CENTER FOR CYBERSIKKERHED

Beskyttelse af OT på vandværker

Dette er en kort guide til, hvordan vandværker kan komme i gang med at beskytte deres OT-systemer. Guiden kommer med anbefalinger til at sikre vandværker mod de mest udnyttede sikkerhedshuller, der bruges til cyberangreb på OT-systemer.

De mest udbredte sikkerhedshuller i OT-systemer er brug af standard-passwords og usikre fjernadgange. Nogle systemer er født med et standard-password, som let kan findes på internettet. Hvis det ikke bliver skiftet, kan hackere udnytte passwordet til at få adgang. Fjernadgang er muligheden for at arbejde med et system fra andre lokationer.

OT (Operational Technology) – OT dækker alle former for teknologi brugt til realtidsstyring, monitorering og indsamling af data i produktioner. På et vandværk er OT f.eks. PLC'er (programmable logic controller) og andre systemer, som bruges til at overvåge og styre processer i eksempelvis sensorer, pumper og ventiler.

Fire anbefalinger til at lukke de største sikkerhedshuller i OT-systemer

- **Brug stærke passwords til alle systemer.** Skift standard-passwords. Brug passwords på minimum 15 tegn og genbrug ikke passwords. Gem ikke passwords i Word-filer, noter eller lignende på computeren.

- **Brug sikker fjernadgang.** Hvis det er nødvendigt at arbejde med OT-systemer fra andre lokationer, så brug en sikker fjernadgang. Beskyt fjernadgangen ved at benytte en sikker VPN (Virtual Private Network). En VPN bruges til at sikre datatrafikken mellem afsender og modtager.

- **Brug flerfaktor-autentifikation.** Fjernadgang til kritiske systemer bør sikres med flerfaktor-autentifikation. Flerfaktor-autentifikation kan f.eks. være en kombination, hvor man både indtaster et password og efterfølgende skal godkende på en smartphone.

- **Implementér leverandørens anbefalinger for at sikre jeres systemer.** Leverandører tilbyder ofte løsninger til at sikre deres systemer.

Styrk derudover OT-sikkerheden med følgende anbefalinger

- **Få overblik over vandværkets mest kritiske systemer og adgangen til dem.** Et overblik giver viden om, hvilke systemer der er kritiske, hvem der skal have adgang til dem, og hvor det er særlig vigtigt at sikre sig mod angreb.

- **Segmenter vandværkets netværk.** Adskil OT-netværket fra resten af vandværkets netværk. Så bliver det eksempelvis sværere for hackere at få adgang til OT-netværket fra andre systemer.

- **Hold alle systemer opdateret.** Al software vil have fejl og sikkerhedshuller, som hackere kan opdage og udnytte. Løbende sikkerhedsopdateringer sørger for at lukke hullerne.

- **Hav logning på fjernadgange.** Ved at logge på fjernadgange kan man f.eks. se loginforsøg, der enten er fejlet eller foretaget på mistænkelige tidspunkter. Undersøg loggen for at få viden om angrebsforsøg mod fjernadgangen.

- **Hav et beredskab klar.** Sørg for, at alle ved, hvad de skal gøre i tilfælde af et cyberangreb, f.eks. hvornår og hvordan man afkobler internettet.

Få mere viden om grundlæggende cyberforsvar og håndtering af cyberangreb i CFCS' vejledning "Cyberforsvar der virker".

Få mere viden om passwords i vejledningen "Passwordsikkerhed".

Læs mere om cybertruslen mod vandsektoren i CFCS' trusselsvurdering (2025), der sammen med vejledningerne ligger på www.cfcs.dk.