NVE

NVES OPPFØLGING AV RIKSREVISJONENS RAPPORT OM NVES ARBEID MED IKT-SIKKERHET I KRAFTBRANSJEN

Eldri Naadland Holo
NVE

NVE

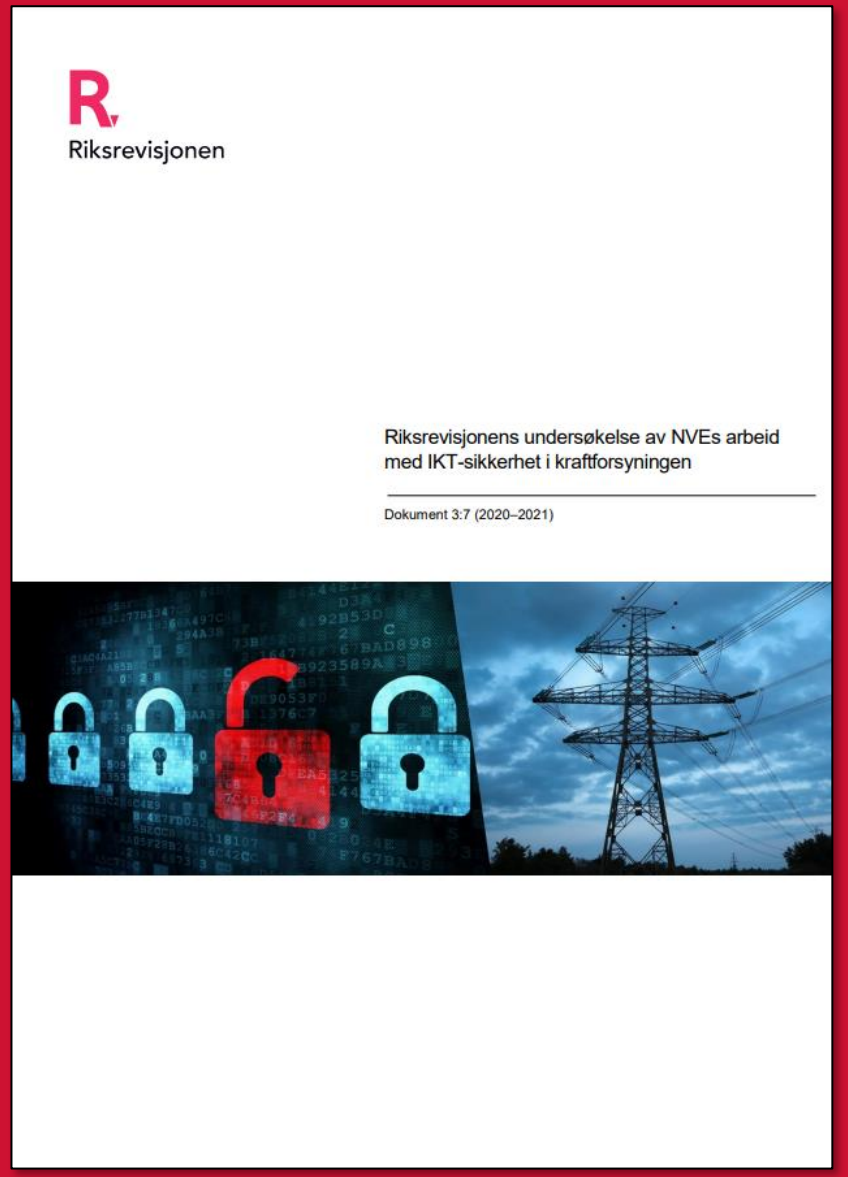
«Kritiske samfunnsfunksjoner og andre norske interesser er avhengige av digitale infrastrukturer som stadig øker i omfang og kompleksitet.

Lange og uoversiktlige digitale verdikjeder, som spenner over flere sektorer og landegrenser, er en kjerneutfordring ved vurdering av digital sårbarhet.»

Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen

Kritikknivå: **Alvorlig**

- Det er alvorlig at NVE ikke i tilstrekkelig grad har påsett at kraftselskapene har god beredskap for å håndtere IKT-angrep mot kraftforsyningen.



Riksrevisjonens rapport – sammenhengen mellom konklusjoner og anbefalinger

NVE har ikke i tilstrekkelig grad påsett at det er god beredskap for å håndtere IKT-angrep i kraftforsyningen:

- NVEs styring og oppfølging av arbeidet med IKT-sikkerhet i kraftforsyningen er svak.
- Det er svakheter ved NVEs tilsyn med IKT-sikkerhet i kraftforsyningen.
- NVE har skjerpet kravene til IKT-sikkerhet i kraftforsyningen, men ikke fulgt opp med tilstrekkelig veiledning.
- Det er svakheter ved NVEs arbeid med overvåking, varsling og beredskap ved IKT-hendelser.
- Oppfølgingen av leverandørene er mangelfull til tross for at de har stor betydning for IKT-sikkerheten i kraftforsyningen.

Sørge for at NVE styrker arbeidet med IKT-sikkerhet i kraftforsyningen, herunder:

- videreutvikler verktøy for å styre og følge opp arbeidet
- sikrer et bedre kunnskapsgrunnlag for IKT-sikkerhetstilstanden
- vurderer tilsynsmetodikken og gjennomfører risikobaserte IKT-sikkerhetstilsyn
- sikrer god veiledning til bransjen
- fortsetter med kompetansehevende tiltak internt og for bransjen
- videreutvikler systemet for avdekking og deling av IKT-sikkerhetshendelser
- oppdaterer beredskapsplanverket og gjennomfører flere IKT-øvelser
- vurderer tiltak for å håndtere utfordringen med å følge opp leverandørenes IKT-sikkerhet

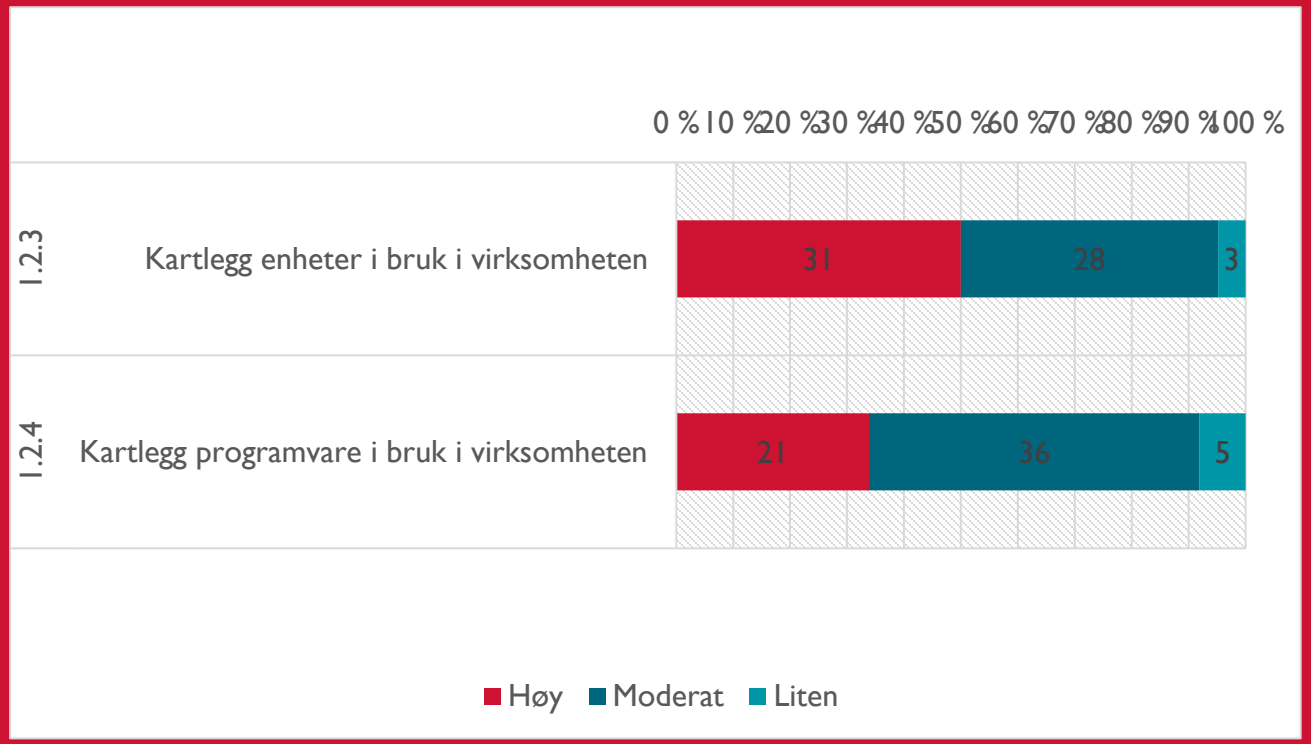
Gode innspill fra bransjewebinar 27. april

- Behov for bedre forståelse av (IKT-)risiko og sårbarhet i ledelse/styre
- Læring fra tilsyn
- Hendelsesdeteksjon
- Oppfølging av leverandører

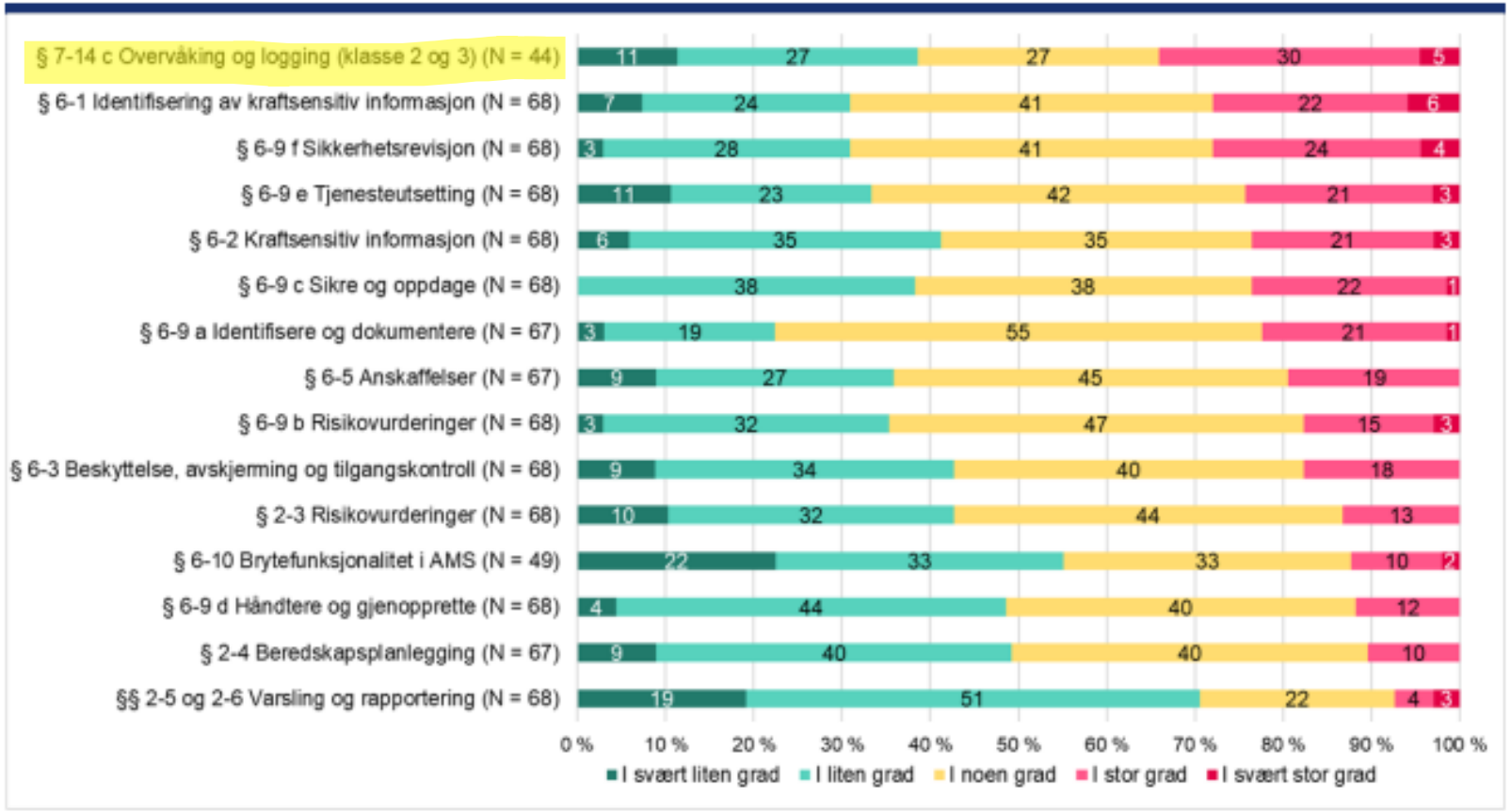
Vi må gjøre hverandre gode

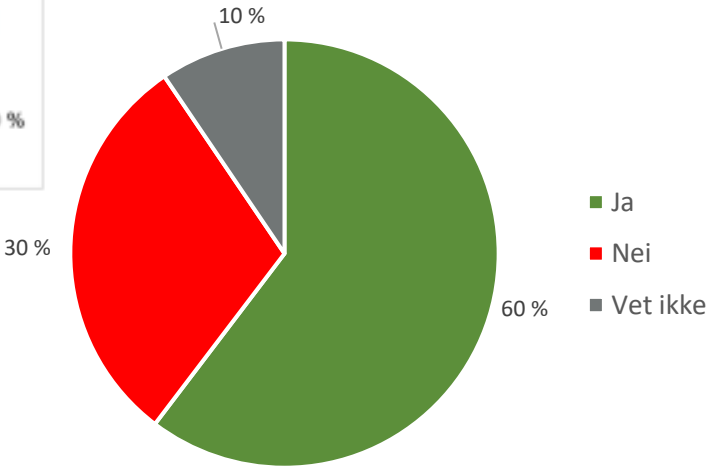
- IKT-SIKKERHETSTILSTANDEN
- TILSYN
- VEILEDNING
- KOMPETANSEHEVENDE TILTAK

IKT-sikkerhetstilstanden 2021 (rapport kommer snart)



Figur 2 IKT-sikkerhetskoordinatorenes svar på om utvalgte krav er utfordrende å etterleve





Sårbarhetsvarsling, avdekking og hendelseshåndtering

Rammeverk for håndtering av IKT-sikkerhetshendelser

Versjon per 07.12.17

NVE

Kraft CERT

Nasjonalt cybersikkerhetssenter

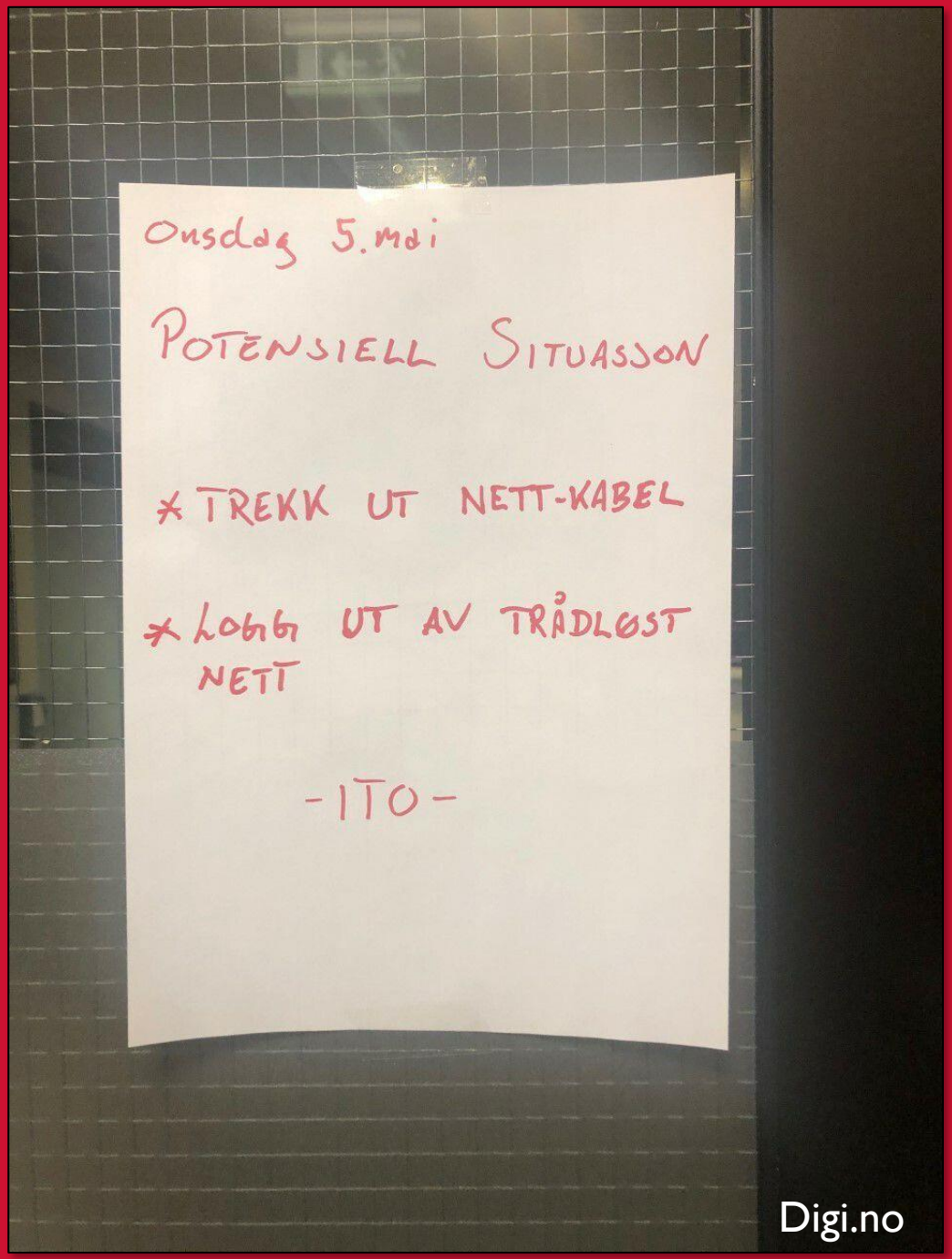
NASJONAL SIKKERHETSMYNDIGHET

HENDELSE I VIRKSOMHET

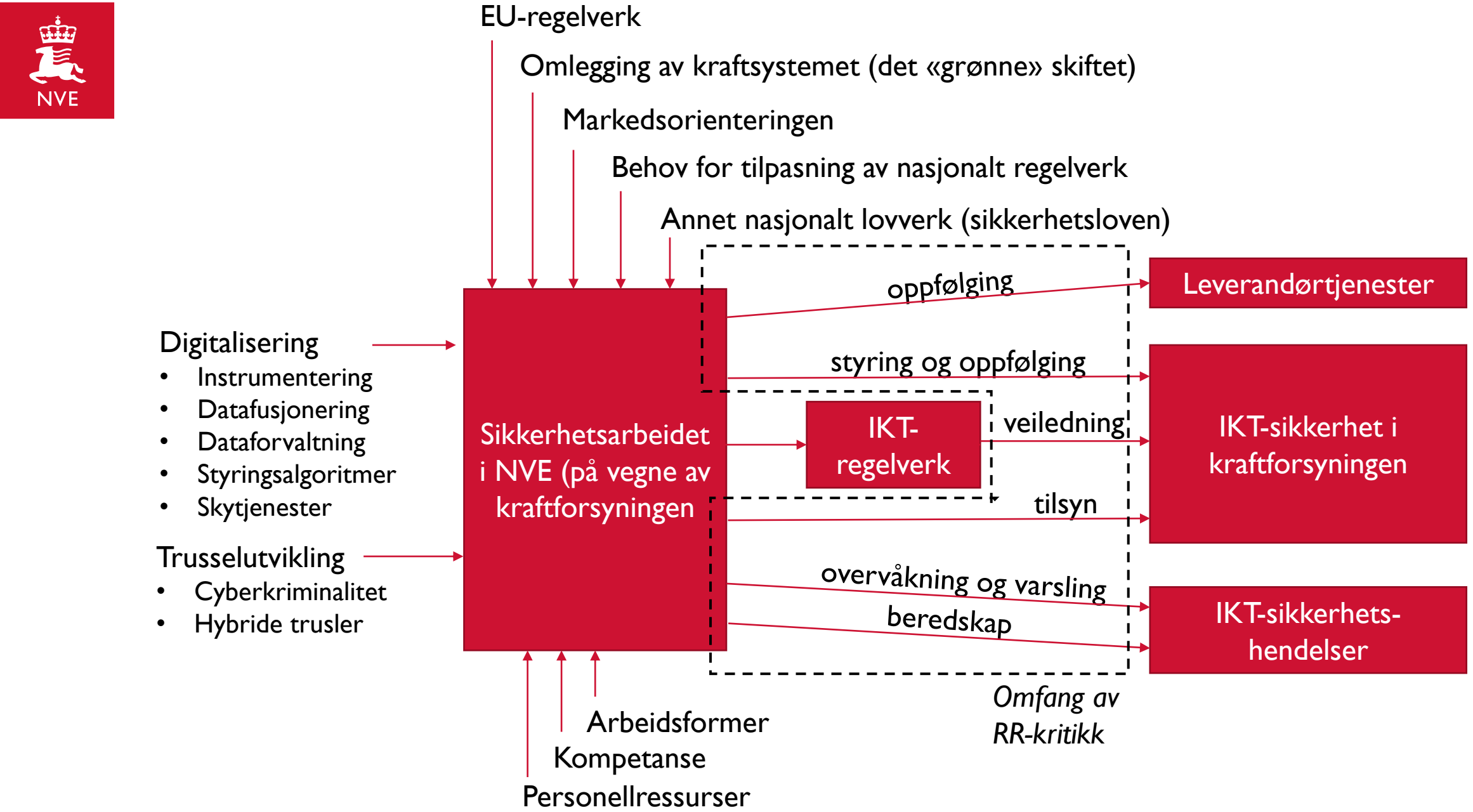
Digitale angrep

Norsk Hydro Cyber Attack a Wake Up Call for Maritime Industry

www.nor-shipping.com



Digi.no


EU-regelverk
Omlegging av kraftsystemet (det «grønne» skiftet)
Markedsorienteringen
Behov for tilpasning av nasjonalt regelverk
Annet nasjonalt lovverk (sikkerhetsloven)
Digitalisering
• Instrumentering
• Datafusjonering
• Dataforvaltning
• Styringsalgoritmer
• Skytjenester
Trusselutvikling
• Cyberkriminalitet
• Hybride trusler
Sikkerhetsarbeidet i NVE (på vegne av kraftforsyningen
IKT-regelverk
oppfølging
styring og oppfølging
veiledning
tilsyn
overvåkning og varsling
beredskap
Leverandørtjenester
IKT-sikkerhet i kraftforsyningen
IKT-sikkerhets-hendelser
Arbeidsformer
Kompetanse
Personellressurser
Omfang av RR-kritikk

Kraftberedskapsforskriften krever **balanserte tiltak**
Eksempel for klasse 2 kraftstasjon (kbf vedl 2 til §5-5)

Sikringsnivå – kombinasjon av tiltak

Tiltakene komplettere hverandre

Fungere uavhengig av utfall i strømforsyning og påregnelige feil i egen forsyning

Betjenes lokalt i ekstraordinære situasjoner

Starte på spenningsløst nett

Ansvarlig digitalisering – i kraftforsyningskontekst

Vi må gjøre vårt – aktørene i kraftbransjen må gjøre sitt


Takk for oppmerksomheten!