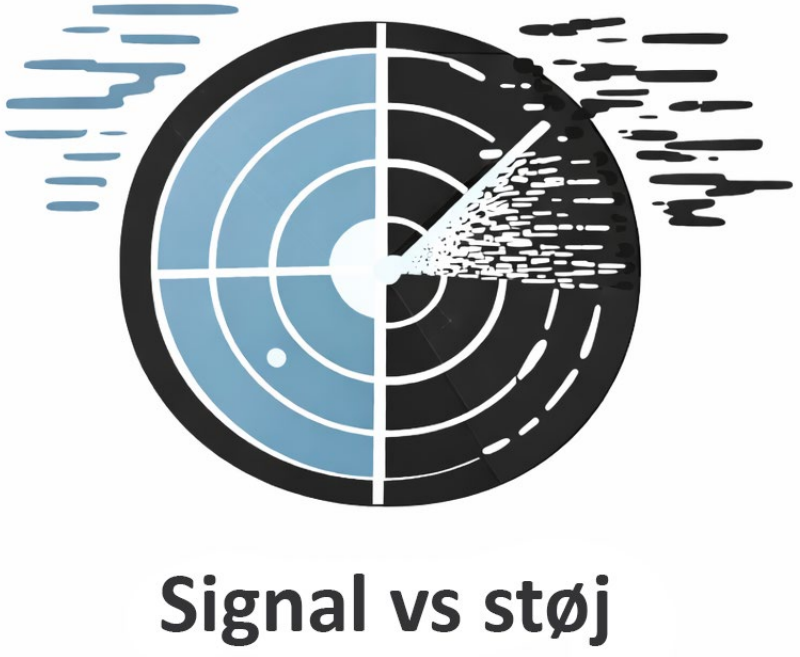
6. Signal vs. støj (Attention Economics)



www.cyber-smv.dk

Værktøjet er tilvejebragt i forbindelse med projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), støttet af Industriens Fond.
Offentliggjort den 09.01.2026.

Signal versus støj

Formål

→At forstå forskellen på vigtige sikkerhedssignaler og daglig støj.

→At blive bevidste om, at opmærksomhed er en begrænset ressourcelærer.

→At prioritere, hvad der kræver handling, og hvad der ikke gør.

→At reducerer risikoen for at overse kritiske advarsler i en travl hverdag.

Mental model

→*Angribere konkurrerer om din opmærksomhed.*

Deltagere

→Alle medarbejdere.

Input

→Oversigt over hændelser.

Hændelser (eksempler)

1. Mail om ændret leverandørkontonummer.
2. Pop-up om softwareopdatering.
3. Kollega spørger om hurtig hjælp.
4. Mail markeret som “haster” fra ukendt afsender.
5. Fejlmeddelelse fra produktionssystem.
6. Notifikation om nyt Teams-møde.
7. IT-mail om mulig phishing.
8. SMS fra “fragtfirma”.
9. Systemadvarsel, der ofte dukker op.
10. Intern besked fra leder uden detaljer.

Fremgangsmåde: Trin 1 - sortér signal og støj

→Deltagerne skal placere hver hændelse i én af tre kategorier:
- →**Signal** kræver opmærksomhed eller handling
- →**Støj** kan ignoreres eller vente
- →**Usikkert** kræver afklaring

→Deltagerne diskuterer:
- →Hvad gør denne hændelse vigtig eller uvigtig?
- →Hvad gør os tilbøjelige til at overse signaler?

Fremgangsmåde: Trin 2 - attention economics (10 min.)

→Deltagerne svarer på følgende refleksionsspørgsmål:

→Hvad konkurrerer mest om jeres opmærksomhed i hverdagen?

→Hvornår er I mest sårbare over for at overse signaler?

→Hvilke typer beskeder “drukner” let i støjen?

👉 **Pointen:** Angribere udnytter, at mennesker ikke kan være opmærksomme på alt hele tiden.

Fremgangsmåde: Trin 3 - design bedre signaler (10-15 min.)

→Deltagerne arbejder med følgende spørgsmål:
- →Hvordan kan vigtige sikkerhedssignaler gøres tydeligere?
- →Hvad kunne organisationen gøre for at reducere støj?
- →Hvad kan medarbejdere selv gøre for at beskytte deres opmærksomhed?

Mulige svar: Trin 1 - sortér signal og støj

→Signal (kræver handling/opmærksomhed):

- →Mail om ændret leverandørkontonummer→ Høj risiko for økonomisk svindel.
- →Mail markeret "haster" fra ukendt afsender→ Klassisk social engineering-mønster.
- →IT-mail om mulig phishing→ Bevidst sikkerhedssignal.
- →SMS fra "fragtfirma" med link→ Kendt angrebsmetode.

→Støj (kan vente/ignoreres):

- →Teams-notifikation om nyt møde.
- →Standard pop-up om softwareopdatering.
- →Kollega, der beder om hjælp til rutineopgave.
- →Systemadvarsel, der ofte dukker op uden konsekvens.

→Usikkert (kræver afklaring):

- →Fejlmeddelelse fra produktionssystem.
- →Intern besked fra leder uden detaljer.

👉 **Pointe:** Det er ikke altid indholdet, men konteksten (afsender, timing, pres), der afgør, om noget er signal eller støj.

Mulige svar: Trin 2 – attention economics

1. Hvad konkurrerer mest om medarbejdernes opmærksomhed?

→ Drift og produktion (”det skal køre”).
→ Tidsfrister og deadlines.
→ Mange mails, beskeder og notifikationer.
→ Afbrydelser fra kolleger og telefon.

2. Hvornår er medarbejdere mest sårbare?

→ Under tidspres eller produktionsproblemer.
→ Sidst på dagen / sidst på ugen.
→ Når beskeden virker “rutinemæssig”.
→ Når afsender udgiver sig for at være autoritet.

3. Hvilke beskeder drukner let i støjen?

→ Generelle sikkerhedsmails.
→ Gentagne advarsler uden tydelig konsekvens.
→ Tekniske beskeder uden klar handling.
→ Lange mails uden prioritering.

👉 **Pointe:** Angribere udnytter, at menneskelig opmærksomhed er begrænset, og gemmer angreb i mængden af legitim kommunikation.

Mulige svar: Trin 3 - design bedre signaler

1. Hvordan kan vigtige sikkerhedssignaler gøres tydeligere?

→ Klare overskrifter: “KRÆVER HANDLING”.
→ Kort og konkret sprog.
→ Én tydelig handling (f.eks. “Klik ikke – videresend”).
→ Kendt og ensartet afsender.

2. Hvordan kan organisationen reducere støj?

→ Færre, men mere målrettede mails.
→ Retningslinjer for brug af “haster”.
→ Samling af information i faste kanaler.
→ Fravælg unødvendige systemnotifikationer.

3. Hvad kan medarbejdere selv gøre?

→ Stoppe op ved tidspres og autoritet.
→ Vente med handling, hvis noget føles forkert.
→ Bruge kendte kontaktveje til verifikation.
→ Acceptere, at det er OK at spørge “en gang for meget”.