NATIONELLT CYBERSÄKERHETSCENTER
EN DEL AV FRA

# Operativ teknik

En särskilt utsatt del av organisationers teknikmiljöer.
Rekommendationer för beslutsfattare och organisationer.

## Operativ teknik – utmaningar i ett föränderligt cybersäkerhetslandskap

**Operativ teknik (OT) är det teknikområde som styr och övervakar fysiska processer och maskiner i industri och annan infrastruktur.**

OT har under en tid identifierats som en särskilt utsatt del av organisationers teknikmiljöer och många har idag brister i sitt systematiska cybersäkerhetsarbete.

I takt med att systemen blir allt mer integrerade och uppkopplade skapas nya möjligheter till effektivare drift. Samtidigt är de särskilt sårbara, eftersom de ursprungligen utformades för isolerade miljöer med fokus på tillförlitlig och långsiktig drift. Cybersäkerheten var inte prioriterad.

Uppkopplade OT-system är sårbara för utpressningsangrepp och andra verksamhetsstörande cyberangrepp. Den långa livslängden innebär att många system är föråldrade. Uppdateringar av programvara är en utmaning då det skapar driftsavbrott i produktionen. Dessutom använder systemen vissa äldre protokoll som ibland saknar grundläggande cybersäkerhetskontroller. Kombinationen av hög ålder och ökande komplexitet i systemsammansättning ökar också risken för felkonfigureringar och mänskliga misstag.

Konsekvenserna av lyckade angrepp mot OT-system kan bli produktionsbortfall, ekonomisk skada, fysisk skada om maskiner förstörs och andra störningar som även kan ge betydande samhällseffekter. Angrepp mot energisektorn eller vattenförsörjningen kan få konsekvenser för liv och hälsa eller skada vår miljö.

Organisationer saknar ofta en tydlig överblick över vilka enheter som ingår i deras OT-system, vilket försvårar prioritering av skyddsåtgärder. Det är också en utmaning att snabbt och effektivt stärka skyddet utan att påverka produktionen. Samtidigt driver digitalisering och automatisering en ökad sammankoppling av system, där nya tekniker som AI och molntjänster införs. OT-system integreras alltmer med den övriga it-miljön och exponeras därmed mot gränsytor som de ursprungligen inte var utformade för.

| IT (informationsteknik) | Livslängd | Fokus |
|---|---|---|
| Hanterar data, kommunikation och affärssystem, t.ex. datorer, servrar, databaser och molntjänster. | 3-5 år | Hanterar information, konfidentialitet viktigt (skydda informationen) |

| OT (operativ teknik) | Livslängd | Fokus |
|---|---|---|
| Styr och övervakar fysiska processer och maskiner i industri och infrastruktur. Exempel är SCADA-system, PLC:er (programmerbara styrsystem), industrirobotar, kraftnät, vattenreningsverk. | 15-30 år | Styra fysiska processer, tillgänglighet viktigt (skydda processen) |

NATIONELLT CYBERSÄKERHETSCENTER
EN DEL AV FRA

## NCSC:s övergripande rekommendationer

### Administrativa åtgärder

- Organisationens ledning har ansvaret för OT-säkerhetsarbetet.
- Säkerställ att det finns en uppdaterad hot- och riskanalys samt tydliga rutiner för tilldelning, ändring och borttagning av behörigheter. Ställ krav på OT-säkerhet vid inköp och upphandling, följ upp leverantörer och inkludera säkerhetskrav i systemutveckling, test, integration och driftsättning.
- Inför ett arbetssätt för säker upphandling och säkra leveranskedjor inom OT, samt säkerställ att det efterlevs.
- Dokumentera och underhåll en inventarielista över samtliga system och komponenter.

### Tekniska åtgärder

- Minska exponeringen av uppkopplade enheter genom att ha kontroll på vilka delar av miljön som är exponerad mot internet.
- Härda OT-systemen genom exempelvis brandväggar, autentiseringsåtgärder och säker lösenordshantering, samt hantera uppdateringar enligt organisationens arbetssätt för patchhantering.
- Säkerställ förmåga att detektera och logga säkerhetsavvikelser, händelser och incidenter. Loggning bör omfatta operativsystemhändelser (som omstarter och krascher), onormalt applikationsbeteende, okända eller obehöriga komponenter och programvaror, nya eller ohanterade sårbarheter samt verksamhetsspecifika avvikelser.
- Hantera incidenter i enlighet med organisationens arbetssätt för incidenthantering.

## Läs mer:


NCSC-SE, 10 rekommenderade säkerhetsåtgärder, www.ncsc.se/sv/cybersakerhet/10-rekommenderade-sakerhetsatgarder/

NCSC-UK, Secure connectivity principles for Operational Technology (OT), www.ncsc.gov.uk/files/ncsc-secure-connectivity-for-operational-technology.pdf

Myndigheten för civilt försvar, www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/cyberfysiska-system/

Cybersäkerhetskollen 2025, Myndigheten för civilt försvar, https://rib.msb.se/filer/pdf/31260.pdf



**Nationellt cybersäkerhetscenter (NCSC)** april 2026



**För mer information och kontakt**
www.ncsc.se och ncsc@ncsc.se