CENTER FOR CYBERSIKKERHED

Håndtering af industri-kontrolsystemer

Vejledning fra Center for Cybersikkerhed om sikring af industrielle kontrolsystemer.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave oktober 2019.

Forsideillustration: Nostal6ie/Getty Images.

Digital styring og overvågning af fysiske processer

Digitale komponenter anvendes ofte til at overvåge og styre både anlæg og udstyr i brancher som bl.a. tele, energi, vand og transport. Disse digitale komponenter indsamler informationer, der bruges til automatisk behandling eller formidles og præsenteres for en bruger på struktureret vis. Brugeren kan på baggrund af præsentationen iværksætte handlinger eller opsætte regler, så systemet kan reagere på bestemte input og eventuelt automatisk iværksætte nogle simple handlinger. Det samlede overvågnings- og styringssystem kan være relativt enkelt, som f.eks. et system, der overvåger ventilationen i en bygning. Mere komplekse systemer overvåger en lang række processer, og kan fremvise et billede af en stor mængde informationer. Det kan fx være et system, der overvåger et kraftværk eller vandsystemet i en by.

Denne vejledning beskriver syv skridt til at opnå bedre sikkerhed i digitale overvågnings- og styringssystemer. Skridtene er beskrevet generelt, så den enkelte kan omsætte rådene til konkrete handlinger på baggrund af kendskabet til egne systemer, netværk og organisation. De syv skridt er prioriteret i den forstand, at hvert skridt i nogen grad er en forudsætning for de videre skridt. Disse syv skridt skal ses som et tillæg til den almene it-sikkerhed organisationerne har implementeret. For en vejledning i almen it-sikkerhed henvises til *Cyberforsvar der virker*, der tidligere er udgivet af Center for Cybersikkerhed.

De syv skridt er:

1. Overblik over det eksisterende system
2. Politikker og procedurer
3. Awareness og uddannelse af systembrugere
4. Segmentering af netværk
5. Adgangsstyring
6. Komponenterne i systemet
7. Overvågning og hændelseshåndtering

Vejledningen bygger på en række internationale vejledninger, best practices og guidelines. Vejledningen indeholder en beskrivelse af de processer og den styring, der med fordel kan implementeres i forbindelse med anvendelsen af digital overvågning og styring af fysiske processer.

Center for Cybersikkerhed (CFCS) har udgivet en supplerende vejledning, der vedrører de overordnede overvejelser vedrørende sikkerheden i denne type systemer. Denne vejledning er møntet på de faglige ledere, der har ansvaret for sikkerheden i ICS, SCADA-systemer eller IOT-komponenter. Vejledningen indeholder ikke konkret instruktion i teknisk opsætning af udstyr, men fokuserer på hvordan man styrer og arbejder med sikkerheden i systemer, der integrerer IT og OT.

Industrikontrolsystemer anvendes som betegnelse for systemer der styrer, overvåger og kontrollerer. I denne vejledning anvendes begrebet som dækkende over både SCADA og ICS.

SCADA (Supervisory Control and Data Acquisition) er en betegnelse for det samlede it-system, der styrer, overvåger og analyser data i realtid, for at fremvise det for en operatør. Traditionelt har SCADA-systemer bestået af sensorer og styringskomponenter, hvis input og output blev analyseret og koordineret i et lukket netværk, med det formål at kontrollere en specifik og afgrænset proces. Et SCADA-netværk er det netværk som forbinder de komponenter, der udgør det samlede SCADA-system.

Begrebet **ICS** (Industrial Control System) kan anvendes som betegnelse for it-systemer eller elementer heraf, der overvåger og kontrollere enkelte OT-systemer. ICS er et bredere begreb end SCADA og kan dække for alle former for digital overvågning og styring af fysiske systemer.

IoT-komponenter er sensorer eller styringskomponenter, der forbindes direkte til et overordnet netværk som for eksempel internettet (heraf Internet of Things, IoT), hvor data analyseres og anvendes i en eller flere fysiske processer. **IIoT-komponenter** er Industrielt (I) anvendt IoT-komponenter, der i industrielle miljøer varetager overvågning eller styring. Disse kan være integreret eller tilknyttet et SCADA-system.

OT dækker over Operational Technology, der er de fysiske systemer, der overvåges eller styres af ICS eller SCADA. Samarbejde og afgrænsning mellem IT-systemer og OT-systemer kan foretages på mange måder, og ICS eller SCADA-systemer kan støtte eller styre OT-systemer.

1. Overblik over det eksisterende system

Et overblik over systemet har betydning for, hvilke tiltag der er mulige at foretage. Overblikket muliggør, at man med simple midler kan gøre netværket væsentligt mere sikkert, da systemets angrebsflader og basale sårbarheder bliver tydelige. For eksempel kan man blive opmærksom på åbne adgange, der ikke længere benyttes.

Identificer alle forbindelser til netværket
Forbindelser til netværket skal identificeres, således at alle gateways og tilkoblinger samt deres funktion beskrives. For at kunne foretage denne identifikation skal systemets netværk defineres og afgrænses, så alle forbindelser, såvel internt som eksternt erkendes. Forbindelser, der anvender offentlig tilgængelig kommunikationsinfrastruktur, så som internettet, indebærer en særlig risiko, og disse bør som minimum klarlægges. Foruden direkte forbindelse fra netværket til internettet, kan der være forbindelser til et virksomhedsnet med produktionsovervågning eller forbindelser til brug for serviceteknikere, der anvender internettet som infrastruktur. Man skal ved kortlægningen være opmærksom på midlertidige forbindelser, der kun er i funktion under service og konfiguration. Det er vigtigt at have fokus på sådanne forbindelser og udarbejde procedurer for anvendelsen af dem.

Fjern forbindelser til netværket, der ikke er absolut nødvendige
Enhver forbindelse til netværket udgør en potentiel angrebsflade. Hvis man skal bruge data fra netværket i andre systemer, bør man sikre, at forbindelsen mellem de to systemer er beskyttet med relevante tekniske tiltag. Hvis man har brug for at tilgå data fra netværket, kan der etableres et data warehouse i et separat netværkssegment. Industrikontrolsystemet leverer data til data warehouse, som stiller data til rådighed for aftagere. Dermed minimeres forbindelserne til netværket til det nødvendige. Der bør endvidere være etableret procedurer for håndtering og overvågning af forbindelsen.

Evaluer de forbindelser som er nødvendige til netværket
Foretag penetrationstest og sårbarhedsanalyse af de forbindelser, der forbinder industrikontrolsystemet med andre netværk. De sårbarheder, der bliver blotlagt i den forbindelse, kan herefter sikres med de relevante tiltag så som firewalls, systemer til detektion af netværksindtrængen (IDS) eller andre tekniske sikkerhedsløsninger.

Fjern eller afbryd unødvendige services

De services, man har aktiveret for at betjene, opdatere eller analysere driften af systemet, kan ligesom andre forbindelser give utilsigtet adgang til industrikontrolsystemet. Dermed udgør de en angrebsflade. Services, der ikke anvendes, men alligevel er aktive, bliver ofte ikke overvåget. Det anbefales, at man har et tæt samarbejde med leverandøren under gennemgangen af services, da leverandøren ofte vil have værdifuld indsigt i systemet. Såfremt man finder behov for at tildele fjernadgang i forbindelse med service, anbefales det, at der foretages en risikovurdering af hver fjernadgang, samt at man anvender en fysisk mekanisme for tilslutning, hvor det er muligt. En fysisk mekanisme kan f. eks. være kabler, der fysisk skal tilkobles i forbindelse med serviceeftersynet.

Stol ikke på, at leverandørspecifikke protokoller alene kan beskytte systemet

Nogle systemer bruger leverandørudviklede protokoller internt i netværket og til kommunikation med leverandørspecifikke løsninger udenfor industrikontrolsystemet. Sikkerheden i et leverandørudviklet system består i, at protokollen kun er kendt af udbyderen (omtales ofte som security by obscurity). CFCS anbefaler ikke, at sikkerheden i et industrikontrolsystem baseres på denne form for sikkerhed, da der er en række uhensigtsmæssigheder:

A. den begrænsede udbredelse medfører, at der er færre brugere til at opdage kompromitteringer og sårbarheder, som kan deles med andre.

B. Det kan være vanskeligt at foretage hændelsesdetektion, systemgenopretning og oprydning i leverandørspecifikke systemer, da det forudsætter dyb systemforståelse.

C. Man bliver afhængig af enkelte medarbejdere eller leverandører, der har udviklet og har indgående kendskab til systemet.

2. Politikker og procedurer

Det er væsentligt at etablere klare politikker og procedurer for industrikontrolsystemer, så ansatte, konsulenter og leverandører forstår sikkerhedsniveauet i systemet. Disse skal bero på et grundigt udarbejdet overblik som beskrevet i trin 1 med tilhørende kontroller. De klare politikker og procedurer kan sammenkædes med it-politikker for almindeligt kontor-it, dette indebærer dog en udfordring, da der kan være væsentlige forskelle i sikkerhedsbehovet, sårbarhederne og håndteringen af kontor-it og industrikontrolsystemer.

CFCS anbefaler, at der udvikles særskilte procedurer for anvendelse, vedligeholdelse og betjening af industrikontrolsystemer.

I forbindelse med udviklingen af politikker og procedurer, bør man undersøge, om der allerede findes en relevant sikkerhedsstandard. Til inspiration kan anvendes IEC-62443/ISA99, der adresserer nogle generelle problematikker inden for cybersikkerhed omkring industrikontrolsystemer. Når man udarbejder politikker, foreskriver IEC 62443, at man medtager nogle basispunkter:

- Klar definition af hvilket system der er genstand for politikken (hvilke enheder, forbindelser, o.s.v.)
- Hvor er systemet placeret (f.eks. en fysisk adresse)
- Hvilke typer af systemer der er omfattet
- Hvordan politikkerne adresserer de forskellige roller medarbejderne varetager i virksomheden
- Hvilket ansvar der hviler på de ansatte i forhold til at efterleve politikkerne
- Konsekvenser for ikke at efterleve politikkerne
- Eventuelle fjernadgange specificeres særskilt
- Bærbare medier
- Patch management
- Anti-virus management
- Change management
- Backup og restore
- Incident response

3. Awareness og uddannelse af systembrugere

Det er vigtigt at uddanne de brugere, der har adgang til systemerne. Brugerne skal uddannes i systemet, således at de kan anvende det korrekt, men de skal også uddannes i sikkerhedsprocedurerne, så de kan anvende dem og forstå, hvorfor man har opstillet disse sikkerhedskrav.

I erkendelse af, at brugerne kan udgøre en væsentlig sikkerhedsrisiko, er det vigtigt, at de har forståelse af de politikker og procedurer, som de konkret anvender i dagligdagen. På trods af grundig uddannelse ved etablering af systemer og modtagelse af nye medarbejdere, skal der med passende intervaller afholdes efteruddannelse. Uddannelsen kan suppleres af awareness-kampagner, der enten er rettet mod en større gruppe af medarbejdere, eller specifikke risici, da personalet over tid kan glemme politikker og procedurer. Indholdet i såvel uddannelse som awareness-kampagner skal løbende opdateres, da truslerne mod systemerne, sikkerheden og sårbarheder i systemerne udvikler sig.

Det er væsentligt, at awareness-kampagner og uddannelsen passer til virksomheden. Derfor forudsætter uddannelsesplanlægning viden om forretningen og opgavefordelingen på tværs af virksomheden. Brugerne bør kun undervises i brug af relevante politikker og procedurer for deres område. Der bør være awareness- og uddannelsestiltag målrettet eksterne, der skal servicere systemkomponenter. Deres rettigheder og adgange bør endvidere begrænses mest muligt og kun være aktive under udførelsen af service i overensstemmelse med trin 1. De centrale procedurer for fjernadgang bør gennemgås ved hver awareness-kampagne. Niveauet i uddannelsen bør tilpasses jobfunktion og roller.

Træning og øvelse i krisehåndtering og beredskabsprocedure er en vigtig del af uddannelse og awareness. Øvelser skal sikre, at alle involverede handler hensigtsmæssigt i krisesituationer, herunder bør der være et særligt fokus på, at træne ledernes viden og styringskompetencer i en krise. Alle medarbejdere skal imidlertid have forståelse af krisehåndteringsmekanismerne og forstå, hvordan de anvender relevante tiltag under en krise. Beredskabstiltag, hvor systemer segregeres eller styres manuelt, bør afprøves og trænes jævnligt, således at alle relevante medarbejdere er fortrolige hermed.

4. Segmentering af netværk

Segmentering af netværk giver meget sikkerhed for begrænsede midler. Formålet med at segmentere netværket er at skabe to eller flere uafhængige miljøer, således at en angriber, virus eller malware ikke har adgang til hele netværket samtidig. Derudover giver segmentering mulighed for implementering af forskelige sikkerhedsprocedurer og tekniske tiltag i forskellige segmenter på baggrund af det enkelte segmentets kritikalitet. Der kan henvises til ANSI/ISA-99, der beskriver zoner og forbindelser nærmere.

Den mest banale segmentering er mellem industrikontrolsystemet og kontor-netværket. Typisk opsættes der kontroller på forbindelsen mellem de to domæner til at mitigere forskellen i sikkerniveauer og behov. Der opstår derfor to separate sikkerhedszoner, da der er forskellige regler og adgangsstyring på de to områder.

CFCS anbefaler, at man ved valg af segmentering anvender disse fire skridt:

1. Identificer grupper af komponenter eller netværk, som har et forretningsmæssigt behov for at kommunikere.
2. Vurder om der er behov for yderligere opdeling i sikkerhedszoner i de forretningsmæssige fællesskaber betinget af forskellige sikkerhedsbehov.
3. Definer de forbindelser mellem sikkerhedszoner, der er nødvendige for at tilgodese forretningsbehovet.
4. Etabler og vedligehold et overblik, således at der kun er én forbindelse eller ét punkt for dataudveksling mellem forskellige segmenter eller sikkerhedszoner.

Efter at have valgt segmenteringen kan man gå i gang med at vurdere, hvordan forbindelserne beskyttes bedst, herunder valg af tekniske tiltag, opsætning af jump-stations, demilitariserede zoner, lognings- og detektionsmekanismer. Backup og systemgenoprettelse bør have en særlig overvejelse i forbindelse med segmentering. Som udgangspunkt bør backup opbevares i separate netværk.

5. Adgangsstyring

Efter opdelingen af systemerne i segmenter eller sikkerhedszoner i Trin 4, skal der etableres både fysisk og logisk adgangskontrol mellem dem.

Fysisk adgangskontrol er f.eks. hegn om virksomheden, adgangssystemer og nøgler til låse og skabe. Logisk adgangskontrol er brugerrettigheder, der giver adgang til netværk og systemer. Det er vigtigt at have flere sikkerhedsniveauer for både den fysiske og logiske sikkerhedskontrol, så der kan iværksættes de rette beskyttelsestiltag uden at vanskeliggøre det daglige arbejde unødigt. Det er vigtigt at beskytte adgangen til industrikontrolsystemet, så man ikke kan få adgang til systemet via en fjernadgang med begrænset beskyttelse, som eksempel en VPN-forbindelse med en simpel certifikat-struktur. Da der kan være behov for adgang fra kontor-it til industrikontrolsystemet, og behov for fjernadgang til kontor-it, er det vigtigt, at der er etableret sikkerhed i flere lag.

Det bør overvejes om der meningsfuldt kan etableres datadioder, der sikrer, at data kun bevæger sig ud af udvalgte systemer men ikke ind. Etablering af datadioder forudsætter segmentering i netværksarkitekturen som nævnt under skridt 4, der dog begrænser muligheden for en samlet adgangsstyring på tværs af segmenter og sikkerhedszoner.

Adgangskontrol såvel fysisk som logisk kræver, at man identificerer, hvem der skal have adgang til hvilken ressource og med hvilke privilegier, og evt. på hvilke fysiske systemer adgangen skal gælde. Adgangen bør være rollebaseret, så man alt efter placering i organisationen får forskellig adgang til systemerne. Det er vigtigt, at man sikrer, at medarbejderne kun har de adgange, der er nødvendige. Der findes mange tekniske løsninger, men det vigtigste er identifikation af medarbejderne, identifikation af nødvendige grupper, beskrivelse af nødvendige procedurer samt definition af alarmer og logning. Ved identifikation forstås en løbende proces, således at adgang fjernes, når medarbejdere afgår, og opdateres ved ændrede roller mv.

Ofte udnytter hackere ubeskyttede eller simple passwords til at få adgang til systemer. Det anbefales derfor, at der udarbejdes en password-politik. Center for Cybersikkerhed har udarbejdet en vejledning om passwords.

6. Komponenterne i systemet

Komponenterne i systemet skal så vidt muligt hærdes. I lighed med sikkerhedsforanstaltninger i det samlede system skal angrebsfladen mindskes og sårbarhederne begrænses lokalt på komponenterne. Nye komponenter er ofte udstyret med sikkerhedsfaciliteter, som bør aktiveres i videst muligt omfang. På flere ældre produkter, der fortsat er aktive, er der ikke nogen indbyggede sikkerhedsfaciliteter. Det medfører, at der skal etableres politikker og procedurer og tekniske tiltag. Ved anvendelse af ældre komponenter, der ikke kan hærdes lokalt, bør der desuden tages de nødvendige skridt til at sikre udstyret i arkitekturen ved bl.a. segmentering.

Det anbefales, at man prioriterer sikkerhed ved anskaffelse af nyt udstyr til introduktion i et ICS-netværk, hvad enten det er IOT-devices eller klassiske SCADA-komponenter.

Nyt udstyr bør have mulighed for opsætning af komplekse passwords. CFCS password-vejledning indeholder nærmere anbefalinger til passwords.

Konfigurationen af netværksudstyret er også vigtig. Generelt skal man lukke netværksporte, som ikke bruges, og tilsvarende skal services på netværket, som ikke benyttes, lukkes. Kun essentielle services, som er nødvendige for driften af anlægget, skal være tilgængelige. Dette medfører, at alle komponenter løbende skal kortlægges og dokumenteres, således at det er muligt at overskue, hvilke services, der er knyttet til hvilke processer og komponenter som beskrevet i trin 1.

Generelt skal adgangen til at tilslutte udstyr til industrikontrolsystemet begrænses så vidt muligt. USB-lagermedier eller en bærbar pc, som kobles på i forbindelse med opdateringer, fejlsøgning eller service, udgør en risiko for malware. Man kan i den forbindelse overveje at etablere og benytte en datadiode til at isolere et netværk, som kun behøver at sende data ud. Det er væsentligt, at regler, der skal beskytte komponenterne også kan forstås og efterleves. Derfor forudsætter opsætning af fysisk beskyttelse med tilhørende regler ofte en sikkerhedsforståelse hos medarbejderne.

7. Overvågning og hændelseshåndtering

Det er lige så vigtigt at kunne opdage og håndtere, at netværket er kompromitteret, som det er at forebygge kompromittering. Derfor er det nødvendigt at skabe et overblik over forsøg på angreb på netværket.

Netværkskommunikationen særligt ind og ud fra industrikontrolsystemet bør monitoreres, således at anormaliteter kan registreres. Der findes mange systemer og produkter, der kan foretage denne monitorering og præsentere dem for operatørerne. Fælles for dem er, at det er opsætningen af alarmer, der definerer evnen til at opdage anormaliteter. Det er vigtigt, at der løbende foretages en opdatering og revidering af opsætningen af monitoreringssystemet. Derved kan nye trusler, IOC'er (indicators of compromise) og driftsforhold løbende indarbejdes. Et eksempel kan være et system, der overvåger og styrer driften af varmeproduktionen i en proces. Dette system vil fungere på en anden måde, hvis processen ændres efter et nyt forretningsbehov, så temperaturen og trykket i den fysiske proces øges. Man må forvente, at en forretningsmæssig ændring kræver en opdatering af moniteringssystemet, da systemet måske vil begynde at levere datapakker af en anden størrelse eller hyppighed, der afspejler et ændret driftsmønster.

Det kan være nødvendigt at monitorere netværkstrafikken på udvalgte knudepunkter i netværket for at opdage mulig ondsindet trafik mellem enhederne på netværket. Monitorering bør som minimum foregå på alle punkter, hvor industrikontrolsystemet er forbundet med andre netværk. CFCS anbefaler, at systemer har mulighed for, at overvågningsloggen gemmes lokalt i mindst 90 dage.
Monitorering kan foregå ved hjælp af logning i kombination med værktøjer til at systematisere og kategorisere de forskellige typer hændelser. Der bør altid etableres et normalbillede. Det vil sige, hvordan enhederne kommunikerer med hinanden ved daglig drift. Logning skal blandt andet fokusere på at opdage unormale forsøg på autentifikation (login) eller unormal netværkstrafik.

Alle ændringer af brugerrettigheder bør registreres ved logning med henblik på at opdage forsøg på at eskalere en brugerkontos rettigheder.

Monitorering kan også foregå ved hjælp af et Intrusion Detection System (IDS), som på baggrund af kendte angrebstyper kan opdage potentielt ondsindet aktivitet.

Hændelseshåndtering
Organisationen skal have et beredskab for at håndtere sikkerhedshændelser. Sådan en plan bør omfatte, hvilke parametre der kan betyde, at en hændelse skal eskaleres til et højere beredskab – eller eskaleres ned. Planen bør ligeledes omfatte opgaver og roller i forbindelse med at udrede sikkerhedshændelsen.

For industrikontrolsystemer er nedetid ofte kritisk. I sådanne tilfælde bør det være en prioritet at have en genoprettelsesplan parat. Planen bør omfatte tiltag for at sikre netværket mod yderligere kompromittering, hvilket eksempelvis kan være at frakoble forbindelser til andre netværk. Det kan også omfatte blokering af brugerkonti, inklusive systemkonti, som bruges af enheder og tjenester på netværket, samt skift af passwords på alle konti. Planen bør også inkludere, at der altid er off-line medier til rådighed med den nødvendige software til en geninstallation af softwaren på udstyret, hvis det er nødvendigt.

CFCS anbefaler, at genoprettelsesplanen opstiller kriterier for at kunne konstatere, om netværket er sikkert.

Det kan eksempelvis være en komplet scanning efter isolation af netværket og geninstallation af software. Det bør i denne sammenhæng bemærkes, at det ofte er vanskeligt at garantere sikring af et netværk, der har været kompromitteret. Genoprettelsesplaner skal i lighed med beredskabsplaner trænes jævnligt, således at der opbygges fortrolighed med planerne og tilhørende procedurer samt evt. udstyr ved de medarbejdere, der forventes at agere i særlige situationer.

Foruden den løbende monitorering, bør der jævnligt gennemføres interne tilsyn med sikkerheden i systemerne. I forbindelse med it-revisioner, bør man inddrage industrikontrolsystemet som et aktiv, der auditeres ud fra egne procedurer, risiko- og sårbarhedsvurderinger, overblik og politikker.

Ved interne tilsyn bør hele systemet indgå. Det vil sige, at det også inkluderer alle komponenter på forskellige fysiske adresser, der har forbindelse til systemet. Man kan i den forbindelse vælge at udføre penetrationstest af systemet, dets forbindelser eller specifikke delkomponenter, samt foretage en gennemgang af de løbende risikovurderinger, overblik og politikker.

Referencer

Center for Cybersikkerhed og Digitaliseringsstyrelsen (2016): *Cyberforsvar der virker*

Center for Cybersikkerhed (2016): *Passwordvejledning*

Department for Digital, Culture, Media and Sports, United Kingdom (2018): *Mapping of IoT Security Recommendations* Samt *Guidance and Standards to the UK's Code of Practice for Consumer IoT Security*

International Society of Automation (ISA): *Industrial Automation and Control Systems Security, ISA 99, ISA/IEC 62443*

National Institute of Standards and Technology, Department of Commerce, United States (2015): *Guide to Industrial Control Systems (ICS) Security*

National Cybersecurity and Communications Integration Center, Department of Homeland Security, United States (2016), *Seven Steps to Effectively Defend Industrial Control Systems*