Norsk helsenett
Helse- og kommuneCERT

# Passord og nettverkssegmentering i operasjonell teknologi

God passordhygiene og tydelig nettverkssegmentering reduserer sannsynligheten for og konsekvensene av cyberangrep.

## Passord

Svake passord er en av de vanligste inngangene for alvorlige cyberangrep, og kan utnyttes både via fjerntilgang og fra kompromitterte interne nettverkssoner. Svake passord og gjenbruk av passord gjør jobben mye enklere for en angriper som har fotfeste i OT-systemene og øker sjansen for et vellykket angrep.

## Segmentering

Et innbrudd i IT-nettverket kan spre seg til OT-systemene. Som regel skyldes dette mangelfull nettverkssegmentering.

## Anbefalinger - passord

**Bruk sterke og unike passord for alle systemer og tjenester. Dette inkluderer:**

- Følg passordanbefalingene våre
- Tilby og bruk passordhvelv
- Bytt alltid fabrikkpassord på OT-/IT-utstyr
- Sett passord på PLS

**Unngå delte brukerkontoer:**

Opprett personlige kontoer og unngå bruk av delte brukerkontoer

**Begrens administratorrettigheter til et minimum:**

Følg prinsippet om det minste privilegium. Brukere bør kun ha de tilgangene og rettighetene som er absolutt nødvendige for å utføre oppgavene sine.

**Bruk MFA, helst phishingresistent:**

Bruk multifaktorautentisering (MFA) der det er mulig. Denne bør være phishingresistent.

# Anbefalinger – segmentering

**Segmenter OT-nettverk:**

Segmenter vekk OT-nettverk fra kontornett og andre IT-nettverk. Ved høy modenhet bør Purdue-modellen følges.

**Begrens trafikk mellom nettverkssoner:**

Begrens trafikken mellom nettverkssoner til bare det som er strengt nødvendig.

**Sikre fjerntilgang:**

Sørg for at fjerntilgang til OT-soner er kontrollert og godt sikret. Fjerntilgangløsninger må sikres med MFA og tilgang bør begrenses til enkelte IP-adresser/IP-nett. MFA bør være phishingresistent.