Norsk helsenett
Helse- og kommuneCERT

Utstyrsoversikt, ansvar og rutiner for operasjonell teknologi

Oversikt er essensielt for utstyr i soner med operasjonell teknologi (OT).

Virksomheter har ofte ulike lokasjoner og nettverkssoner med systemer som kjører operasjonell teknologi (OT). Noen av systemene er nye og andre er eldre.

I tillegg til OT-systemer inneholder sonene også mer tradisjonelt IT-utstyr. IT-systemene er typisk levert av ulike leverandører, og forskjellige systemer brukes for styring og fjerntilgang.

Dette gjør det krevende å holde oversikt over infrastruktur som ligger i eller i tilknytning til OT-soner.

I dagens trusselbilde er en av de største farene at systemer kan nås fra internett, enten det er med vilje eller ikke.

Dette kan for eksempel være administratorgrensesnittet til en 4G-ruter, eller en fjerntilgangsløsning som ikke vedlikeholdes.

Tilgang medfører i verste fall løsepengevirus, nedetid eller misbruk av systemene. Det er derfor kritisk med en god oversikt over infrastrukturen som forsvares, enhetene i sonene og alle mulige veier inn.

Her er eksponeringer mot internett det mest risikable, men tilgang gjennom virksomhetens interne nettverk brukes også ofte av angripere.

En utstyrsoversikt er også viktig for operasjonell sikkerhet og essensiell for håndtering om en hendelse først inntreffer.

Ansvar og rutiner

Det må være definert hvem som har ansvar for drift, oppdateringer, sikkerhetskopiering og utfasing av alt utstyr. Dette kan være én person eller flere.

Det er virksomhetens ansvar å sørge for at utstyret driftes. Dette kan gjøres selv, eller avtalefestes med leverandør. Virksomheten må følge opp at det gjøres, uansett hvem som står for selve driften.

Utstyr som kan oppdateres og er kritisk for drift, samt utstyr med eksponeringer mot internett/andre interne nett i virksomheten, bør prioriteres i dette arbeidet.

Dette krever et samarbeid mellom de som jobber med både IT og OT, samt leverandørene virksomheten benytter seg av.

Hva er det viktig at vi gjør?

Oversikt over utstyr og rutiner for drift, sikkerhetskopiering og utfasing av utstyr er essensielt. Oversikten bør oppdateres regelmessig eller ved endringer. Følg anbefalingene nedenfor.

Kartlegg OT-soner
Etabler en oversikt over nettverkssoner med operasjonell teknologi (OT). Spesielt viktig er det å kartlegge og dokumentere alle mulige nettverksmessige veier inn i OT-sonen.

Etabler oversikt over IT- og OT-utstyr
Etabler en oversikt over IT- og OT-utstyret i OT-sonene. CISA har en god veileder for å utarbeide utstyrsoversikt for systemeiere av OT-systemer.

Avklar hvem som har ansvar for drift, sikkerhetskopiering og utfasing
Utstyret i OT-sonene bør ha ansvarlige for sikkerhetsoppdateringer på utstyr der det er mulig. OT-utstyr kan ofte ikke oppdateres på samme måte som IT-utstyr.

Det bør også tas sikkerhetskopier av utstyret, og man bør ha på plass rutiner for utfasing og fornying av gammelt utstyr.

Dersom leverandører har ansvar, bør ansvaret defineres gjennom avtale. Det er fortsatt virksomhetens ansvar å overse at dette gjennomføres

Etabler ansvarlige systemeiere for utstyret
Utstyret i OT-sonene bør ha ansvarlige systemeiere som overholder at systemene driftes iht. rutiner.

Etabler en oversikt leverandørtilganger
Etabler en oversikt over hvilke leverandører virksomheten benytter seg av inn mot OT. Kartlegg spesielt alle fjernaksessløsninger inn til OT-infrastruktur.

Virksomheten må ha kontroll på oppdaterings- og bruksstatus på fjerntilgang, og sørge for at sikre løsninger brukes. Ofte vil det enkleste være at man krever at leverandører bruker virksomhetens egen fjerntilgangløsning som følger virksomhetens policy. Dersom leverandøren følger policy, og oppdateringsstatus og brukslogger er tilgjengelig, kan dette også fungere.

Fjernaksessløsninger må sikres med multifaktorautentisering (MFA), og tilgang bør begrenses til enkelte IP-adresser/IP-nett. MFA bør være phishingresistent.