NVE

NORGES ENERGIDAGER 2021

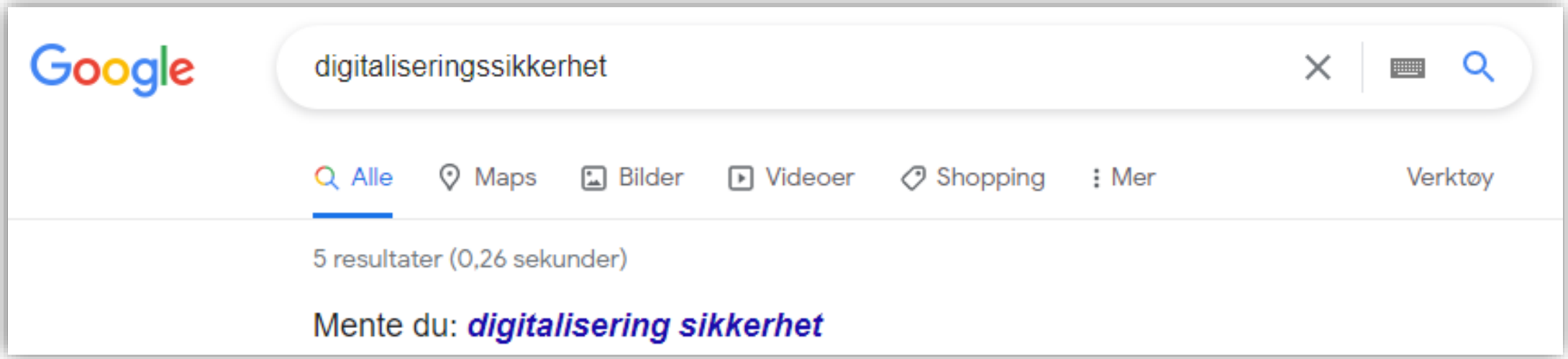
DET STORE BILDET

Sesjon 1

Digitaliseringssikkerhet i energibransjen

NVE 100 ÅR

Viktig funksjon – mange begreper…



Viktig funksjon – mange begreper…

NVE

NORGES ENERGIDAGER 2021

› DET STORE BILDET

DIGITALISERING OG IKT-SIKKERHET I ENERGIBRANSJEN

Sesjon 1

NVE 100 ÅR

Agenda for Sesjon 1 – Digitalisering & IKT Sikkerhet

Forventninger til energibransjen – planer for digitaliseringsforum og intro til bransjesamarbeidet DIGIN

08:30 – 08:40: Energi Norge v/Lars Berthinussen (Programleder DIGIN)
08:40 – 08:50: NVE/RME v/Jørgen Tjersland (Avdelingsingeniør)

Det grønne taktskiftet – økt digitalisering

08:50 – 09:15: Statnett v/Beate Krogstad (Fung. Konserndirektør Transformasjon og Digitalisering)

Nasjonalt digitalt risikobilde i 2021

09:15 – 09:40: Nasjonal sikkerhetsmyndighet (NSM) v/ Bente Hoff (Avdelingsdirektør)

Cybersikkerhet – sårbarheter i energibransjen ved økt digitalisering

09:40 – 10:00: ABB v/Judith Rossebø (Cyber security specialist)

Bruk av skytjenester hos KBO-enheter (Kraftforsyningens beredskapsorganisasjon)

10:00 – 10:15: Advokatfirma Hjort DA v/Ola Hermansen (Advokat) & Eivind Grimsø Moe (Advokat)

IKT-sikkerhet: Kravene som stilles til energibransjen nå og fremover

10:15 – 10:30: NVE v/Janne Hagen (Spesialrådgiver) og NVE/RME: Øyvind Toftegaard (Seniorrådgiver)

Spørsmål + pause (neste sesjon starter kl. 11:00)

NVE

NORGES ENERGIDAGER 2021

› DET STORE BILDET

DIGIN – NETTBRANSJENS DIGITALISERINGSINITIATIV

Lars Berthinussen, DIGIN/Energi Norge

NVE 100 ÅR

Digitaliseringssikkerhet i energibransjen

- forventninger til bransjen

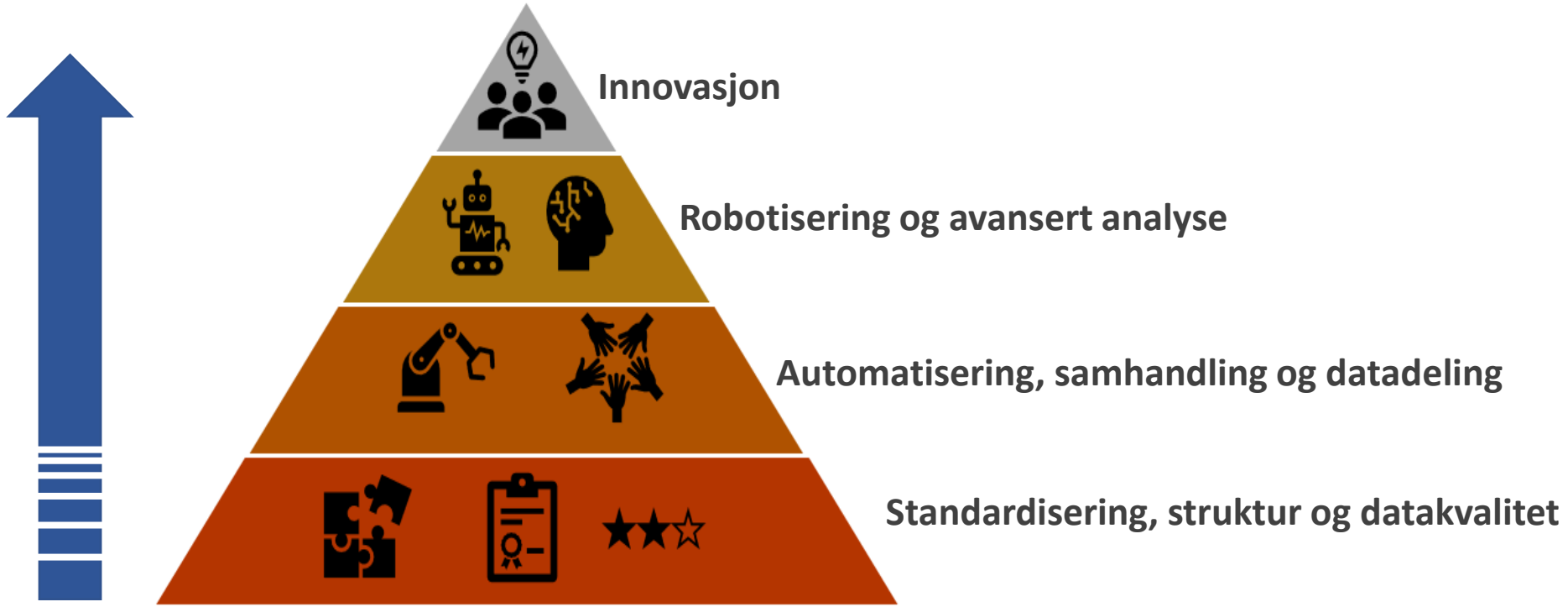
Norges Energidager 22. oktober 2021

Lars Berthinussen
Leder for DIGIN

DIGIN er et bransjesamarbeid om digitalisering for å løse fremtidens nett- og kraftsystemutfordringer på en smart måte

Støttespillere:

Digitaliseringspyramiden og veien til innovasjon gir retning til arbeidet



DIGIN

NVE

NORGES ENERGIDAGER 2021

› DET STORE BILDET

DIGITAL SAMHANDLING I NETTBRANSJEN

Jørgen Tjersland, NVE/RME

NVE 100 ÅR

NVE
Reguleringsmyndigheten for energi – RME

NORGES ENERGIDAGER 2021

DET STORE BILDET

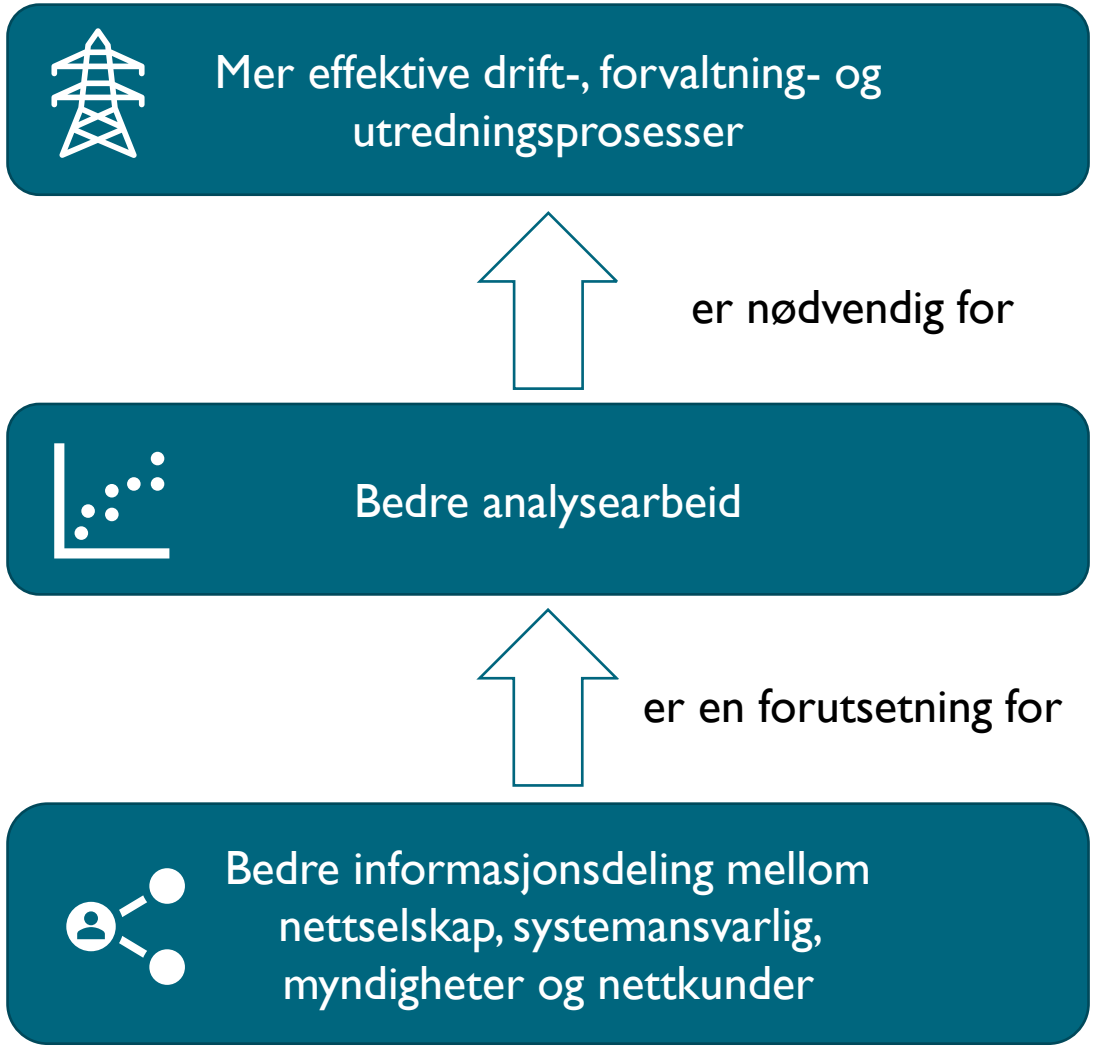
DIGITAL SAMHANDLING I NETTBRANSJEN

Prosjekt om målbilde, veikart og styringsmodell for samhandling

Jørgen Tjersland (NVE-RME)

Foto: Navn Navnesen, NVE

Informasjonsdeling er en muliggjører



Prosjektet tar utgangspunkt i EIF-modellen:

Vi ser på ulike mulighetsdimensjoner for hvordan et Forum for Digitalisering kan etableres

Vi ønsker å etablere et målbilde sammen med bransjen og har et sterkt fokus på kontinuerlig forankring

Gevinstene vil i hovedsak ligge hos nettselskapene og systemansvarlig

Problemstillingene er komplekse og kan ikke løses av én aktør

Vi må ha god dialog på tvers av bransjen for å finne de beste løsningene sammen

NVE

NORGES ENERGIDAGER 2021

› DET STORE BILDET

DET GRØNNE TAKTSKIFTET – ØKT DIGITALISERING

Beate S. Krogstad, Statnett

NVE 100 ÅR

Det grønne taktskiftet

- er *avhengig av økt digitalisering*

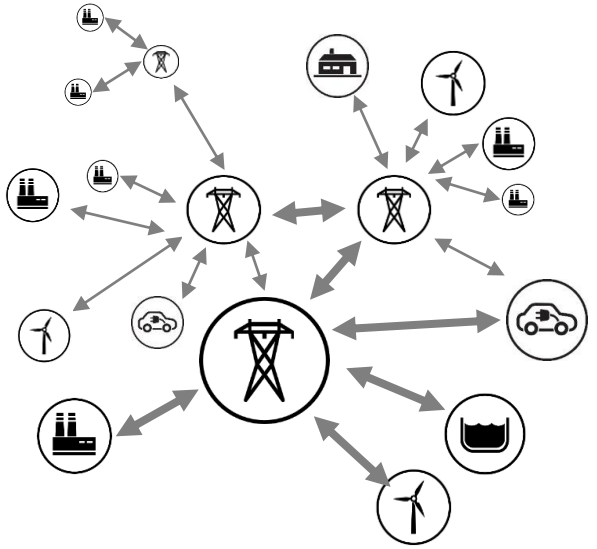
Beate S. Krogstad

Statnett

NVEs Energidager 2021

Bakgrunn - Store endringer i kraftsystemet

Nullutslippssamfunnet gir radikale endringer av kraftsystemet i Europa og Norge



Tettere integrasjon mellom land og sektorer

Ny teknologi og digitale løsninger gjør omstillingen mulig

Vi må planlegge for økt tempo og dynamikk

Fra Statnetts strategi:

Statnett

.. er avhengig av
økt digitalisering

Statnett

Digitalisering er nødvendig for effektiv styring, overvåking og utnyttelse av kapasiteten i nettet

Mer effektiv gjennomføring av prosjekter fra plan til drift

Statnetts anlegg har gjenanskaffelsesverdi på mer enn 250 mrd. Enkelte anlegg er mer enn 70 år gamle..

Effektiv forvaltning av eksisterende anleggsmasse

Statnett

Kraftsystemdriften av det fornybare kraftsystemet krever økt automatisering og digitalisering

Statnett

Digitalisering, innovasjon og transformasjon er nødvendig for å håndtere raskere utvikling og økt gjennomføringskraft

Statnett

Viktige digitale byggeklosser

Helhetlige digitale virkemidler bidrar til å realisere målbildet

Eks. på mulige effekter

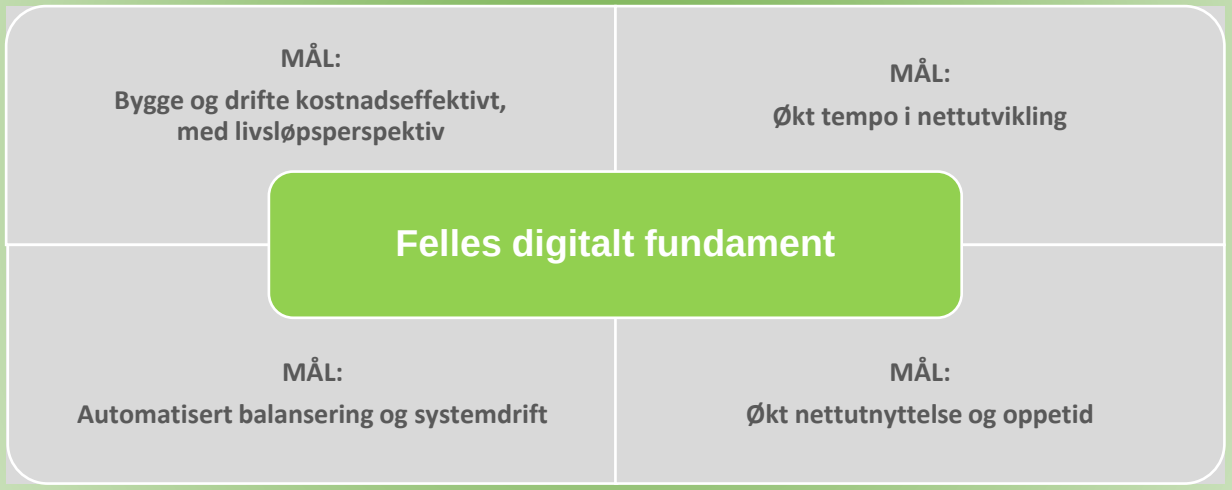
Redusere livsløpskostnader for anlegg med 25 %

Ledetiden på nettplanleggingen er kraftig redusert

Betydelig mer effektiv kraftsystemplanleggingen

Fra komponentkjøp til tjenestekjøp ("Sensor as a service")

Reduksjon av timeforbruk i tidligfase med 30% og gjennomføring med 10 %



Feil avdekkes i primærkomponentene før de oppstår

Industriell "app-store" og standardiserte datamodeller kutter prisen på nye applikasjoner

Reduserte driftsforstyrrelser v.h.a automatiserte tester på digital tvilling

Modellering av endringer i kraftsystemet går 10x raskere

Driftsstanser koordineres optimalt

Dynamic Line Rating øker termisk kapasitet på ledningene med 10 %

Takk for oppmerksomheten

Statnett

NVE

NORGES ENERGIDAGER 2021

DET STORE BILDET

NASJONALT DIGITALT RISIKOBILDE 2021

Bente Hoff, NSM

NVE 100 ÅR

Nasjonalt digitalt risikobilde 2021

NASJONAL
SIKKERHETSMYNDIGHET

Et taktskifte innenfor digital risiko

NASJONAL
SIKKERHETSMYNDIGHET

Foto: Beate Oma Dahle NTB, Colourbox

LØSEPENGEVIRUS

NSM advarer kommuner og offentlig sektor om løsepengevirus

NSM advarer kommuner og offentlig sektor etter flere høyprofilerte angrep med løsepengevirus den siste tiden. (Foto: Colourbox/40185522)

NTB SIKKERHET 18. JAN. 2021 - 09:32

Globale hendelser krever samlet respons

Foto: BBC,Techrepublic.com, Kaseya.

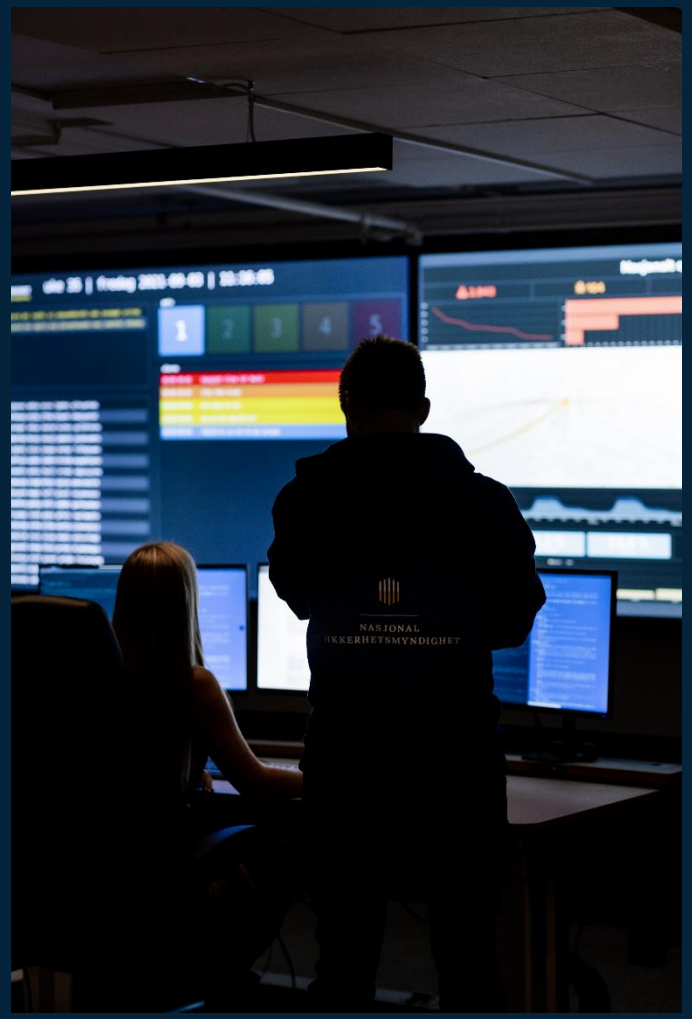
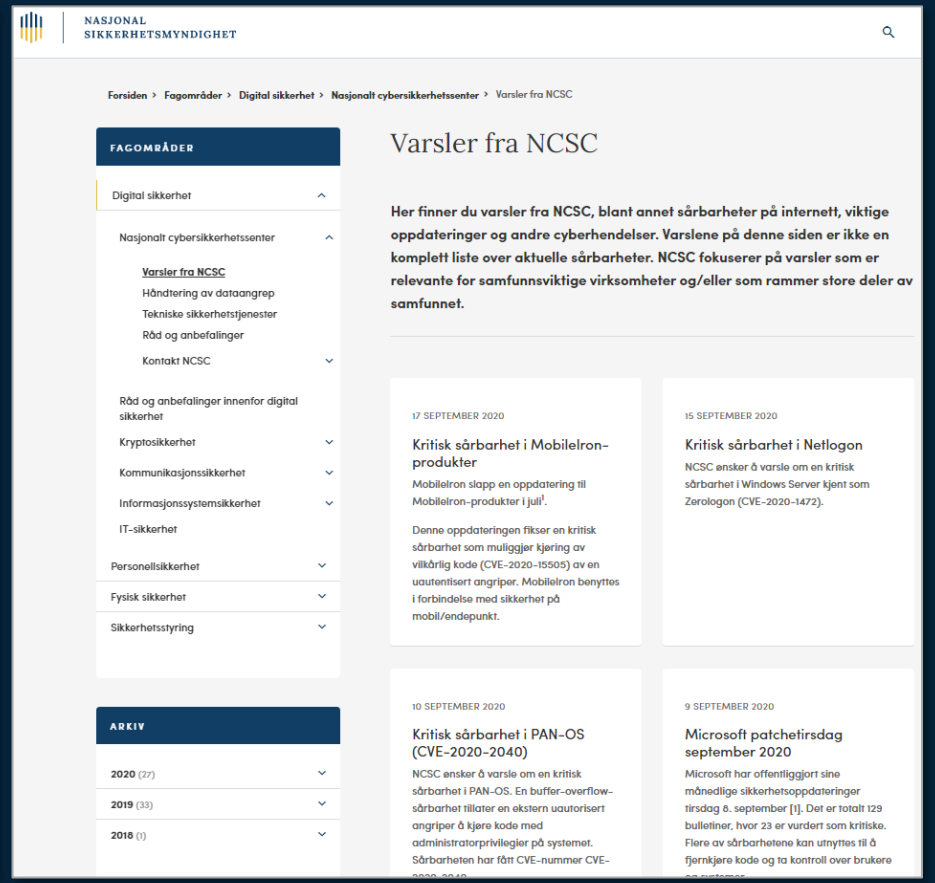


Foto: NTB, NSM.

NASJONAL
SIKKERHETSMYNDIGHET

Foto: NTB Scanpix / Monica Strømdahl / Aftenposten

Situasjonsforståelse og tiltak nytter



Et økosystem for digital sikkerhet

Teknologi i utvikling og digitalisering fremover

Foto: Datafjellet

Et taktskifte innen digital risiko

- Økning i antall alvorlige hendelser
  - Omfattende hendelser mot flere sektorer og mål
  - Konsekvenser for stas- og samfunnssikkerhet
- Cyberoperasjoner får synligere konsekvenser
  - Globale leverandørkjedeangrep
  - Løsepengevirus
- Digital sikkerhet har blitt et strategisk tema globalt
- Det haster å implementere risikoreduserende tiltak
- God digital grunnsikring krever en nasjonal innsats

NASJONAL
SIKKERHETSMYNDIGHET

Takk for oppmerksomheten!

NASJONAL
SIKKERHETSMYNDIGHET

NVE

NORGES ENERGIDAGER 2021

DET STORE BILDET

CYBERSIKKERHET & SÅRBARHETER I ENERGIBRANSJEN VED ØKT DIGITALISERING

Judith Rossebø, ABB PA Energy Industries

NVE 100 ÅR

2021-10-22

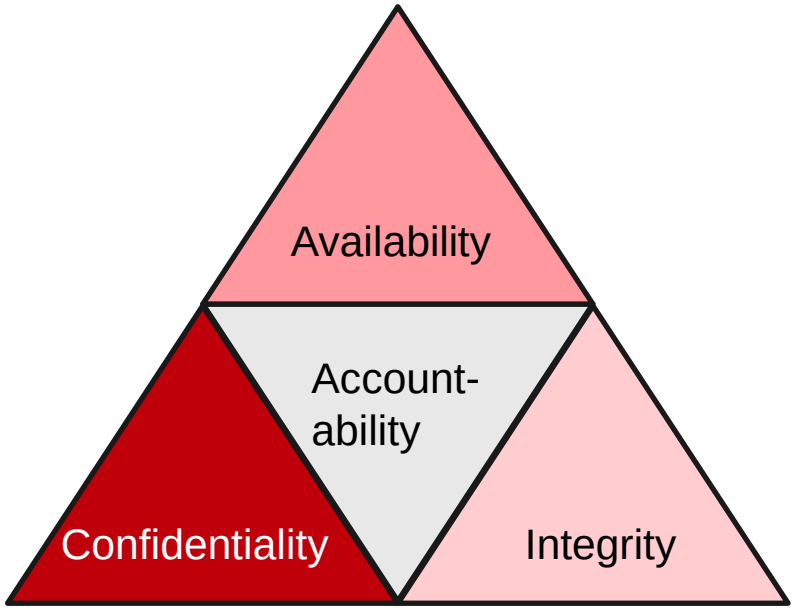
Cybersikkerhet & sårbarheter i energibransjen ved økt digitalisering

Norges Energidager 2021

Judith Rossebø, Cyber Security Specialist, ABB PA Energy Industries

Cybersikkerhet – hva er det?

Cybersikkerhet – å sikre fysiske infrastruktur og fysiske ting som er sårbare via IKT

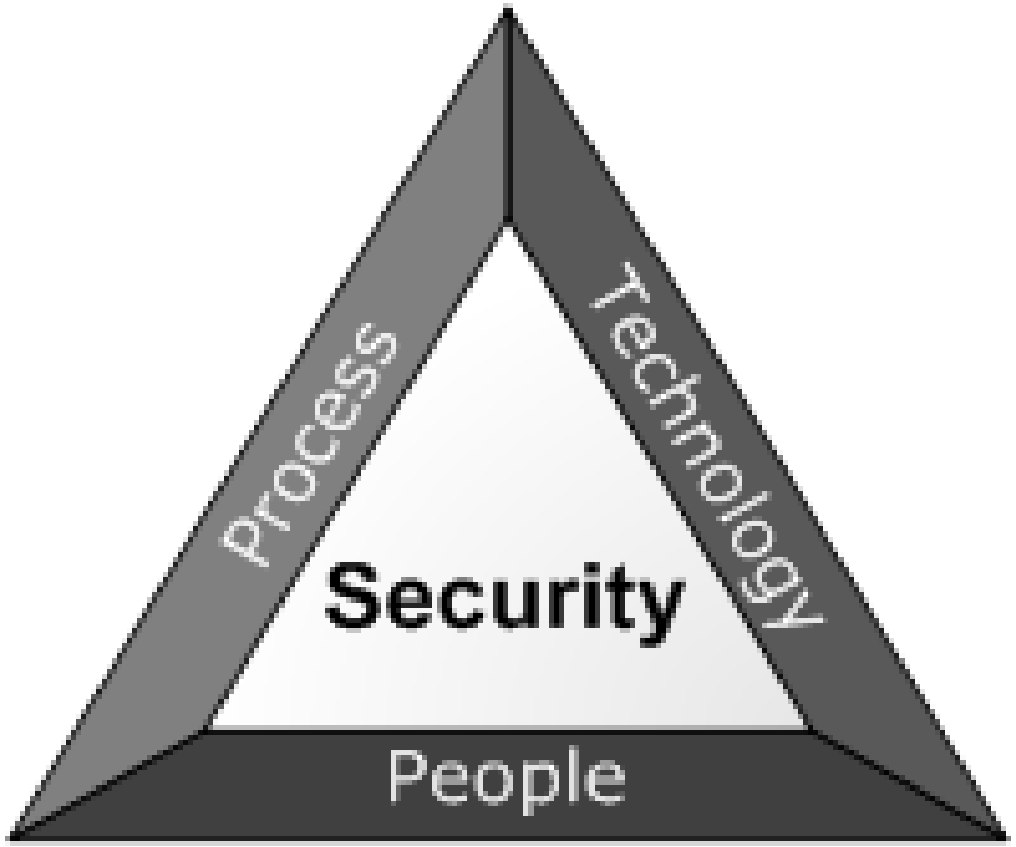


«CIA triad» + Accountability:

- **Confidensialitet** – hindre tilgang for uvedkommende
- **Integritet** – hindre endring/sletting fra uautoriserte personer
- **Tilgjengelighet** – sikre tilgjengelighet til enhver tid for de autoriserte brukerne
- **Sporbarhe**t – å kunne dokumentere hendelsens forløp i ettertid med tidelig ansvar

Cybersikkerhet i praksis

Identifisere
Beskytte
Detektere
Respondere
Gjenopprette



- Risk assessment
- Asset Inventory
- Perimeter Defense
- Network Segmentation
- Access Control
- Secure Remote Access
- System Integrity and Availability
- Software Management
- Hardening
- Security Awareness & Training
- Event & Incident Management

Cyberangrep skjer!

Ødelegge industrielle prosess

Forårsake Strømbrud

Løsepengevirus

Forsyningskjede-angrep

"This release includes bug fixes, increased stability and performance improvements."

Sources:
https://www.wired.com/story/crash-override-malware/, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

Energibransjen – Trusselbildet og Hendelser

2006 – Black Energy 1 - DDoS verktøy

2010 – Black Energy 2 – Viderutviklet til å inkludere spioneringsverktøy og spam verktøy

2011 – Night Dragon – Sjulte cyberangrep rettet mot sensitive informasjon i energibransjen

2013 – Havex malware – Cyberspionasje rettet mot bla energibransjen

2014 – Black Energy 3 – Videreutviklet med evner til å skaffe tilgang til SCADA nettverk

2015 – Cyberangrep: Malware infiserer 3 regionale energiselskaper og brukes i en koordinert angrep

- 225 000 kunder uten strøm i opp til 6 timer

2016 – Industroyer/CrashOverride skadevare designet til å angripe elnettet

2016 – Cyberangrep: automatisert angrep (Industroyer) årsaker strømbrud i en storby

- 760 000 kunder uten strøm i 1,5 hrs

2016 – Nå – Pågående intrengniger i energisektoren

2020 – Cyberangrep: - Solar Winds – forsyningskjedeangrep

2021 – Cyberangrep: - Volue RYUK Løsepengevirusangrep

Digitalisering i energisektoren

“Digitale” Komponenter

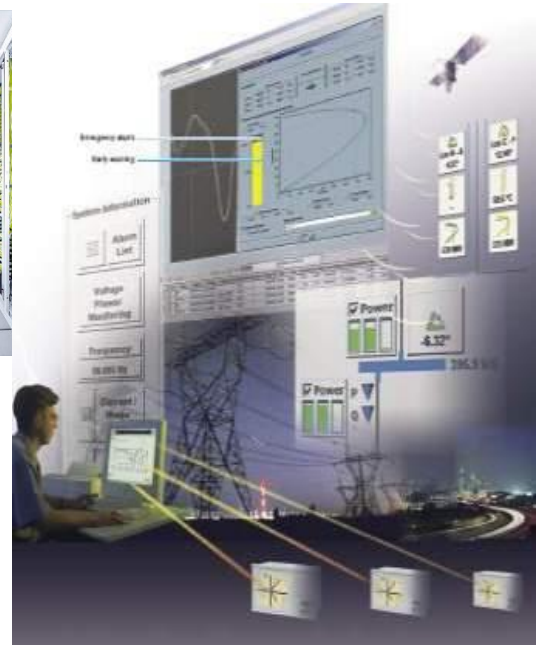
Ulike sensorer i vindturbiner gir fra seg informasjon om tilstand til ulike komponenter

Detektere, monitorere, kommunisere …

“Digitale” Kraftlinjer

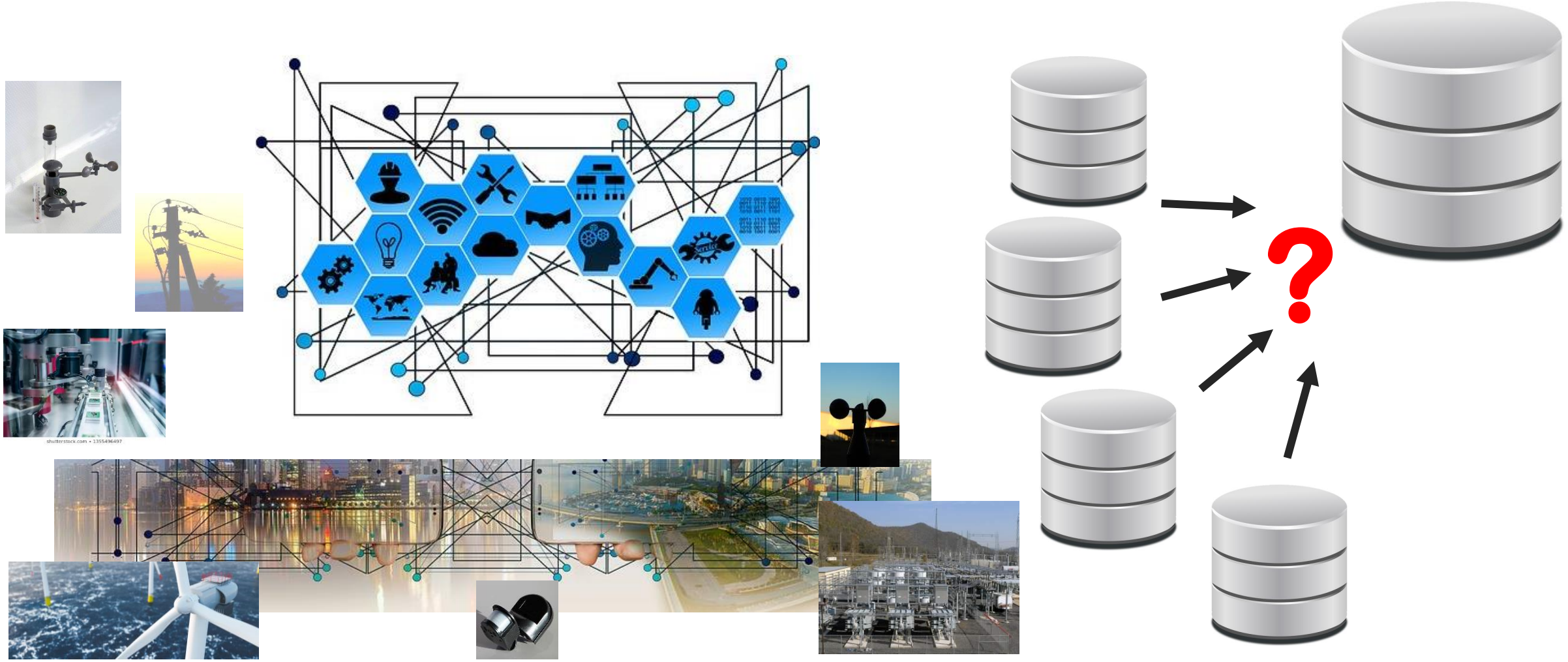
Sensorer langs kraftlinjene måler temperature, vibrasjon, ising, linjenes helningsvinkel..

Sanntids “Digitale” SCADA



Sensorer i alle stegene i verdikjeden – for optimalisering av energisystemene

Digitalisering – fra mange kilder til et harmoniserte datasett



Data Analyse – Hva er viktig? Hvordan håndterer vi sikkerhet?

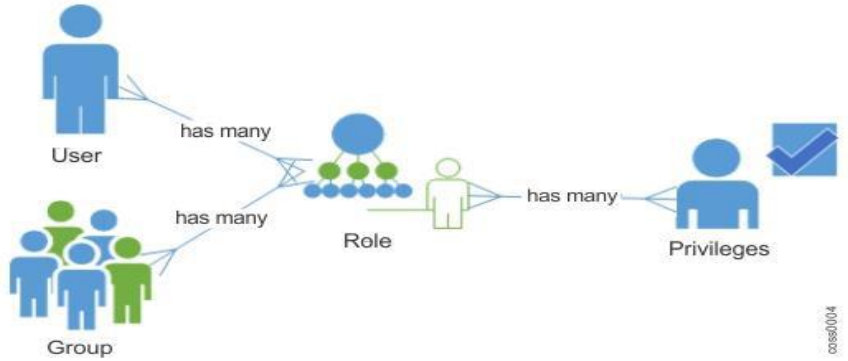
Hvem trenger tilgang til hva?

Hvor sikker er teknologien som brukes i løsningen?

Hvem har eierskap?

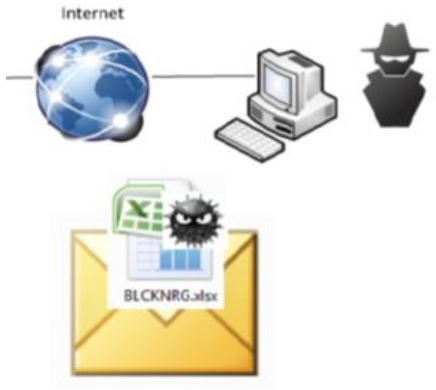
Hvem har ansvar?

Hva med trusler og trussel aktører? Risikostyring er et viktig punkt.



Risikostyring

RISIKO:
Trussel-aktører får tilgang til data, de etablerer et bilde av kraftsystemet og forstår hvordan de skal gå inn å gjennomføre et målrettet angrep. Trusselaktørene finner alltid det svakeste ledd.



De største truslene er etterretning og påvirkning fra statlige aktører, samt kriminelle

Bevisstheten om digital sikkerhet er avgjørende

Risikobildet

Angrepene blir mer og mer sofistikerte, men det finnes en del fellesnevner

Ukrainian Attack - 2015

- Spearphishing for å stjele credentials, legg igjen malware
- Mulig å beveger seg fritt og kartlegger miljøet (uoppdaget)
- Lett å hoppe fra IT til OT
- Utnyttet svak beskyttet VPN
- Koordinert angrep – åpnet brytere manuelt hos 3 energiselskap
- Resultat var umiddelbar strømbrud
- Bruk av en Wiper for å hindre restaurering

Ukrainian Attack - 2016

- Spearphishing for å stjele credentials, legg igjen malware
- Mulig å beveger seg fritt og kartlegger miljøet (uoppdaget)
- Lett å hoppe fra IT til OT
- Utnyttet flat OT net
- Tidsinstilt malware for automatisk kontrol av svitsjene og bryterne
- Resultatet var umiddelbar strømbrud
- Bruk av en Wiper for å hindre restaurering

2020 - Forsyningskjedeangrep

- Utnyttet svake windows passord for å komme inn hos SolarWinds WIN365/AD.
- La inn en «bakdør» i Solarwinds programvare oppdateringer (uoppdaget) for å ramme kundene
- Mulig å beveger seg fritt og kartlegger miljøet (uoppdaget) hos kundene
- Utnyttet en kombinasjon av on-premise and Cloud-based networks (uoppdaget) over lengre tid

Source:
https://www.dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf

Cyberangrep - lessons learned

Angriperne gjør kun det som trengs for å oppnå målene

- Initial Intrenging - Identifisere svakheter for å komme inn
  - Spearphishing epost
  - Svakheter i VPN, nettverksutstyr, eller servere som kan nåes fra utsiden
  - «Zero days» og sårbarheter i operativsystemer (Win, Linux)

- Ventetid og plannlegging – datainnsamling og kartlegging
  - Opprettthold tilgang og gjemme seg
  - Utvikle og teste angrepsverktøy

- Gjennomføre angrep
  - Spesialiserte malware
  - Med konsekvenser for Offrene

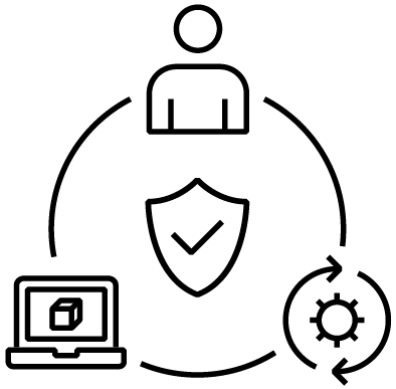
Bevisstheten om digital sikkerhet er avgjørende for å kunne oppdage inntrengerne

Cybersikkerhet en prosess mer enn et enkelt tiltak

Det er viktig å engasjere og utdanne mennesker, utvikle og ta i bruk prosesser, og designe og levere beskyttet teknologi

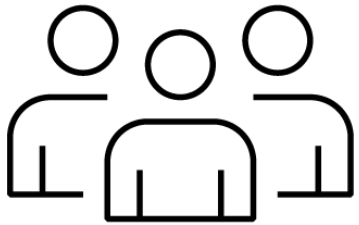
3 komponenter:

- Mennesker, Prosesser, og Teknologi: Hver av disse må aktiverers for å beskytte digitale systemer



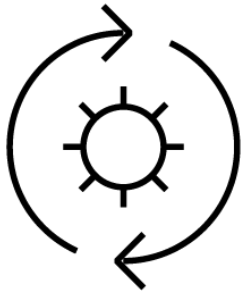
Mennesker

- Mennekser er kritisk for å kunne forebygge og beskytte mot cyber trusler.
- Organisasjoner trenger kompetente mennesker til å implementere og ivareta cybersikkerhets tiltak (teknologi og prosess).



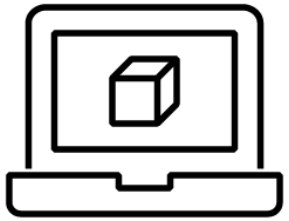
Prosesser

- Policier and Prosedyrer er nødvending for organisasjonens effective sikkerhets strategi.
- Disse må kunne endres I takt med endringer i trusselbildet.

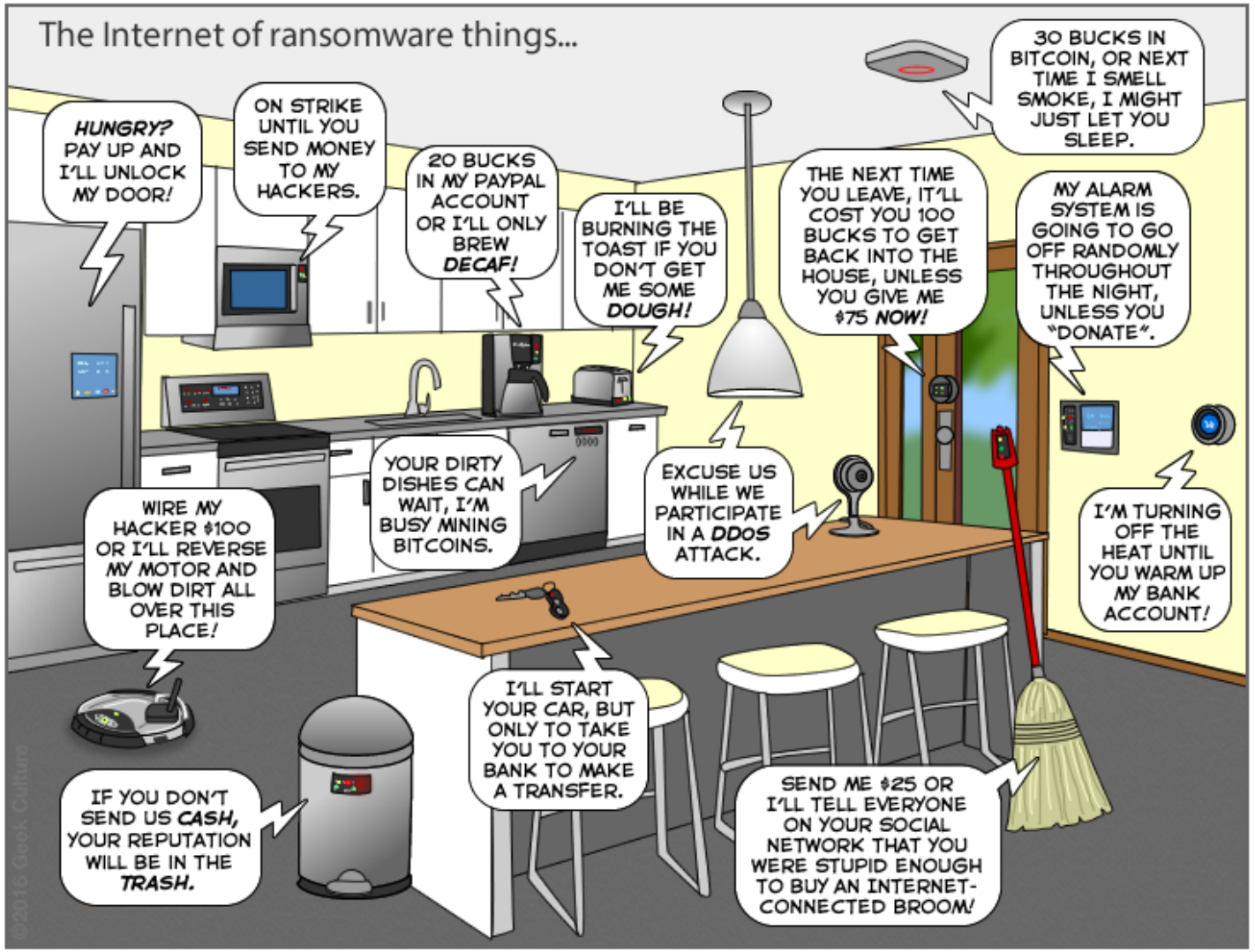


Teknologi

- Teknologi er viktig for å forebygge og mitigere cyber risiko.
- Teknologi er avhengige av mennesker, prosessor og prosedyrer for å kunne mitigere risiko.



The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com


ABB

NVE

NORGES ENERGIDAGER 2021

› DET STORE BILDET

BRUK AV SKYTJENESTER I KBO-ENHETER

Ola Hermansen & Eivind Grimsø Moe, Advokatfirmaet Hjort DA

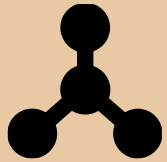
NVE 100 ÅR

HJORT

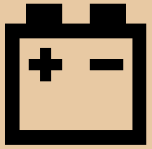
Bruk av skytjenester i KBO-enheter

NVEs Energidager, 22. Oktober 2021

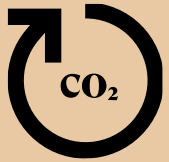
Juridiske rådgivere for det grønne skiftet



Ammoniakk



Batteriteknologi



CCS & CCUS

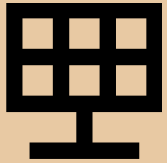
Havvind

Hydrogen

Landvind

Markedsplass

Nettanlegg og nettregulering



Solceller

Vannkraft

Agenda

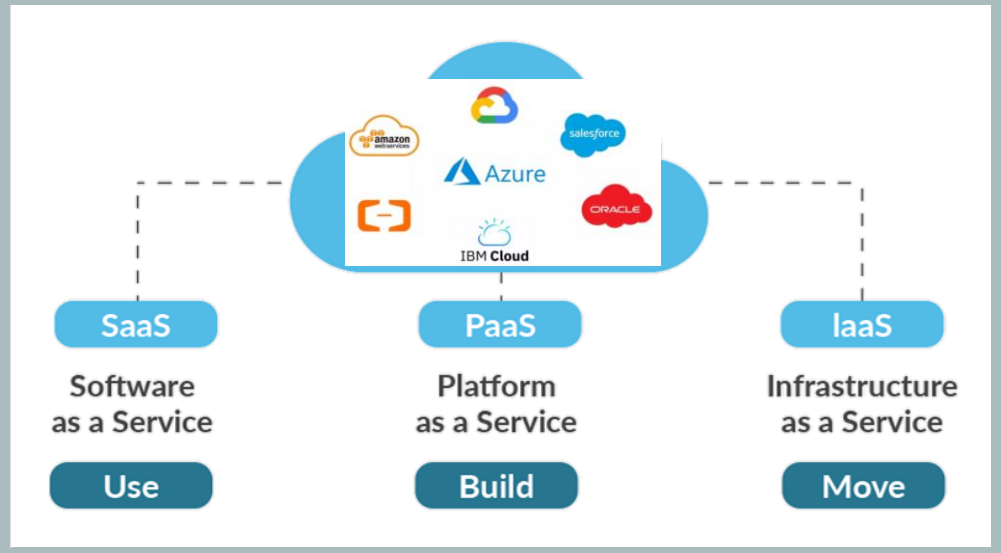
1 Kort om skytjenester

2 Hva kan KBO-enheter benytte skytjenester til?

3 Hva må KBO-enheter passe på ved bruk av skytjenester?

Skytjenester

- Databehandlingskapasitet levert over Internett
  - Lagring
  - Prosessorkraft
  - Samhandling
  - Konkrete tjenester
- Ulike leveransemodeller
  - SaaS, PaaS, IaaS
  - Public, Privat, Hybrid, Community



Fordeler

- Skalerbarhet og kapasitet
- Tilgjengelighet
- Økonomi
- God sikkerhet

Risikoer

- Digital sårbarhet
- Avhengighet av leverandør
- Sikkerhetspolitiske utfordringer

- Økende bruk av skytjenester
- Økende funksjonalitet
- De store blir større
- Fokus og satsing på cybersikkerhet
- Datasentre etableres lokalt, også i Norge

- Man snakker om «The energy cloud»
- Digital disrupsjon: Industri 4.0, IoT, AI, Big Data
- Økende behov for lagring og prosessering av data
- Investeringer i teknologi og kompetanse kan være risikofylt og kostbart, særlig for enkeltaktører

- Ingen spesifikk regulering av skytjenester
- GDPR, Schrems II, FFD-forordningen, fragmenterte nasjonale regler
- Økt fokus på digital sikkerhet
- Myndighetene stadig mer positive til skytjenester
- Nasjonal skyløsning?

Bruk av skytjenester i KBO-enheter

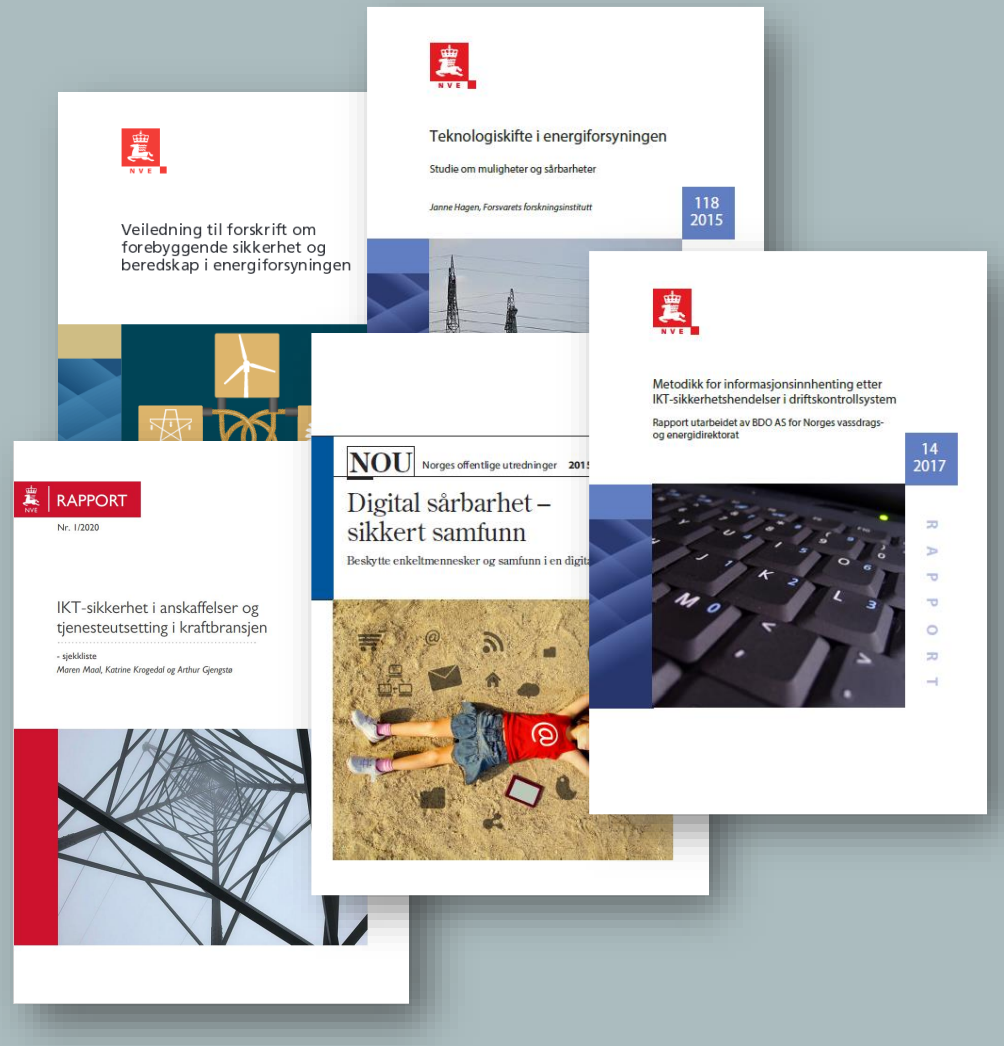
KBO-enhet: Virksomhet som er del av Kraftforsyningens beredskapsorganisasjon

Ingen konkret regulering av skytjenester i lov eller forskrift, verken generelt eller for KBO-enheter

Beredskapsforskriften: Begrenser i noen grad KBO-enheters bruk av skytjenester

- Geografi
- Sikkerhet
- Krav til systemdokumentasjon mv
- Kontroll med systemendringer
- Tilgangskontroll
- Drift og vedlikehold
- Tilsyn

Personvern: Ingen spesielle regler for KBO-enheter, men må hensyntas



Hva kan KBO-enheter benytte skytjenester til?

Informasjon

- Kraftsensitiv informasjon
  - Som hovedregel forbudt, men må vurderes konkret
  - Må lagres i EØS/NATO, med kopi i Norge
- Personopplysninger
  - Som hovedregel tillatt, på gitte forutsetninger
  - Utfordringer utenfor EØS
- Annen informasjon
  - Som hovedregel tillatt

Funksjon

- Driftskontrollsystemer (SCADA)
  - Som hovedregel forbudt
  - Tilgrensende/samhandlende systemer kan være problematisk
  - Kan endre seg med ny teknologi mv
- Andre systemer
  - Som hovedregel tillatt
  - Begrensninger for informasjon, ikke funksjon
  - DMS, ERP, BI, CRM, HRM, SCM, O365 osv

Hva må KBO-enheter passe på?

Bruk av skytjenester innebærer utkontraktering/tjenesteutsetting

Krav til risikovurderinger og dokumentasjon

- Type informasjon
- Type system
- Den aktuelle skytjeneste og leverandør
- Avhjelpende tiltak

Krav til kontrakt, anskaffelsesprosesser og oppfølgning

Krav til interne rutiner

Styret har ansvaret

Hør vår podkast!

Eivind Grimsø Moe

911 20 355
egm@hjort.no

Ola Hermansen

911 22 930
olher@hjort.no

Energisk

www.hjort.no/energisk

Apple Podcasts
Google Podcasts
Spotify

NVE

NORGES ENERGIDAGER 2021

DET STORE BILDET

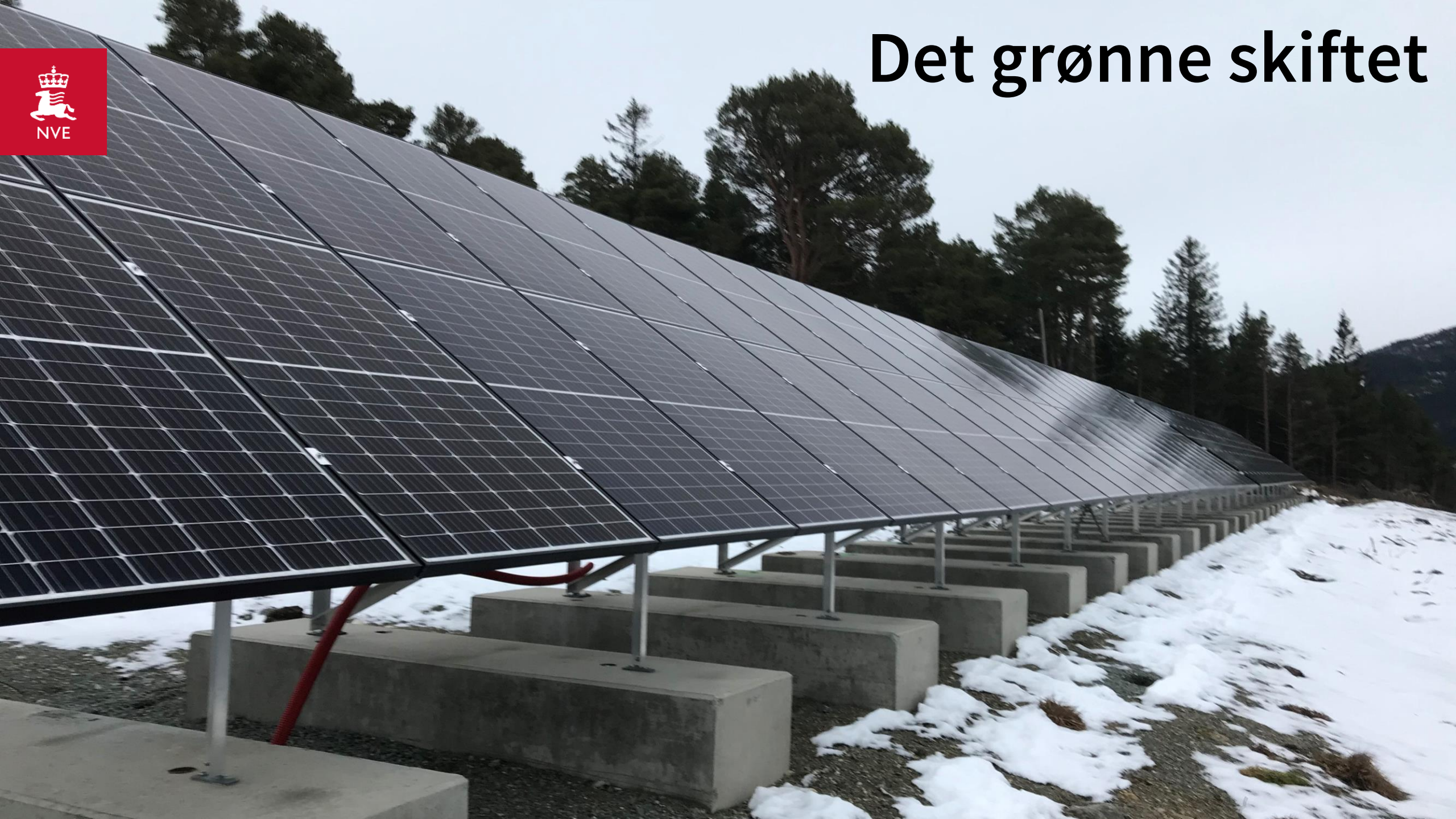
IKT-SIKKERHET: KRAVENE SOM STILLES TIL ENERGIBRANSJEN NÅ OG FRAMOVER

….kommer ikke bare fra oss men i økende grad fra EU

Janne Hagen og Øyvind Toftegård
NVE og RME

NVE 100 ÅR

Det grønne skiftet



NVE

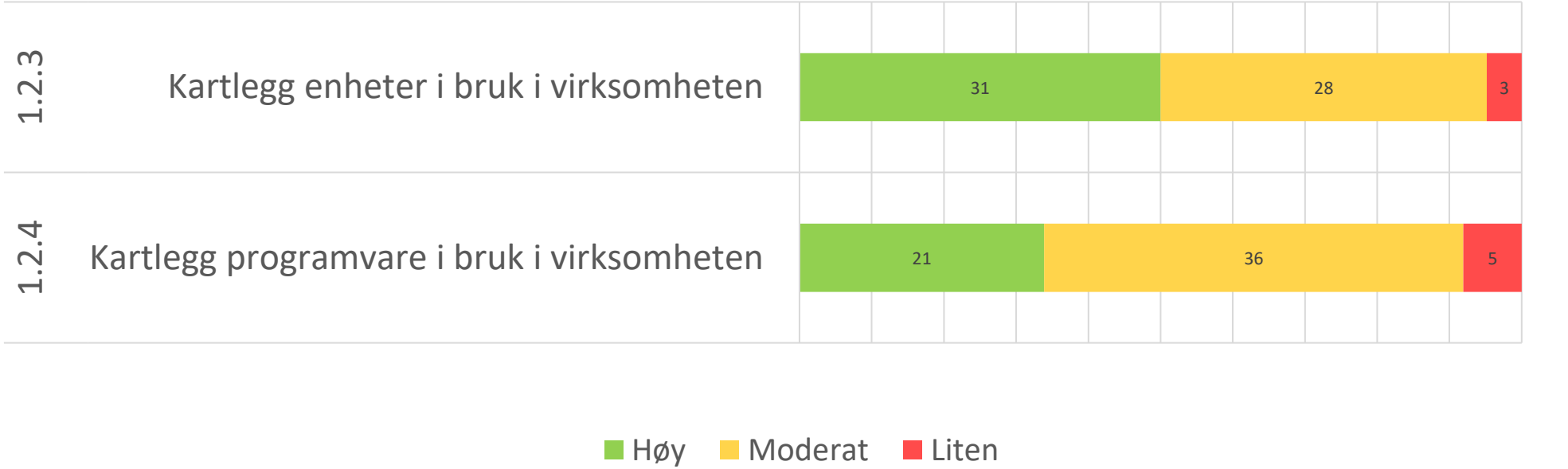

"During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface."
in ETL 2020
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

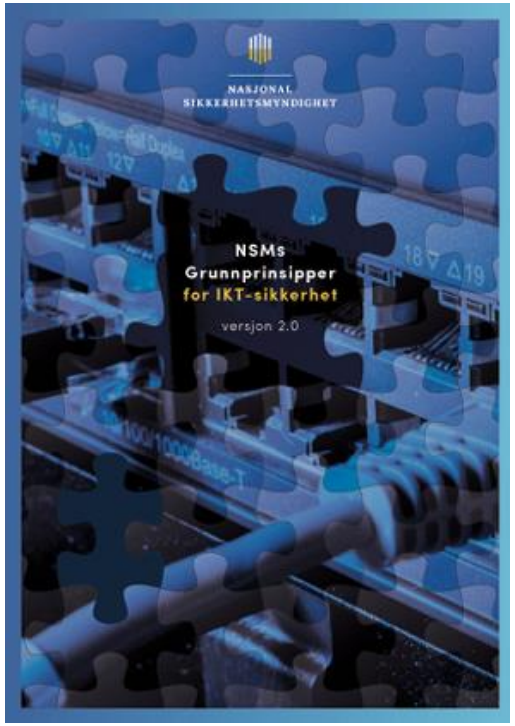
Oppdaterte krav til sikkerhet i AMS

Sikkerhetskrav for AMS i målepunkt knyttet til sluttbrukere i lavspennings-anlegg gjelder fra **1. januar 2022**.

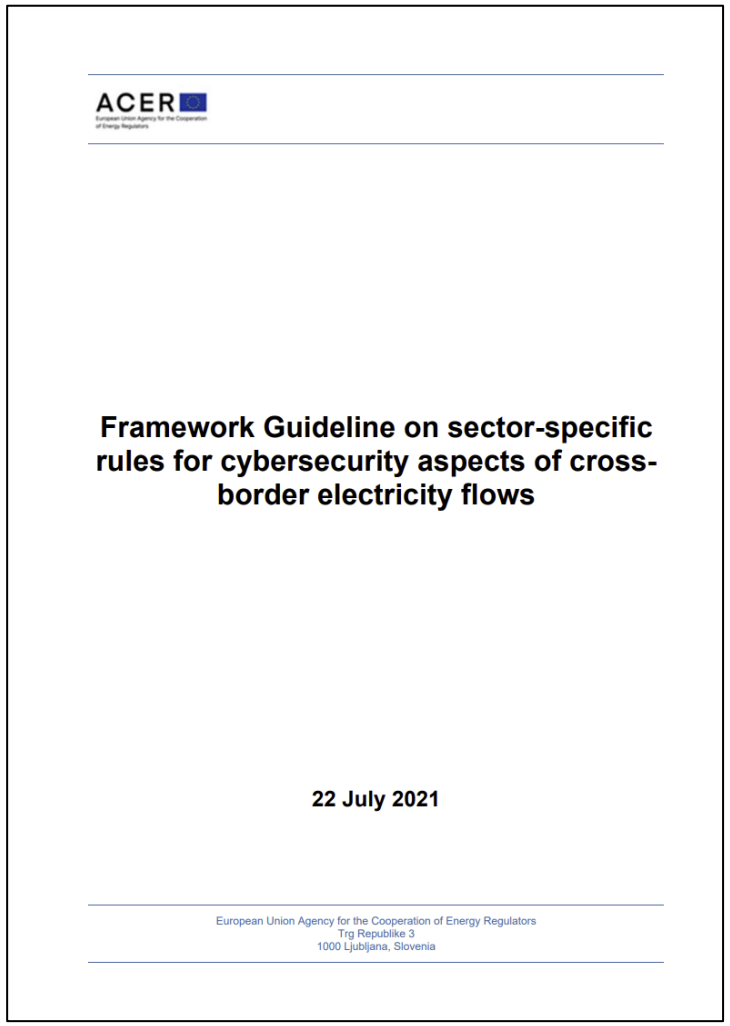
Sikkerhetskrav for AMS i andre målepunkt gjelder fra **1. juli 2023**.

Kraftberedskapsforskriftens krav til IKT-sikkerhet





EU-regulering og ACERs arbeid



ACER
European Union Agency for the Cooperation of Energy Regulators

Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

22 July 2021

European Union Agency for the Cooperation of Energy Regulators
Trg Republike 3
1000 Ljubljana, Slovenia

ACER
European Union Agency for the Cooperation of Energy Regulators

ec.europa.eu/

NVE

NORGES ENERGIDAGER 2021

DET STORE BILDET

SMARTE HUS OG ELEKTRISKE BILER

Krav til IKT-sikkerhet er nødvendig for framtidig driftssikkerhet

Takk for oss

Janne Hagen og Øyvind Toftegård

Foto: Navn Navnesen, NVE

NVE

NORGES ENERGIDAGER 2021

DET STORE BILDET

Sesjon 1

Digitaliseringssikkerhet i energibransjen

NVE 100 ÅR