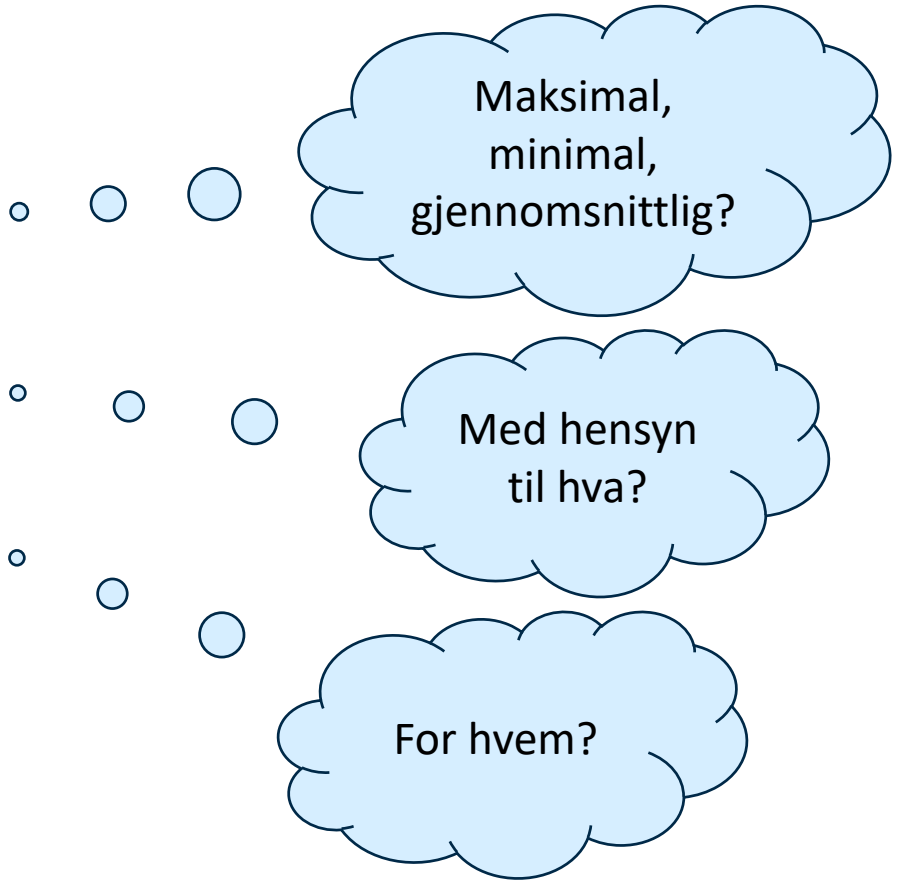
| Hyppighet |
| --- |
| Garantert |
| Sannsynlig |
| Mulig |
| Usannsynlig |
| Sjelden |




SINTEF

# Hva med denne?

| Konsekvens |
| --- |
| Katastrofal |
| Stor |
| Moderat |
| Liten |
| Ubetydelig |

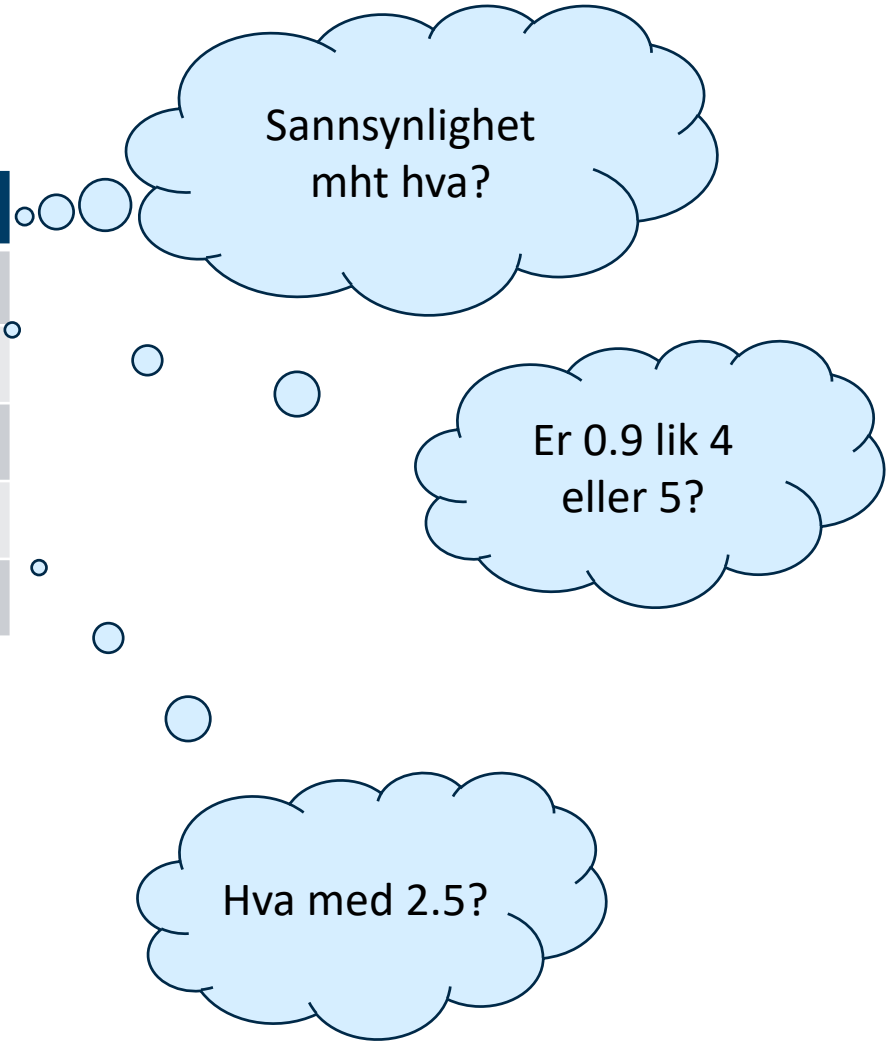





SINTEF

# Og denne?

| Verdi | Sannsynlighetsintervall |
|---|---|
| 5 | 0.9-1.0 |
| 4 | 0.7-0.9 |
| 3 | 0.3-0.6 |
| 2 | 0.1-0.2 |
| 1 | 0.0-0.1 |



# Hvilke typer skaler finnes?

# To hovedtyper av skalaer

Kvalitative: Verdier definert eller eksemplifisert i naturlig språk

Kvantitative: Verdier definert på en slik måte at konvensjonelle regneregler er veldefinerte

# To varianter av kvalitative skalaer

Nominalskala:

Verdiene svarer til ulike kategorier

Ordinalskala:

Verdiene svarer til ulike kategorier og disse kategoriene er ordna

# Kvalitativ nominalskala

| Aktiva kategori | Beskrivelse |
|---|---|
| Informasjon | Digital informasjon; under lagring så vel som kommunikasjon |
| Programvare | Kildekode, binærkode, dokumentasjon |
| Maskinvare | Datautstyr, men også annet utstyr/ting av relevans |
| Tjenester | Eksterne så vel som interne |
| Folk | Kunder, brukere så vel som ansatte |
| Immaterielle verdier | Omdømme, ekstern tillit |

# Kvalitativ ordinalskala

| Konsekvens | Beskrivelse |
|---|---|
| Katastrofal | Lekkasje av informasjon som kan utnyttes av terrorister |
| Stor | Lekkasje av informasjon som har juridiske implikasjoner |
| Moderat | Lekkasje av konkurranserelevant informasjon |
| Liten | Lekkasje av informasjon om ansatte |
| Ubetydelig | Lekkasje av informasjon som i vesentlig grad er offentlig |

# Huskeliste for kvalitative skalaer

- Utnytt det naturlige språket til fulle slik at verdiene blir mest mulig klare
- Pass på at definisjonene bruker ord og vendinger som egner seg for brukerne av skalaene
- Eksempler er ofte nyttige
- Er skalaen ordnet bør ordningen reflekteres i definisjonene
- Verdiene må dekke hele utfallsrommet

# To varianter av kvantitative skalaer

Differanseskala:

Subtraksjon (og addisjon) er veldefinert

Forholdsskala:

Divisjon (og multiplikasjon) er også veldefinert

# Dette er en kvantitativ differanseskala

| Hyppighet | Beskrivelse |
|---|---|
| Reelt positivt tall | Antall forekomster i snitt per år |

5 – 3 = 3 – 1 = 2

5 forekomster i snitt per år – 3 forekomster i snitt per år =
3 forekomster i snitt per år – 1 forekomster i snitt per år =
2 forekomster i snitt per år

# Det er også en kvantitativ forholdsskala

| Hyppighet | Beskrivelse |
|---|---|
| Reelt positivt tall | Antall forekomster i snitt per år |

6 / 3 = 2 / 1 = 2

6 forekomster i snitt per år / 3 forkomster i snitt per år =
2 forekomster i snitt per år / 1 forekomster i snitt per år =
dobbelt så mange forekomster i snitt per år

# Dette er også en kvantitativ forholdsskala

| Konsekvens | Beskrivelse |
|---|---|
| Naturlig positivt tall | Antall journaler lekket |

6 / 3 = 2 / 1 = 2

6 journaler lekket / 3 journaler lekket =
2 journaler lekket / 1 journal lekket =
dobbelt så mange journaler lekket

# En differanseskala som ikke er en forholdsskala har en tilfeldig valgt nullverdi

**Men** kan vi ikke bare regne på de talla vi har?

SINTEF

# Hvis regneoperasjonene ikke er veldefinerte må nytten av beregningene sjekkes empirisk

# Eksempel på beregning som må sjekkes empirisk

The first step is to select one of the options associated with each factor and enter the associated number in the table. Then simply take the average of the scores to calculate the overall likelihood. For example:

| **Threat agent factors** | | | | | **Vulnerability factors** | | | |
|---|---|---|---|---|---|---|---|---|
| Skill level | Motive | Opportunity | Size | | Ease of discovery | Ease of exploit | Awareness | Intrusion detection |
| 5 | 2 | 7 | 1 | | 3 | 6 | 9 | 2 |
| Overall likelihood=4.375 (MEDIUM) | | | | | | | | |

Next, the tester needs to figure out the overall impact. The process is similar here. In many cases the answer will be obvious, but the tester can make an estimate based on the factors, or they can average the scores for each of the factors. Again, less than 3 is low, 3 to less than 6 is medium, and 6 to 9 is high. For example:

| **Technical Impact** | | | | | **Business Impact** | | | |
|---|---|---|---|---|---|---|---|---|
| Loss of confidentiality | Loss of integrity | Loss of availability | Loss of accountability | | Financial damage | Reputation damage | Non-compliance | Privacy violation |
| 9 | 7 | 5 | 8 | | 1 | 2 | 1 | 5 |
| Overall technical impact=7.25 (HIGH) | | | | | Overall business impact=2.25 (LOW) | | | |

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

# Huskeliste for kvantative skalaer

- Pass på at det ikke er luker mellom verdier
- Pass på at verdiene ikke overlapper
- Pass på at hele utfallsrommet dekkes
- Vær mest mulig eksplisitt med hensyn til definisjoner og antagelser
- Er beregning viktig bruk skalaer for hvilket regneoperasjonene er veldefinerte
- I motsatt fall må beregningene sjekkes empirisk

# Oppsummering

- Skal vi måle cybersikkerhet må vi først bestemme fornuftige skalaer
- Mye av den "målingen" som foregår i praksis henger ikke på greip
- Kvantitativ er ikke (nødvendigvis) bedre enn kvalitativ
- Hva som er best egnet avhenger av situasjon og det som skal måles
- Uansett type skala er det viktig å være mest mulig presis