## Zero day (1/2)

Du sitter på jobb på regionssentralen. Kontrollsystemet gir varsel om feil et sted i nettet, og du blir satt på saken om å undersøke hendelsen og finne en løsning. Etter nærmere undersøkelser viser feilene seg å ikke ha rot i virkeligheten.

## Zero day (1/2)

Spm 1:
Hvikle årsaker mistenker du?

Spm 2:
Hva skulle tilsi at dette er et hackerangrep?

Spm 3:
Hvilke prosedyrer følges i dette tilfellet?

## Zero day (2/2)

Dette er et angrep IT-ekspertene ikke har sett før (Zero-day angrep), og flere ressurser satt på saken. Kontroll av systmet avslører at firmwaren i PLCene i nøkkelsensorenheter har blitt overskrevet, noe som gjør at informasjon om styring og kobling blir hentet ut og erstattet med feil data. Dette fører til at man ikke kan stole på verdiene kontrollsystemet gir.

## Zero day (2/2)

Spm 1:
Hvor langt må det gå før man må overvåke strømnettet manuelt?