Samfunnet er avhengig av strøm,
IKT-sikkerhet i kraftsektoren er viktigere enn noen gang

IKT-sikkerhet

Hovedbudskap

- Selskapene i fornybarnæringen setter IKT-sikkerhet høyt på agendaen og jobber med forebygging, hendelseshåndtering og kunnskapsdeling i samarbeid med hverandre, leverandørene, NVE, KraftCERT og Nasjonal sikkerhetsmyndighet (NSM).

Bakgrunn

- I sin risikorapport for 2020 slår NSM fast at Norges største sårbarhet er vår avhengighet av strøm, både i hverdagen og i driften av en rekke samfunnskritiske funksjoner.
- Kraftnæringen har lenge brukt digitale verktøy for å styre kraftsystemet, såkalt operasjonsteknologi. Ved introduksjonen av informasjonsteknologi har man kunnet koble disse styringssystemene i kraftsystemet til større nettverk, bl.a. for bedre drift. Men systemene er dermed også blitt tilgjengelige for angrep utenfra.

Nøkkeltall / Fakta

- Leveringssikkerheten for strøm er svært høy i Norge og var på 99,989% i 2019.
- Det er oftest uvær og snøvær som fører til avbrudd.

- Angrepet på Hydro i 2019 viser at produksjonsselskap kan bli utsatt for angrep, men det regnes som mer samfunnskritisk dersom et nettselskap blir utsatt for et angrep som gir avbrudd for sluttbruker.
- Nettselskapene i Norge har forskjellig kapasitet for å jobbe med IKT-sikkerhet og det er viktig med samarbeid mellom selskapene og leverandørene. Særlig de små avhenger av samarbeid med leverandør.
- I "Ren energi"-pakken har EU-kommisjonen bestilt et regelverk (nettkode) som skal sikre et felles nivå for IKT-sikkerhet. Det er viktig at dette regelverket blir en del av EØS-avtalen så snart som mulig. Energi Norge og våre medlemmer bidrar med innspill til at dette regelverket treffer så godt som mulig.

Mer informasjon

- NSMs risikorapport 2020: https://bit.ly/NSM-risiko-2020
- Energi Norge om kraftsystemet, sikkerhet og beredskap: https://bit.ly/kraftberedskap

13. oktober 2020

Energi Norge
Hele Norge på strøm