Norsk helsenett
Helse- og kommuneCERT

Overvåkning og logging i OT-nettverk

Sørg først for endepunktsmonitorering på utstyr i OT-nettverk som kan ha dette, og pass på alarmene følges opp. Jobb videre med å få på plass sentralisert logging.

Overvåkning

Overvåkning av hva som skjer i et OT-miljø er avgjørende for å kunne oppdage cyberangrep tidlig. Dette kan være med å begrense omfanget og skaden av angrepet.

For overvåkning bør man benytte endepunktsdeteksjon- og respons (EDR) eller tilsvarende løsninger. Det er mange systemer i OT-nettverk som ikke har muligheten til å kjøre slike agenter for overvåkning, så fokuset bør være å kjøre det på utstyr som arbeidsstasjoner og servere som kan benytte det.

Passiv overvåkning av nettverkstrafikk i OT-nettverk er ellers et effektivt tiltak for overvåkning, og påvirker ikke operasjonell drift.

Effekten av overvåkningstiltak er svært begrenset dersom alarmer ikke følges opp. Derfor bør alarmer samles sentralisert og følges opp av administratorer. Dette krever et godt samarbeid mellom IT- og OT-personell.

Logger

Logger er helt kritisk for å kunne finne ut av hva som har skjedd. Ved et cyberangrep gir logger muligheten til å finne ut hva angriper har gjort, og dermed få god oversikt over angrepet. Logger gir også stor verdi for feilsøking ved driftshendelser.

Dersom man ikke har logger er man helt blinde ved en hendelse. Det kan bli umulig å finne ut hva angriper har gjort, og hvordan de fikk tilgang til å gjøre det.

Generelt bør det samles inn logger både fra IT- og OT-endepunkter, samt fra nettverkstrafikk, som for eksempel fra en brannmur. Start med å innføre logging på de mest kritiske systemene, inkludert fjernaksessløsninger som gir tilgang til OT-nettverk, og bygg videre over tid.

For å effektivt kunne søke i og lagre logger over tid må loggene samles og sendes til en sentralisert loggserver. Hvis man ikke sentraliserer loggene vil en angriper kunne slette loggene lokalt på maskinene de har fotfeste på, og gjøre det umulig å spore handlingene deres.

Ofte er det leverandører som har installert servere og tilhørende programvare i OT-nettverk. I slike tilfeller må man samarbeide med leverandør slik at alarmer og logger overføres til riktig sted.

Logger og alarmer skal kun overføres ut av OT-nettverk. Åpninger som settes opp for det må være enveis, slik at det ikke er mulig å benytte de til å angripe inn mot OT-nettverk.

Anbefalinger

Installer endepunktsbeskyttelse på utstyr i OT-nettverk som kan ha det

Der det er mulig bør endepunktsdeteksjon- og respons (EDR) eller tilsvarende løsninger installeres. Utover dette kan tradisjonell antivirus brukes.

Passiv overvåkning av nettverkstrafikk i OT-nettverk er et svært godt supplement til endepunktsdeteksjon.

Følg opp alarmer som går i OT-sonen

Effekten av alarmering er svært begrenset dersom de ikke følges opp. Alarmer bør samles sentralisert og følges opp regelmessig av administratorer.

Samle inn logger fra OT-sonen

Logger bør lagres på en sentral loggserver. Start med tilgangslogger og logger fra de mest kritiske systemene og bygg videre over tid.

Vi anbefaler at logger tas bare på i to år. Se vår logganbefaling for tips til gode logger og arbeid med logger.