





Penetrasjonstest av OT-miljø

I dagens samfunn kobles flere og flere digitale enheter på internett, derfor er det svært viktig å sikre at dine mest kritiske systemer skjermes for en potensiell angriper. I de fleste tilfeller er det ikke mulig å utføre en IT-orientert penetrasjonstest av

OT-miljøer, da dette kan føre til driftsproblemer eller -brudd. En penetrasjonstest av OT-miljøer blir derfor alltid utført under kontrollerte former og i dialog mellom våre pentestere og anleggseier.

Under en penetrasjonstest og sikkerhetsgjennomgang av OT vil vi for eksempel teste:

-  Segmentering mot IT
-  Sikkerhetsovervåking av nettverk og endepunkt
-  Kartlegging av enheter
-  Analyse av nettverkstrafikk

-  Kommunikasjonsprotokoller
-  Autentiseringsmekanismer
-  Koblinger mot leverandører
-  Stresstest av systemer

Vi kan hjelpe dere å få oversikt over sikkerhetstilstanden til OT-systemene gjennom:

- Kartlegging av enheter (assets)
- Arkitekturgjennomgang
- Test av nettverkssegmentering
- Passiv analyse av nettverkstrafikk
- Stresstest av systemer før produksjonsigangsetting
- Gjennomgang av kommunikasjonsprotokoller
- Evaluering av autentiseringsmekanismer
- Evaluering av kommunikasjonsløsninger mot kontorsystemer og fjerntilganger