NATIONELLT CYBERSÄKERHETSCENTER
EN DEL AV FRA

Fördjupade råd och rekommendationer för skydd av OT-miljöer

OT-relaterade enheter, oavsett om det rör sig om så kallade PLC:er[1] eller datorer med HMI-mjukvara[2], bör betraktas som icke uppdaterade och därmed sårbara. De ska skyddas utifrån denna utgångspunkt. Detta beror dels på att leverantörers säkerhetsuppdateringar ofta är fördröjda, dels på att det i vissa branscher inte är tillåtet att uppdatera underliggande operativsystem, exempelvis på grund av certifieringskrav. Historiskt har det dessutom förekommit flera fall av hårdkodade standardlösenord i enheter och system.

Det är viktigt att förstå konsekvenserna av att en hotaktör tar över en OT-miljö. Ett sådant övertagande innebär i praktiken full kontroll över systemen och möjliggör därmed förstörande angrepp. Varje beslut som sänker säkerhetsnivån i miljön måste därför noggrant vägas mot de risker detta medför. Samtliga beslut bör dokumenteras och regelbundet omprövas, särskilt vid förändrad riskaptit.

Eftersom många OT-enheter är ganska statiska och inte tillåter större förändringar i mjukvara eller konfiguration, är det viktigt att kompensera för detta genom omkringliggande infrastruktur. Bristande loggning i en enhet bör exempelvis kompenseras med utökad loggning i närliggande system. Samtidigt bör den statiska karaktären i miljön utnyttjas, eftersom systemen är avsedda för ett begränsat syfte blir det enklare att definiera förväntat beteende. Detta möjliggör mer finkorniga skyddsåtgärder och detektionsregler, där avvikelser – i såväl program som nätverk – kan blockeras eller generera larm.

1. Begränsa exponeringen av OT-tillgångar mot internet

Tidigare angrepp mot OT-miljöer har möjliggjorts genom användning av etablerade nätverksskanningsverktyg, såsom Nmap eller OPENVAS, för att identifiera exponerade tjänster, exempelvis VNC-servrar och andra fjärråtkomstlösningar. OT-tillgångar ska inte exponeras direkt mot internet, och i möjligaste mån inte heller mot organisationens internetanslutna it-miljö. Säkerställ att OT-enheter och system skyddas av en strikt konfigurerad brandvägg och att fjärråtkomst endast tillåts via VPN.

Om VPN inte är möjligt att använda ska den dedikerade brandväggen framför OT-miljön vara mycket restriktiv och endast tillåta den trafik som är absolut nödvändig, baserat på specifika IP-adresser, portar och protokoll. Geoblockering, där åtkomst begränsas till IP-adresser från exempelvis en viss nation, utgör inte ett tillräckligt skydd.

Om OT-miljön är åtkomlig från organisationens övriga it-miljö bör skyddet dimensioneras utifrån antagandet att it-miljön förr eller senare blir kompromitterad. Samma restriktiva principer som ovan ska därför tillämpas även i detta fall. OT-enheter och system bör inte heller tillåtas initiera utgående anslutningar mot internet, annat än när det är absolut nödvändigt. I de fall internetkommunikation krävs bör denna styras via en proxy som begränsar åtkomst till specifika och godkända resurser.

2. Konfigurera system för att minska angreppsytan

Även om möjligheterna att ändra konfiguration i OT-system ofta är begränsade bör de säkerhetshöjande åtgärder som är möjliga alltid genomföras. Utgå inte från att standardinställningar innebär en hög säkerhetsnivå. Genomför istället en systematisk genomgång av inställningarna och fatta medvetna riskbaserade beslut. Där det är möjligt bör skydd mot skadlig kod, till exempel anti-virus eller EDR[3], installeras. Vid osäkerhet är det bättre att initialt konfigurera sådana skydd för övervakning

och larm, utan att blockera aktivitet. Observera att många antivirus och EDR-lösningar kräver anslutning till en central server. Detta kan i sin tur skapa oönskade kopplingar mellan it- och OT-miljöer och därmed öppna en angreppsväg, exempelvis genom övertagande av OT-miljön från konsolen för antivirus/EDR.

3. Säkerställ stark autentisering och robust lösenordshantering för OT-tillgångar

Granska särskilt inbyggda konton och standardlösenord, och säkerställ att dessa ändras eller inaktiveras. Undersök även möjligheten att justera behörigheter för konton. Målsättningen bör vara att samtliga konton tilldelas så låga behörigheter som möjligt. Där det är möjligt bör stark autentisering användas, exempelvis flerfaktorautentisering. Om detta inte är genomförbart bör åtkomsten till relevanta gränssnitt istället begränsas på nätverksnivå, så att autentisering endast kan ske från specifika och godkända källor. Om lösenord används ska de vara starka och unika för varje enhet. Detta minskar risken att en angripare, som fått tillgång till en enhet, kan använda samma inloggningsuppgifter för att få åtkomst till ytterligare system.

4. Nätverkssegmentera mellan OT- och it-nätverk

Nätverkssegmentering är en central åtgärd för att begränsa konsekvenserna av ett intrång. Om ett system angrips kan segmentering försvåra för en angripare att komma vidare i nätverket och nå andra system. Säkerställ därför att kommuniktionsmöjligheter mellan it- och OT-miljöer hålls på en minimal nivå. Trafiken ska styras genom restriktivt konfigurerade brandväggar som endast tillåter den kommunikation som är nödvändig, baserat på specifika behov.

Direkta nätverksanslutningar mellan it och OT bör, om möjligt, undvikas. Säkerställ att exponering och dataflöden sker via proxyfunktioner eller så kallade push-/pull-lösningar. Ett exempel är att OT-miljön lämnar av information till en delad filyta i gränsen mellan miljöerna, varifrån it-system hämtar data vid behov. Direkta anslutningar från it till OT bör endast tillåtas som en sista utväg, och då under mycket kontrollerade former (se även punkt 5). Givet att det är förekommande att även VPN-lösningar kan innehålla sårbarheter som kan utnyttjas av angripare bör sådana enheter placeras i dedikerade nätverkssegment. Trafik till och från dessa segment bör filtreras noggrant och övervakas kontinuerligt.

5. Övervaka och samla in data om trafik mellan OT- och övriga nätverk

Implementera nätverksövervakning i gränsytan mellan OT-miljön och andra nätverk. Brandväggar i denna gräns bör som huvudregel logga både tillåtna och blockerade anslutningar (se även punkt 1). Okända eller avvikande anslutningsförsök, både in och ut från OT-miljön, bör generera larm och följas upp. Säkerställ att nätverksloggar sparas under en tillräckligt lång tidsperiod och att de är lättillgängliga för analys. Överväg även att samla in och analysera metadata (exempelvis i form av Netflow eller Zeek-data), för att möjliggöra effektiv detektion och spårbarhet. Vid behov av fördjupad analys kan fullständig trafikinsamling (full packet capture, PCAP), användas.

Utgående trafik från OT-miljön bör övervakas särskilt noggrant för att upptäcka avvikelser. Detta kan exempelvis indikera att ett system blivit angripet och kommunicerar med externa så kallade C2-system (Command and Control) för att ta emot instruktioner eller skadligkod[4].

6. Implementera och öva incidenthantering i verksamheten

Öva incidenter i OT-miljön, det kan vara särskilt viktigt att öva scenarier där drift behöver upprätthållas genom manuell hantering. Erfarenheter från tidigare incidenter visar att varningssignaler ofta har funnits, men inte hanterats. Säkerställ därför att det finns tydliga rutiner för att ta emot, prioritera och hantera larm samt att dessa rutiner är kända och efterlevs i praktiken.

1. Programmable logic controller, styrsystem som används för att automatisera och styra processer och maskiner.
2. Human-Machine Interface, teknik för människors interaktion med maskiner och automatiserade system.
3. Endpoint detection and response, säkerhetslösning för att övervaka och skydda enskilda enheter.
4. För vidare läsning, se NCSC rapport Cybersäkerhet i Sverige 2024 avsnitt 7.

Nationellt cybersäkerhetscenter (NCSC) april 2026

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