Myndigheten för samhällsskydd och beredskap

VÄGLEDNING

Grundläggande säkerhet i cyberfysiska system

Grundläggande säkerhet i cyberfysiska system

Enhet: Enheten för säkerhet i cyberfysiska system/
Avdelningen för cybersäkerhet och säkra kommunikationer

Produktion: Advant

Publikationsnummer: MSB1880 - december 2021
ISBN: 978-91-7927-213-5

Förord

Elförsörjning, dricksvattenförsörjning, hälso- och sjukvård och transporter är exempel på samhällsviktiga verksamheter. Ett avbrott eller svår störning i en samhällsviktig verksamhet kan leda till att en allvarlig kris inträffar i samhället. Många av de processer som behövs för styrning och övervakning av den infrastruktur som ingår i samhällsviktig verksamhet är beroende av cyberfysiska system. Med cyberfysiska system menas gränssnittet mellan en digital miljö och en fysisk process. Ett cyberfysiskt system kan antingen vara ett industriellt informations- och styrsystem eller ett IoT-system (eng. Internet of Things).

MSB:s tidigare publikation ”Vägledning till ökad säkerhet i industriella informations- och styrsystem[1]” har etablerats till en form av branschpraxis för arbetet med cybersäkerhet inom dessa typer av samhällsviktig verksamhet.

Vi har tagit fram den här vägledningen för möta den allt snabbare digitala utvecklingen och minska gapet mellan cybersäkerhetsarbete och cyberhot. Vägledningen är tänkt att utgöra ett konkret stöd för dig som arbetar inom en samhällsviktig verksamhet. Vi hoppas också att den ska bidra till att öka medvetenheten om behovet av säkerhet i cyberfysiska system. Vägledningen kommer att publiceras på MSB:s digitala plattformar.

Stockholm i december 2021

Åke Holmgren, avdelningschef

Enheten för säkerhet i cyberfysiska system/
Avdelningen för cybersäkerhet och säkra kommunikationer
Myndigheten för samhällsskydd och beredskap

1. Vägledning till ökad säkerhet i industriella informations- och styrsystem (MSB718 – juli 2014).

Innehåll

Introduktion

Introduktion

I princip all verksamhet använder i någon form cyberfysiska system för interaktion mellan, och styrning av, maskiner, fordon och annan utrustning, samt för inhämtning av data från omgivningen. Med cyberfysiska system menas flera typer av datorbaserade styrsystem, däribland industriella informations- och styrsystem (eng. Industrial Control Systems, ICS).

Traditionellt har dessa system varit fysiskt isolerade och byggda på specialutvecklad teknik. De består av till exempel ställdon som omvandlar styrsignaler till fysiska händelser i maskinen, fordonet eller apparaten de är kopplade till. Systemen kan också bestå av sensorer för insamling av data om omgivningen, exempelvis temperatur, varvtal eller flöde, för att använda i styrprocessen.

Cyberfysiska system blir allt mer uppkopplade och integrerade med andra it-system. Integrationen med andra it-system görs oftast i syfte att effektivisera verksamheten. Detta medför ökad exponering mot internet, och andra nätverk, vilket medför att de cyberfysiska systemen i allt större utsträckning utsätts för samma hot som de traditionella it-systemen.

Digitaliseringen ger en förändrad riskbild med ökad sårbarhet som bland annat beror på den ökade exponeringen mot andra nätverk och komplexiteten i integrationerna. Digitaliseringen gör att risken för oönskade händelser i cyberfysiska system ökar. Dessa händelser kan ge allvarliga konsekvenser såsom avbrott i samhällsviktig verksamhet, fysiska skador hos människor, förstörd utrustning, förlorad och förändrad information eller att information sprids till obehöriga.

Det är din egen organisation som har ansvar för att det ska finnas en tillräcklig och god säkerhet för den information och de informationssystem som finns i verksamheten. Glöm inte att detta även innefattar de cyberfysiska systemen.

Denna vägledning innehåller generella råd och rekommendationer som utgör stöd i den inledande processen av det systematiska informations- och cybersäkerhetsarbetet.

De generella rekommendationerna i denna vägledning går att använda inom alla verksamheter med cyberfysiska system. Rekommendationerna är uppdelade i två delar:

1. *Öka medvetenheten i hela organisationen om behovet av informations- och cybersäkerhet i cyberfysiska system (fem rekommendationer)*
   Informations- och cybersäkerhet är verksamhetskritiska frågor och därför måste ledningens engagemang och ansvar tydliggöras i ett tidigt skede. Det är även viktigt att roller och ansvar inom verksamheten beslutas och att en god säkerhetskultur etableras och anammas i organisationen.

2. *Kartlägg verksamhetens enheter och säkerställ utbildning av personal (tre rekommendationer)*
   De delar av organisationen som arbetar med cyberfysiska system behöver i många fall öka sin kunskap om informations- och cybersäkerhet. Likaså behöver personal med ansvar att förvalta de traditionella it-systemen mer kunskap, och förståelse, om de cyberfysiska systemen och de begränsningar som den underliggande fysiska processen för med sig. Även personer som är inblandade i upphandling, anskaffning och verksamhetsplanering behöver utbildning i dessa frågor.

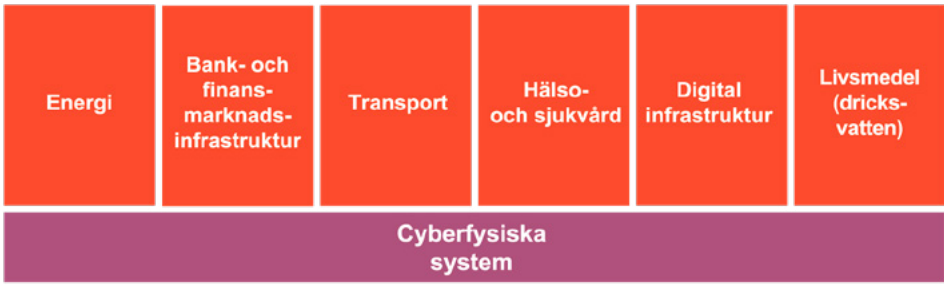
Alla rekommendationer och råd som finns i vägledningen bygger på branscherfarenheter, praxis och standardiserade arbetssätt. Vägledningen hänvisar till relevanta publikationer och källor inom området.

Bakgrund och läsanvisning

MSB:s arbete med uppdatering av ”Vägledning till ökad säkerhet i industriella informations- och styrsystem” (MSB718 – juli 2014) har resulterat i två nya vägledningar, en som behåller det tidigare namnet och denna med namnet ”Grundläggande säkerhet i cyberfysiska system”. Denna vägledning erbjuder stöd för att uppnå en högre cybersäkerhetsnivå för alla former av cyberfysiska system till skillnad från tidigare material som enbart fokuserar på industriella informations- och styrsystem.

Tack vare att vi publicerar vägledningen digitalt på webben har vi möjlighet att snabbare publicera och uppdatera våra rekommendationer. Det innebär att vi bättre kan möta den digitala utvecklingen och de önskemål om stöd som finns från målgruppen. Figur 1 visar inom vilka sex områden vi kommer ta fram rekommendationer och stödmaterial för informations- och cybersäkerhet i cyberfysiska system.

Vi inleder här med en introduktion till begreppet cyberfysiska system och ger därefter åtta konkreta rekommendationer kring grunden för det systematiska arbetet för ökad informations- och cybersäkerhet inom cyberfysiska system.



Figur 1. Denna vägledning kommer fokusera på att möta behovet inom dessa sektorer.

Syfte, målgrupp och upplägg

Syftet med vägledningen är att, genom råd och rekommendationer, stödja samhällets aktörer i sitt arbete med informations- och cybersäkerhet inom området för cyberfysiska system. Detta ska leda till bättre cybersäkerhet i miljöer som hanterar cyberfysiska system. Målet är att öka samhällets förmåga att skydda mot och förebygga it-relaterade störningar och incidenter, samt öka medvetenheten om risker och sårbarheter mot cyberfysiska system.

Vägledningen riktar sig till dig som påverkar utformningen och införandet av informations- och cybersäkerhetsåtgärder hos aktörer med cyberfysiska system. Rekommendationerna är även till nytta för dig som arbetar med design, underhåll eller övervakning av cyberfysiska enheter.

MSB planerar att även publicera ytterligare rekommendationer som vänder sig till respektive samhällssektor (se figur 1) samt mot specifika områden som exempelvis IoT, molntjänster och leveranskedjor. Allteftersom vi identifierar ytterligare behov av stöd kommer vi ta fram fler publikationer och främst publicera dem på MSB:s webbplattformar.

Del A
Cyberfysiska system – en översikt

Cyberfysiska system – vad är det?

Cyberfysiska system är gränssnittet mellan den digitala och den fysiska miljön och är datorbaserade system för interaktion med maskiner, fordon och annan utrustning, inklusive sensorer som kan inhämta data från omgivningen. Idag är cyberfysiska system vanligt förekommande i en stor mängd processer i alla typer av samhällsviktiga verksamheter, exempelvis i drift av vattenkraftverk, distribution av fjärrvärme, kontroll av växlar i tågsystem, styrning av trafikljus, röntgensystem, robotkirurgi och fastighetsautomation.

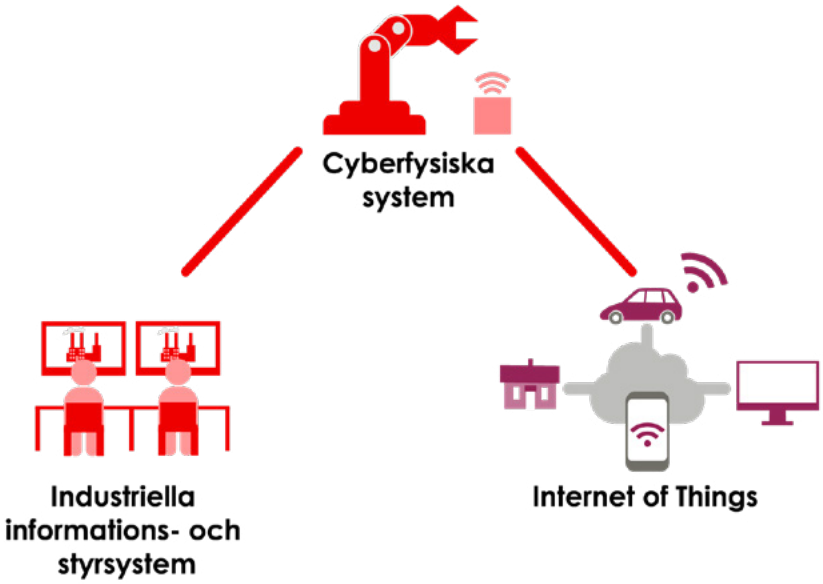
Cyberfysiska system kan bestå av många olika typer av enheter: små sensorer, inbyggda system, eller enheter som är byggda av sådana komponenter som finns i traditionella datorer. I systemen ingår också trådlös- och trådbunden kommunikation.

Ett cyberfysiskt system som ska övervaka en fysisk process kan i huvudsak bestå av följande funktioner:

1. En sensor som kan rapportera den fysiska processens läge (t.ex. flödeshastighet eller temperatur).
2. En styrenhet som tar emot data från sensorn samt information från en övervaknings- och konfigurationsenhet.
3. En kommunikationslänk till övervaknings- och konfigurationsenheten.
4. Ett ställdon (t.ex. en ventil eller varvtalsregulator) som justeras utifrån styrsignalerna från styrenheten så att systemet hålls inom önskat tillstånd.

MSB delar in cyberfysiska system i två delar: Industriella informations- och styrsystem (ICS) och Sakernas internet (IoT).

1. Industriella informations- och styrsystem är ett begrepp som samlar flera typer av styrsystem, bland annat SCADA-system (Supervisory Control and Data Acquisition). Andra benämningar kan vara processkontrollsystem, processautomation, process-it, OT-system (operational technology), tekniska it-system, anläggnings-it, distribuerade kontrollsystem och inbyggda realtidssystem (RTE).
2. Internet of Things, IoT (sv. sakernas internet) definieras här som uppkopplade enheter och tjänster för mätning, övervakning eller system och enheter för styrning som kopplas samman med övriga informationsnätverk. Användning av dessa enheter och tjänster inom industrin benämns IIoT (Industrial Internet of Things).



Figur 2. Visualisering av Cyberfysiska system och dess två ingående delar: Industriella informations- och styrsystem samt Internet of Things.

Egenskaper hos cyberfysiska system

Digitaliseringen har medfört att de ICS, som tidigare varit isolerade, integreras med den allmänna it-miljön, till exempel affärssystem, e-post och webbservrar. Integrationen har inneburit att de risker, som finns i den allmänna it-miljön numera även kan påverka funktioner i ICS. Det är därför viktigt att vara medveten om följande:

1. De enklaste cyberfysiska systemen har utvecklats med fokus på tillgänglighet, kontinuitet och stabilitet baserat på mjukvara i hårdvara (firmware) och utan operativsystem eller med en avskalad och enkel version av ett operativsystem.
2. Vissa installationer i styrsystem medger inte avbrott med mindre än att processen stoppas. System, vars uppgift är att övervaka och styra processer i realtid, får i dessa fall inte störas ut eller förändras på ett sätt som innebär att systemet beter sig felaktigt.
3. Många system har en lång planerad livslängd, ibland långt över 15 år, och riskerar därför att bli föråldrade eftersom leverantören slutar att ge ut nya versioner och säkerhetsuppdateringar.

Det innebär att kontinuerlig uppdatering (eng. patching) av mjukvara inte kan genomföras på samma sätt som i den allmänna it-miljön och att sårbarheter inte kan hanteras med säkerhetsuppdateringar. Enheter som görs tillgängliga, direkt eller indirekt, via internet, eller baseras på sådan hård- och mjukvara som vanligtvis återfinns i traditionella it-system, blir extra utsatta eftersom sårbarheter i sådana upptäcks regelbundet och därför kan utnyttjas av angripare under lång tid.

Många cyberfysiska system är starkt beroende av nätverk eftersom händelser och mätvärden måste skickas (och tas emot) vid exakta tidpunkter för att koordinera kritiska processer. Systemen har därför höga krav på tillförlitlig

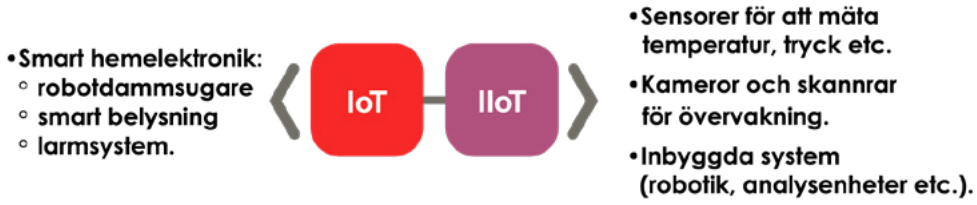
och snabb överföring av data mellan olika systemkomponenter och enheter. Tidigare användes seriell kommunikation i stor utsträckning för processnära komponenter men idag tillämpas ofta IP-kompatibla nätverksprotokoll, och det blir allt vanligare att enheter kommunicerar med trådlösa protokoll.

Särskilt om Internet of Things

Internet of Things, eller sakernas internet som är den svenska översättningen, är ett begrepp som används för att beskriva system eller enheter för fysiskt mätande, avläsande eller påverkande via interoperabla protokoll, ofta implementerade i inbyggd elektronik, och som sammankopplas med informationsnätverk. IoT-enheter har vanligtvis begränsad beräkningskraft, strömförsörjning och liten möjlighet att ändra på inbyggd programvara. Enheterna kan vara framtagna med fokus på stort antal till lågt pris och att de ska vara enkla att ersätta.

Det är inte ovanligt att IoT-enheter saknar krav på att fungera under lång tid och därför saknar möjlighet till mjukvaruuppdatering eller implementering av nya säkerhetsåtgärder. Det är viktigt att vara medveten om att IoT-enheter ofta utvecklats utan fokus på säkerhetsaspekten, något som gjort dessa enheter till attraktiva mål att angripa för att exempelvis använda enheterna i botnät. Då IoT-enheter kopplas samman via informationsnätverket kan sårbarheterna i IoT-enheterna påverka hela it-miljöer och de cyberfysiska systemen.

I denna vägledning ligger fokus på IoT-enheter som används inom industrin, IIoT. Både IoT och IIoT är koncept som beskriver enheter med likartad karaktär och utformning, men de används i olika syfte och miljö. IoT-enheter som exempelvis används för privat bruk är exempelvis smart hemelektronik och smart belysning. Med IIoT-enheter avses sådana som används inom industrin i syfte att underlätta i produktionen, övervaka leveranskedjor och varuhantering.



Figur 3. Exempel på enheter inom IoT och IIoT.

Systematiskt informationssäkerhetsarbete är viktigt

I princip behöver all information skyddas på något sätt. I vissa fall behöver informationen skyddas extra mycket, till exempel den i medicintekniska system eller i styrsystemen i kärnkraftverk. De konsekvenser som kan bli följden av bristande skydd är för allvarliga för att förbise.

Informationen skyddas utifrån principerna[2]

2. Observera att informationen i cyberfysiska system skyddas utifrån samma säkerhetsprinciper som it-system. Dock är oftast tillgänglighet och riktighet viktigast för att säkerställa funktion och säker drift när det gäller cyberfysiska system, till skillnad från IT-system där informationens konfidentialitet följt av riktighet ofta är viktigast.

- att den alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer kan ta del av den (konfidentialitet).

Alla säkerhetsåtgärder som införs ska skydda informationen utifrån någon av de tre principerna. Beroende på skyddsbehovet kommer vissa av dessa principer vara viktigare än andra. För cyberfysiska system tenderar tillgänglighet att vara viktigast följt av riktighet. Skyddet behöver givetvis anpassas efter behovet så att det är tillräckligt bra och inte för svagt eller alltför krångligt och dyrt.

Arbetet med informationssäkerhet omfattar att införa och förvalta säkerhetsåtgärder. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge lämpligt skydd åt organisationens information. Exempel på säkerhetsåtgärder:

- regelverk, exempelvis policyer och riktlinjer (organisatoriska)
- tekniskt skydd, exempelvis brandväggar och kryptering (tekniska)
- fysiskt skydd, exempelvis skal- och brandskydd (fysiska).

Grundläggande informationssäkerhetsutbildning för all personal är en viktig grund i säkerhetsarbetet. Målet är att höja medvetenheten om risker för att därmed minska antalet incidenter som beror på misstag och handhavandefel samt minska risken att bli utsatt för it-angrepp. För att lyckas med detta behöver informations- och cybersäkerhetsarbetet vara förankrat och ha ett engagemang hos organisationens ledning. Det är också viktigt att se informations- och cybersäkerhetsarbetet som något ständigt pågående, en kontinuerlig process, och inte som en engångsinsats.

Ett systematiskt arbete med informationssäkerhet leder till att ledning och medarbetare får en gemensam bild av vilka risker som finns och att de arbetar för att införa och följa de säkerhetsåtgärder som finns. MSB har tagit fram ett metodstöd som kan hjälpa verksamheter med det systematiska informationssäkerhetsarbetet. Detta metodstöd bygger på standarderna ISO/IEC 27001 och 27002, ”Ledningssystem för informationssäkerhet – Krav” respektive ”Riktlinjer för informationssäkerhetsåtgärder”. Det finns även standardserien ISA/IEC 62443 – ”IT-säkerhet i industriella automationssystem” som är mer inriktad mot cyberfysiska system.

Cybersäkerhet

Medvetenheten och kunskapen om it-angrepp är i många fall låg hos såväl utrustnings-, system- och programleverantörer som upphandlare och beställare. It-angrepp har tidigare inte varit ett reellt hot mot cyberfysiska system eftersom de inte varit uppkopplade och exponerade. Samtidigt är kunskapen om cyberfysiska system fortfarande låg hos de som arbetar med den allmänna it-miljön, vilket gör att det som skiljer de olika miljöerna åt inte alltid hanteras rätt:

- Cyberfysiska system ingår ofta i installationer med lång livslängd vilket gör att de innehåller tekniklösningar från flera generationer och där de äldsta inte nödvändigtvis var utvecklade med tanken att vara uppkopplade på ett delat nätverk.

- Cyberfysiska system har ofta krav på hög tillgänglighet vilket kan medföra svårigheter för snabba förändringar för att skydda mot nyupptäckta och kända säkerhetsbrister. Det kan innebära att det inte går att göra uppgraderingar, ändringar i inställningar eller utbyte av komponenter efter det att systemet tagits i drift.
- Skydd mot aktörsdrivna hot (angrepp) har ofta inte setts som en prioriterad fråga av leverantörer eller beställare vid utvecklingen av cyberfysiska system.
- De säkerhetsåtgärder som är vanligt förekommande i system i den allmänna it-miljön kan saknas i cyberfysiska system vilket gör att kompenserande åtgärder behöver införas istället.

Detta medför att kravställningen kan bli otillräcklig och att miljöer med cyberfysiska system inte utformas med tillräcklig skyddsnivå för skydd mot antagonistiska hot.

Att säkerheten i cyberfysiska system skulle vara hög på grund av att de är ovanliga, eller proprietära i sin konstruktion och konfiguration har ibland använts som argument för att de är säkra. Detta argument har alltid varit felaktigt. ICS har stor variation i sin konstruktion och konfiguration, vilket kräver ett stort engagemang av en eventuell angripare men det innebär inte att de inte kan bli angripna. På internet har dessutom mängden beskrivningar och kartläggningar av aktuella sårbarheter i olika cyberfysiska system, samt tydliga instruktioner för skapandet av skadlig kod ökat i takt med att ICS blivit mer attraktiva mål för angripare. Det finns även färdiga verktyg, ramverk och hjälpmedel för att utföra cyberangrepp.

Allriskperspektiv

Arbetet med informations- och cybersäkerhet inom cyberfysiska system är inte begränsat till antagonistiska hot. En mycket stor del av de incidenter som sker i cyberfysiska system beror på helt andra saker än antagonistiska hot. Det kan exemplevis bero på handhavandefel eller miljörelaterade orsaker så som översvämningar eller blixtnedslag. Det är därför viktigt att ha ett allriskperspektiv i de risk- och sårbarhetsanalyser som verksamheten genomför.

Organisatoriska, fysiska och tekniska säkerhetsåtgärder

För att effektivt kunna skydda information och de system som genererar, behandlar och reagerar på informationen så måste organisationen arbeta med organisatorisk, fysisk och teknisk säkerhet. I arbetet med informations- och cybersäkerhet kan dessa områden beskrivas enligt nedan:

- Organisatoriska – Det finns personal som har tid, kompetens och förmåga att arbeta med informations- och cybersäkerhet. Alla medarbetare i organisationen har en grundläggande förståelse för informationssäkerhet och de regelverk som gäller för organisationen.
- Fysiska – Informationstillgångar och system skyddas fysiskt från till exempel obehörigt tillträde, brand och vattenskador.
- Tekniska – Säkerhetsåtgärder som införs i it-miljön och den cyberfysiska miljön, till exempel autentisering, nätverkssegmentering, kryptering, filtrering av nätverkstrafik.

Alla tre områden måste samverka för att nå önskad skyddsnivå. Rekommendationerna i del B är uppdelade utifrån dessa tre områden.

Principen ”säkerhet på djupet”

För att öka säkerheten i de cyberfysiska systemen rekommenderar vi att säkerhetsåtgärder implementeras enligt principen ”säkerhet på djupet” (eng. defence-in-depth). Principen innebär att olika säkerhetsfunktioner överlappar varandra och att skyddet byggs i flera lager. Om en säkerhetsfunktion visar sig vara otillräcklig, ska andra säkerhetsfunktioner finnas som upprätthåller ett skydd, om än inte fullt ut, tills den fallerande säkerhetsfunktionen är åtgärdad.

Principen med säkerhet på djupet gäller även vid utveckling och förvaltning av IT-miljön. Hur miljöerna är utformade och integrerade avgör även vilka krav som ställs på åtgärder som måste införas för att få till säkerhet på djupet. Exempel på säkerhetsåtgärder som kan utgöra de olika lagren är nätverkssegmentering, nätverks- och klientbrandväggar, trafikfiltrerande proxys, nätverksbaserade detektions- (IDS) och skyddssystem (IPS) samt kontinuerlig övervakning.

Det är viktigt att vara medveten om skillnaderna mellan vilka åtgärder som går att vidta för att bygga upp cybersäkerhet inom it-miljöer och vilka som går att vidta för rent cyberfysiska miljöer. Att implementera en säkerhetsåtgärd kan vara olika svårt och ge olika effekter i en cyberfysisk miljö jämfört med en it-miljö. Exempelvis är det ofta enkelt att implementera och uppdatera ett antivirusskydd i en it-miljö, samtidigt som samma säkerhetsåtgärd i en cyberfysisk miljö är mycket riskfylld och kräver extra åtgärder för att implementeras. Om man inte vidtar extra åtgärder vid implementering kan exempelvis antivirusprogrammet placera viktiga filer i karantän eller ta för mycket beräkningsresurser i anspråk. Även själva separationen mellan de två miljöerna gör det svårare att regelbundet, eller automatiskt, uppdatera antivirusprogram i den cyberfysiska miljön.

Det är viktigt att säkerhetsarbetet omfattar hela organisationen och inte bara en specifik del som kan anses vara skyddsvärd. Risken om en enskild informationstillgång har ett lägre skydd är att en angripare kan använda detta lägre skydd för att initialt skaffa sig åtkomst till it-miljön och därefter successivt skaffa sig åtkomst till andra, mer värdefulla, informationstillgångar.

Säkerhet på djupet innebär arbete inom flera områden, exempelvis:

Säkerhetsarkitektur – Rekommendationer, policyer, procedurer.

Fysisk säkerhet – Fältelektronik, kontrollcenter, behörighet för fysisk åtkomst.

Nätverkssäkerhet – DMZ, nätverkssegmentering, trafikfiltrering.

Värdsäkerhet – Patch- och sårbarhetshantering, kryptering, fältenheter, virtuella maskiner och härdning.

Övervakning – Intrångsdetektering, loggning, incident och händelseövervakning.

Försörjningskedja av tjänster – Hantering av leveranskedjor, outsourcing och molntjänster.

Personal – Policyer, procedurer, utbildning och kunskap.

För att lyckas få de olika lagren på plats och uppnå säkerhet på djupet behöver organisationen kontinuerligt utgå från riskbedömningar och omvärldsbevakning.

Kontinuitetshantering

Många samhällsviktiga tjänster är beroende av cyberfysiska system. De flesta sjukhus förlitar sig på medicinisk utrustning som är digitaliserad. Inom transportsektorn är mycket av logistiken automatiserad, och laster och transporter koordineras utifrån digitaliserade arbetssätt. El- och vattenförsörjning är också starkt beroende av cyberfysiska system, både vid produktion och vid överföring. Fastighetsautomation är ytterligare ett område där cyberfysiska system är centralt, bland annat för övervakning och styrning av temperatur och ventilation.

Många av de säkerhetsåtgärder som vidtas för att hantera vardagliga händelser är även sådana åtgärder som behöver vidtas för att skydda verksamheten vid en eventuell kris, exempelvis vid stora samhällstörningar. Säkerhetsåtgärderna behöver vara införda innan en kris uppstår. De åtgärder som behöver prioriteras är mest sannolikt sådana som också identifieras i det kontinuitetsarbete som organisationen bedriver.

Ett avbrott eller störning kan komma att påverka möjligheten att exempelvis fjärrstyra processer, eller ge upphov till avbrott i tjänster som verksamheten är beroende av. Störningar i ICS kan i sin tur leda till att verksamhetens processer påverkas och i sämsta fall att anläggningen förstörs. För att skydda anläggningen kan det i vissa lägen vara motiverat att koppla bort den, eller till och med hela organisationen, från internet. Behövs det är det bättre att stänga ned verksamheten på ett kontrollerat vis istället för att stänga den abrupt till följd av en kris. Vid ett försämrat läge kan det vara mycket svårt att få stöd av konsulter, till exempel på grund av att andra organisationer har tecknat förtursavtal eller att personalen är krigsplacerad i en annan tjänst. Samtidigt kan det behövas mer personal om it-systemen kopplas ned och ICS-systemen ställs om till att kräva mer manuella handgrepp. Det är viktigt att verksamheten har planerat för att säkerställa resurser och åtgärder om denna situation skulle uppstå.

Kontinuitetshantering handlar om att planera för att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för. Exempel på störningar kan vara att personalen inte kommer till jobbet, lokalerna inte går att använda, leveranser av viktiga varor och tjänster inte kommer, it-systemen har slutat fungera eller att anläggningarna drabbas av strömavbrott.

Läs mer om kontinuitetshantering: https://www.msb.se/kontinuitetshantering

Del B
Rekommendationer

Rekommendationer

Rekommendationerna är uppdelade i två delar och innehåller råd på sådant som utgör grunden i en organisations systematiska informations- och cybersäkerhetsarbete. Mer specifika rekommendationer kommer att finnas i andra vägledningar som inriktas mot specifika sektorer och områden. För att underlätta säkerhetsarbetet är rekommendationerna kategoriserade utifrån tre olika delområden baserat på typ av åtgärd och var inom verksamheten de ska införas. Eftersom det ofta är olika roller som arbetar med olika typer av delområden är avsikten att kategoriseringen ska underlätta den interna dialogen.

Det finns inga färdiga recept för hur det systematiska informations- och cybersäkerhetsarbetet ska utformas. Det är verksamhetens behov som avgör vad som behövs. Det finns dock ett antal vedertagna arbetsmetoder och rekommendationer som rekommendationerna i den här vägledningen utgår ifrån.

Organisatoriska åtgärder
Organisatoriska åtgärder består av en organisations regelverk, policyer, rutiner, bemanning och arbetssätt. Syftet med denna typ av åtgärd är att exempelvis medarbetare ska erbjudas stöd och regler i sitt arbete för att säkerställa att det utförs på ett säkert sätt.

Fysiska åtgärder
Detta är åtgärder som fysiskt begränsar eller förhindrar åtkomst till it-system eller utrymmen där cyberfysiska system är placerade.

Tekniska åtgärder
Tekniska åtgärder består av hård- eller mjukvara samt konfigurationsinställningar vars syfte är att skydda it-system och cyberfysiska system.

Avsikten med att definiera säkerhetsåtgärder utifrån olika delområden är att underlätta dialogen inom organisationen eftersom det ofta är olika roller som arbetar med de olika delområdena.

Lägg grunden 1
Öka medvetenheten om behovet av informations- och cybersäkerhet

Lägg grunden 1

1.1 Säkra ledningens engagemang och ansvar för säkerheten

Typ av rekommendation, organisatoriska åtgärder

I dialog med organisationens ledning är det viktigt att förmedla de risker som uppstår om inte cybersäkerhetsarbetet tas på allvar. Ledningen behöver förstå dessa frågor och att riskerna med osäkra cyberfysiska system i förlängningen kan orsaka bland annat ekonomisk skada eller personskada. Det medvetandegörande arbetet kräver ett uthålligt pedagogiskt arbete och fokus bör ligga på att verksamheten blir bättre av höjd cybersäkerhet.

- Begär att få tid för korta presentationer vid ledningsmöten.
- Var väl förberedd och beskriv nyttan med fokus på cybersäkerhet.
- Undvik skrämselpropaganda och ge exempel på rimliga konsekvenser.
- Beskriv risker på ett konkret sätt och hur ni kan hantera riskerna genom säkerhetsåtgärder. Ge konkreta förslag på vad nästa steg är – till exempel en riskbedömning på en avgränsad del av de industriella informations- och styrsystemen.

I arbetet med att säkra ledningens engagemang är en viktig målsättning att säkerställa att de cyberfysiska systemen ses som ett viktigt område i organisationens övriga arbete med informationssäkerhet. Saknar organisationen ett sådant arbete behöver ledningen ge någon ansvar och mandat att ta fram detta.

Rekommendationer

- Jobba långsiktigt och försök få ledningen att intressera sig för säkerhetsarbetet och den nytta det gör för verksamheten.
- Beskriv vad olika åtgärder kostar – både i investering och i arbetstid. Relatera sedan kostnaden till den nytta som åtgärderna gör för verksamheten.
- Föreslå konkreta förändringar i verksamhetens styrdokument med målsättningen att ni ska ta hänsyn till de cyberfysiska systemen i det systematiska cybersäkerhetsarbetet
- Var tydlig med att ökad säkerhet inte enbart betyder tekniska åtgärder. Lägg fokus på hur effektiviteten kan förbättras i takt med ett ökat säkerhetsfokus.
- Använd konkreta exempel som ligger nära den egna verksamheten för att förklara vad cybersäkerhet i de cyberfysiska systemen innebär.
- Dokumentera ansvar och befogenheter samt uppdatera styrdokument kontinuerligt.

1.2 Tydliggör roller och ansvar för säkerheten

Typ av rekommendation, organisatoriska åtgärder

Det kan finnas skillnader i sättet att förvalta och genomföra förändringar i administrativa it-system och sådana som beskrivs som cyberfysiska system. I det förstnämnda kan det finnas roller såsom systemägare, objektsägare, informationsägare, förvaltningsansvarig, driftansvarig och systemadministratör.

I det sistnämnda saknas ofta dessa definierade roller. I vissa fall kan det exempelvis vara leverantörsrepresentanter som antar rollen som systemadministratörer.

En avsaknad av tydlig roll- och ansvarsfördelning riskerar att leda till att organisationen får dålig, eller ingen, kunskap om de cyberfysiska systemens egenskaper, dess konfiguration och om de cybersäkerhetsrisker som existerar.

Rekommendationer

- Se till att organisationens informationssäkerhetspolicy omfattar de cyberfysiska systemen. Se också till att tydligöra ansvarsfördelningen för säkerhetsfrågor.
- Samordna och definiera roll- och ansvarsfördelningen för de administrativa it-systemen och för de cyberfysiska systemen. Det bör tydligt framgå vilka system som verksamhetens centrala it-stöd förvaltar och vilka system som förvaltas lokalt ute i produktionen.
- Låt organisationens centrala it-stöd ansvara för den totala systemintegrationen för att skapa en sammanhållen syn på säkerhetsfrågor, trots att en del system förvaltas lokalt.
- Utse systemägare för de cyberfysiska systemen och dokumentera tydligt vilka krav som ställs på rollen.
- Det är viktigt att driftorganisationen äger sina informationssystem för att bland annat minimera risken att informationen placeras i en molntjänst utan att en riskbedömning genomförts.

1.3 Samverka i användarföreningar, standardiseringsorgan och andra nätverk för säkerhet.

Typ av rekommendation, organisatoriska åtgärder

Delta och samverka i olika nationella och internationella organisationer samt intressegrupper. Deltagandet kan medföra att det går att ställa högre, tydligare och mer samlade säkerhetskrav på leverantörer, systemintegratörer och applikationsutvecklare. Samverka i olika forum kan även ge dig vetskap om hot och risker innan de har orsakat problem för din egen verksamhet.

Att samverka genom användarföreningar, branschorganisationer, standardiseringsorgan och andra nätverk är ett ekonomiskt realistiskt alternativ för många små och medelstora användare och leverantörer.

Rekommendationer

- Samverka i användarföreningar, sociala nätverk och organisationer som kompetensutvecklar och stödjer medlemmarna i deras dagliga säkerhetsarbete.
- Se till att representationen dokumenteras och att aktiviteter som genomförs i respektive nätverk kontinuerligt avrapporteras till berörda medarbetare.
- Stäm av representationen med ledningen och motivera på vilket sätt deltagande i nätverken stärker säkerheten i verksamheten.

1.4 Inkludera säkerhetskrav från början i all planering och upphandling.

Typ av rekommendation, organisatoriska åtgärder

Säkerhetskrav behöver inkluderas från början i arbetet med systemspecifikationer och behovsanalyser. Det är svårare och dyrare att uppnå en godtagbar säkerhetsnivå i de cyberfysiska systemen i efterhand. Lägg därför särskild uppmärksamhet på säkerhetsfrågor vid kravställning inför anskaffning.

Säkerhetsaspekter måste tydligt framgå i upphandlingsunderlag, test- och överlämnandehantering, samt kontrakt och styrdokument för underhåll eller driftuppdrag. Upphandling kan omfatta såväl nyinstallation som hel eller delvis modernisering av befintliga lösningar. Säkerhetskrav bör ingå som en viktig del i alla leverantörsavtal, även i service- och underhållsavtal.

För vägledning se MSB:s publikation ”Upphandla Informationssäkert – en vägledning” (MSB1177 – november 2018).

I samband med moderniseringar av cyberfysiska system krävs en särskild hänsyn till cybersäkerhetsfrågor. Detta eftersom förändringarna med största sannolikhet kommer att påverka de befintliga systemen på ett sätt som de ursprungliga konstruktörerna inte hade tänkt på. Exempelvis är det ofta ett underförstått antagande i äldre industriella informations- och styrsystem att åtkomst till utrustning enbart kan ske via lokal fysisk närvaro. Idag är fysisk separation inte alltid möjlig vilket ställer höga krav på en logisk separation mellan olika delar av de industriella informations- och styrsystemen.

Rekommendationer

- Säkerställ att det finns dokumenterade rutiner för hur ni ska väga in säkerhetsaspekter vid anskaffning.
- Genomför riskbedömningar för att samla in krav på cybersäkerhet.
- Följ upp att leverantörerna lever upp till detaljerade krav på säkerhetsfunktioner i system och applikationer, exempelvis genom validering hos tredje part.
- Kräv att leverantörerna redovisar vilka egna metoder eller arbetssätt (exempelvis interna utvecklarhandböcker) de använder för att garantera kvaliteten på sitt säkerhetsarbete.
- Var noga med att leverantörer som får ta del av känslig information om de industriella informations- och styrsystemen skriver på och följer era sekretess- och säkerhetsavtal.
- Ställ krav på att driftsatt utrustning ska kunna testas på ett säkert sätt. En styrdator ska till exempel klara av den trafikvolym som uppstår vid ett penetrationstest.
- Ställ krav på att internetanslutning inte ska krävas för att: utrustning ska kunna installeras, uppdateringar laddas ned och installeras samt att licenser ska fungera.
- Genomför regelbundna uppföljningar för att säkerställa efterlevnaden.

1.5 Möjliggör en god säkerhetskultur och höj medvetenheten om behovet av säkerhet.	
Typ av rekommendation, organisatoriska åtgärder 	För att verksamheten ska lyckas uppnå och upprätthålla hög säkerhet i de cyberfysiska systemen krävs kunskap om cybersäkerhet, verksamhetens cyberfysiska system, samt de underliggande processerna. Cybersäkerhetsarbetet kräver därför ett tätt samarbete och förtroende mellan personer från olika yrkeskulturer med varierande säkerhetstraditioner och organisatoriska hemvister.
Rekommendationer	• Se över de organisatoriska säkerhetsrutinerna och säkerställ att medarbetare är medvetna om dess innehåll. För att uppnå systematisk informations- och cybersäkerhet behöver ni fokusera på både den organisatoriska, fysiska och tekniska säkerheten. • En person som får tillgång till de cyberfysiska systemen ska först ha genomgått lämplig utbildning. • Genomför regelbundet utbildning och träning av it-personal och ansvariga för de cyberfysiska systemens drift, samt avsätt tid och resurser för att olika delar av verksamheten ska kunna träffas och utbyta erfarenheter.

Lägg grunden 2
Kartlägg verksamhetens enheter och säkerställ utbildning av personal

Lägg grunden 2

2.1 Underhåll processer för systemkartläggningar och riskhantering

Typ av rekommendation, organisatoriska åtgärder

I organisationen behöver det finnas ett arbetssätt för att kartlägga informationsflöden, informationstillgångar och systemberoenden.

Det krävs en förståelse för vilka konsekvenser en felaktig funktion eller störning kan få. Det gäller både för den fysiska processen och för verksamheten övergripande. Förståelsen är en förutsättning för att kunna analysera verksamhetens processer för systemkartläggning och riskhantering, system och information samt för att kunna göra en riskvärdering samt klassificering över vilka system och vilken information som är verksamhetskritisk.

En dokumenterad verksamhets- och systemkartläggning visar åtkomst- och anslutningsmöjligheter, systemklassificeringar samt driftmässiga prioriteringsindelningar. Varje verksamhet bör ha en sammanställning över vilka cyberfysiska system som tillhandahålls. Sammanställningen ska vara tillräckligt detaljerad för att kunna identifiera kritiska komponenter och system. Rekommenderat innehåll är bland annat:

- IP-adresser och kommunikationsprotokoll
- versionsnummer
- uppgifter om operativsystem hos datorresurser
- tekniska uppgifter om lokala enheter såsom exempelvis PLC:er.

Varje komponent i systemdiagrammet rekommenderas ha en unik beteckning som pekar på en post i en konfigurationsdatabas. För att kunna fastställa den elektroniska säkerhetsperimetern måste alla anslutningar till de cyberfysiska systemen identifieras. Här ingår, förutom intranät, exempelvis fjärranslutna kopplingar till samarbetspartner, leverantörer och internet. Observera att alla trådlösa anslutningar bör behandlas som fjärranslutna punkter. Anslutningar till organisationens administrativa informationssystem (intranät) bör betraktas som externa anslutningar.

Rekommendationer

- Inventera organisationens tillgångar och identifiera de som är kritiska. Identifiera därefter de kritiska datorbaserade tillgångarna.
- Upprätta ett arbetssätt för hur och när riskbedömningar ska genomföras och dokumenteras. Välj riskanalysmetod utifrån analysens syfte och den tillgängliga informationen. Ta hänsyn till möjligheten att enkelt uppdatera riskbedömningar när ni väljer metod[3].
- Upprätthåll och skydda en konfigurationsdatabas. Konfigurationsdatabasen är viktig ur återställningssyfte i händelse av en incident.

3. För mer information om riskanalys, se MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

2.2 Säkerställ en systematisk förändringshantering

Typ av rekommendation, organisatoriska åtgärder

Att vara systematisk i hanteringen av förändringar ökar möjligheten att undvika störningar, onödiga felsökningar eller allvarliga problem. Det gäller alla typer av förändringar, till exempel en ny version av parametersättningar, inställnings- och datafiler eller program.

Det är särskilt viktigt med strikt kontroll och dokumentation av förändringar vid hantering av system och applikationer som din verksamheten planerar att använda under lång tid. Det bör finnas en formell dokumenterad process som talar om hur man får tillstånd att göra förändringar. Detta bör även gälla tillfälliga förändringar och förändringar av stödutrustning. Allt som inte är explicit tillåtet bör vara förbjudet.

Det är även viktigt att alla inblandade parter – leverantörer, systemansvariga och systemanvändare – har en korrekt och gemensam förståelse av den aktuella konfigurationen och driftstatusen hos verksamhetens cyberfysiska system.

Separata test-, utvecklings och driftmiljöer är vanliga när det gäller administrativa informationssystem. Tyvärr är det inte lika vanligt i cyberfysiska system. Det innebär att det är viktigt att lägga tillräckliga resurser på att upprätthålla en systematisk förändringshantering i dessa system.

Rekommendationer

- Uppgradera programvara stegvis. På grund av juridiska krav, såsom leverantörsavtal eller lagkrav, och tekniska krav bör ni göra det i samarbete med systemleverantörer.
- Säkerställ att den formella processen för förändringshantering omfattar:
  1. en beskrivning av vad som är belagt med tillståndskrav
  2. en procedur för att få tillstånd att göra förändringar
  3. en beskrivning av hur tester före och efter en förändring ska genomföras (inklusive en beskrivning av vilka förändringar som kräver tester i separat testmiljö)
  4. krav på hur dokumentation ska uppdateras efter förändringar
  5. krav på hur personal ska ta del av förändringar (exempelvis i vilka fall det krävs särskild utbildning av operatörer).
- Säkerställ att regler och rutiner som rör ändringar i de cyberfysiska systemen harmonierar med befintliga förändringsregler i fysiska processer eller anläggningar.
- Upprätta regelverk för hantering av verktyg (datorer/laptops) som används för uppdateringar av inställningar och program.
- Upprätta regelverk för hantering av de hård- och mjukvaruverktyg, till exempel kompilatorer och filöverföringsmetoder, som används i förändringsprocessen.
- Kontrollera enheter så att endast känd och verifierad systemprogramvara (firmware) används.
- Genomför differenskontroller mot tidigare versioner före och efter alla uppdateringar. Detta för att kontrollera att den nuvarande installationen inte blivit obehörigt modifierad och för att verifiera, validera och testa korrekt funktionalitet i den nya versionen.
- Kravställ att leverantören ska leverera signerade uppdateringar.
- Om separata test och utvecklingsmiljöer finns, se till att även dessa är skyddade.

2.3 Säkerställ systematisk kontinuitetsplanering och incidenthantering, samt övning

Typ av rekommendation, organisatoriska åtgärder

Säkerställ upprätthållandet av drift vid allvarligare störning genom kontinuitetsplanering som tydligt beskriver de fastställda rutinerna och roll- samt ansvarsfördelning vid krisläge. Exempel på krisläge är avbrott i kraftförsörjningen, haveri av styrsystem, eller sjukdom hos operativa nyckelpersoner.

Förutom att kontinuerligt följa upp och uppdatera kontinuitetsplaner är det viktigt att säkerställa personalens kontinuerliga kompetensutveckling eftersom många som arbetar med cyberfysiska system saknar erfarenhet av it-relaterade attackscenarion. Det är därför även viktigt att de färdigheter, rutiner och processer som tagits fram övas. Med hjälp av övning kan ni uppnå de färdigheter och erfarenheter som krävs för att vara mentalt och praktiskt förberedda för en incident när den faktiskt inträffar. Att genomföra en helt oprövad rutin i skarpt läge innebär ofta stora risker. Övningar ger er också möjlighet att testa och förbättra metoder, rutiner och verktyg.

Alla oväntade händelser (incidenter) måste dokumenteras för att senare kunna analyseras. En av svårigheterna med incidenthanteringen är att finna en balanserad struktur över hur incidenter ska kunna fångas in utan att det uppfattas som ett hinder i den normala arbetsprocessen. Det är därför viktigt att motivera organisationen genom att kommunicera syftet med incidentrapporteringen och dokumenterandet, samt att återkoppla resultaten av incidenthanteringen. Utan denna kommunikation kan det bli svårt att bevara motivationen att rapportera incidenter och sårbarheter.

Rekommendationer

- Upprätta och underhåll incidenthanteringsrutiner och kontinuitetsplaner för de industriella informations- och styrsystemen.
- Analysera incidenter för att fastställa och förstå ursprungsproblem, omfattning (spridning), direkta och indirekta konsekvenser. Kontrollera till exempel om det är enkla fel och om de uppstod på grund av uppsåtliga eller ouppsåtliga händelser.
- Se till att följande punkter ingår i kontinuitetsplaneringen:
  1. rutiner för att sköta verksamheten manuellt (driva processen utan datorstöd)
  2. rutiner för att återställa både data och konfigurationsinställningar samt återstarta processen
  3. kontaktuppgifter till systemägare, operatörer, drifttekniker, övrig personal, leverantörer och support
  4. beskrivning av supportavtal och inställelsetider
  5. beskrivning av hur centrala komponenter i styrsystemet återanskaffas och vilka som bör finnas i eget reservlager.
  6. beskrivning av hur, och varifrån, nöddrift genomförs om störningen är allvarlig.
- Se till att alla som har ansvar inom området har upparbetat god kompetens och att de genom kompetensutveckling behåller denna kompetensnivå inom sina respektive ämnesområden.
- Planera och genomför olika typer av övningar kring incidenter. Som ett inledande steg kan övningar användas som ett lärande moment inom incidenthantering där it har ett centralt inslag. När rutiner, processteg och kunnande finns på plats kan övningarna istället ha som mål att behålla kompetens men även utvärdera och finjustera rutiner, metoder, verktyg och arbetsformer.
- Ha en dokumenterad strategi för övnings- och utbildningsverksamhet som regelbundet stäms av med ledningen. Det bör finnas en roll med ansvar för att uppdatera övnings- och utbildningsstrategin.
- Dela incidentrapporter mellan intressenter och myndigheter i syfte att långsiktigt stärka samhällets motståndskraft mot oönskade it-relaterade händelser.
- För mer information om incidenthantering, se MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

Referenser

Referenser

Nedan följer en lista på rekommendationer för vidare läsning.

Källa	Beskrivning	Kostnadsfri
NERC CIP	North American Electric Reliability Corporation: Critical Infrastructure Protection	X
NIST 800-82	National Institute of Standars and Technology: Guide to Industrial Control Systems (ICS) Security	X
CPNI	Centre for the Protection of National Infrastructure: Good Practice Guide Process Control and SCADA Security	X
DOE 21 Steps	Department of Energy: 21 Steps to Improve Cyber Security of SCADA Networks	X
Norwegian Oil & Gas	Information security baseline requirements for process control, safety and support ICT systems	X
US-CERT CISA	Cyber Security Procurement Language for Control Systems	X
IAEA	Nuclear security series #17 (Computer Security at Nuclear Facilities)	X
2700[X]	SS-ISO/IEC 27000-serien: Ledningssystem för informations-säkerhet	
IEC 62443-[X-X]	IEC 62442-serien: Security Guidelines and User Resources for Industrial Automation and Control Systems	
MSB	MSBs Metodstöd för systematiskt informationssäkerhets-arbete	X

Rekommendation	Referens- och informationsmaterial
Lägg grunden 1	
1.1 Säkra ledningens engagemang och ansvar för säkerheten	27001 27002 (kap. 5, 6.1.1) CAPSS Norweigan Oil & Gas (No. 4, 13) Norweigan Oil & Gas (No.1) IEC 62443-1-1 (kap. 5.8.2)
1.2 Tydliggör roller och ansvar för säkerheten	NERC CIP (003-6) NIST 800-82 (kap. 4.2–4.5, 6.2.4, 6.2.12) CAPSS DOE 21 Steps (No. 12, 16, 20) 27002 (Kap. 6,7) IAEA (Kap. 4, 5.1)
1.3 Samverka i användarföreningar, standardiseringsorgan och andra nätverk för säkerhet	27002 (Kap. 6) 27010
1.4 Inkludera säkerhetskrav från början i all planering och upphandling	NIST 800-82 (Kap. 6.2.14) CAPSS Norweigan Oil & Gas (No. 8, 9) PL (alla kapitel) 27002 (kap. 6.2, 15) IEC 62443-2-1(4.3.4.3, A.3.4.3.4)
1.5 Möjliggör en god säkerhetskultur och höj medvetenheten om behovet av säkerhet	NERC CIP (004-4) DOE 21 Steps (No. 21) Norweigan Oil & Gas (No. 5) IAEA (Kap. 4.2) 27002 (Kap. 7.2)

Rekommendation	Referens- och informationsmaterial
Lägg grunden 2	
2.1 Underhåll processer för systemkartläggningar och riskhantering	NERC CIP (002-4) DOE 21 Steps (No. 13) DOE 21 Steps (No. 14, 18) Norweigan Oil & Gas (No. 2, 3, 11) 27002 (Kap. 8) 27005 IAEA (Kap. 5) IEC 62443-1-1 (Kap. 5.6) IEC 62443-3-2-1 (Kap. 4.2, 4.3)
2.2 Säkerställ en systematisk förändringshantering	NERC CIP (003-4) DOE 21 Steps (No. 17) Norweigan Oil & Gas (No. 10, 15) 27002 (Kap. 15.2.2, 14.2.2)
2.3 Säkerställ systematisk kontinuitetsplanering och incidenthantering, samt övning	NERC CIP (008-4, 009-4) NIST 800-82 (Kap. 6.2.6) CAPSS DOE 21 Steps (No. 7, 16) Norweigan Oil & Gas (No. 7, 16) 27002 (Kap. 16, 17) 27035 IEC 62443-1-1 (Kap. 4.3.2.5) IEC 62443-2-1 (Kap. 4.3.4.5, A.3.4.5, 4.3.2.5, A.3.2.5) IAEA (Kap. 4.2.1) Norweigan Oil & Gas (No. 5) 27002 (Kap. 8.2.2) 27035 IEC 62443-2-1 (Kap. 4.3.2.4)

Ordlista

Ordlista

Administrativa system	It-system som används för administrativ databehandling, kontorsautomation eller affärssystem.
Botnät	Ett nätverk av infekterade datorer som kan styras av en och samma angripare. Botnät kan bland annat användas till överbelastningsattacker och spridning av skadlig programvara.
Cyberfysiska system	Med cyberfysiska system menas gränssnittet mellan en digital miljö och en fysisk process. Ett cyberfysiskt system kan antingen vara ett industriellt informations- och styrsystem eller ett IoT-system (eng. Internet of Things).
Cybersäkerhet	Cybersäkerhet är all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot möjliga handlingar, omständigheter, eller händelser som på ett negativt sätt påverkar nätverks- och informationssystemen och människor. Cybersäkerhet handlar främst om att möta antagonistiska hot.
Data	Data kan syfta på information eller rådata (uppgifter som ej bearbetats/analyserats).
DMZ	(Eng. *DeMilitarized Zone*.) Ett isolerat subnät som placeras utanför det administrativa nätet och endast innehåller system som behöver exponeras mot omvärlden.
Firmware	Mjukvara som är inbyggd i hårdvara.
Fysiskt skydd	Skydd som bland annat stoppar angripare från att fysiskt komma åt information eller informationstillgångar. Fysiskt skydd kan också skydda informationstillgångar från brand, översvämningar, jordbävningar, etc.
Fysisk säkerhet	Informationstillgångar och system skyddas fysiskt från till exempel obehörigt tillträde, brand och vattenskador.
Härdning	(Inom it) Processer och rutiner som syftar till att minska systemets attackyta och därmed bättre motstå angrepp och angreppsförsök.
ICS	(Eng. *Industrial Control Systems*.) En vanligt förekommande förkortning som ibland används synonymt med industriella informations- och styrsystem.

Inbyggda system	Datorer eller datorliknande system som ingår i enheter som har en eller ett fåtal speciella funktioner, ofta med någon form av realtidskrav. Mjukvaran i ett inbyggt system ligger oftast lagrat i ROM-minne eller flashminne. Inbyggda system är ofta en del av en apparat eller maskin inklusive hårdvara och mekaniska delar. Inbyggda system förekommer ofta i industriella informations- och styrsystem. Kallas även inbäddade system.
Industriella informations- och styrsystem	Industriella informations- och styrsystem är ett begrepp som samlar flera typer av styrsystem, bland annat SCADA-system (Supervisory Control and Data Acquisition). Andra benämningar kan vara processkontrollsystem, processautomation, process-it, OT-system (operational technology), tekniska it-system, anläggnings-it, distribuerade kontrollsystem och inbyggda realtidssystem (RTE).
Information	En mängd data som har betydelse.
IoT	Internet of Things, IoT (sv. sakernas internet) är ett begrepp som används för att beskriva att allt fler föremål, både för privat och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk.
IIoT	Användning av IoT inom industrin benämns IIoT (Industrial Internet of Things) och är enheter som används för mätning och övervakning, eller system och enheter för styrning som kopplas samman med övriga informationsnätverk.
Informationssäkerhet	Informationssäkerhet handlar om att skydda information så att den alltid finns när vi behöver den (tillgänglighet), att vi kan lita på att den inte är manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet). Informationssäkerhet handlar om att skydda informationen i sig, oavsett vilket medium den förmedlas på. Informationssäkerhet uppnås genom att vidta administrativa, organisatoriska, tekniska och fysiska åtgärder.
Konfigurationsdatabas	Databas som innehåller information om hur ett it-system eller cyberfysiskt system är konfigurerat, vilka resurser som finns i systemet och hur de är kopplade till varandra. Databasen är till för att underlätta återställning av system efter en incident. Konfigurationsdatabasen har ett högt skyddsvärde.
Molntjänster	Tjänst som tillhandahålls av leverantör via internet från ett nätverk av servrar, till exempel datalagring på distans via internet.
Organisatorisk säkerhet	Det finns personal som har tid, kompetens och förmåga att arbeta med informations- och cybersäkerhet. Alla medarbetare i organisationen har en grundläggande förståelse för informationssäkerhet och de regelverk som gäller för organisationen.

PLC	(Eng. *Programmable Logic Controller.*) Digital dator som används för automation. Ofta avancerad enhet som kan utökas eller programmeras att utföra nya uppgifter och styra fysisk interaktion med systemkomponenter (t.ex. ställdon).
Riskbedömning	En riskbedömning utgörs av tre olika delar: riskidentifiering, riskanalys och riskvärdering.
Samhällsviktig verksamhet	MSB definierar samhällsviktig verksamhet som verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet.
SCADA	(Eng. *Supervisory, Control and Data Acquisition.*) Ett övergripande, ofta geografiskt distribuerat, industriellt styrsystem för övervakning och styrning av processer för industriellt bruk.
Systemklassificering	Analysen av konfidentialitet, riktighet, och tillgänglighet kopplat till varje system leder fram till en klassificering som sedan ger svar på om en eller flera åtgärder ska införas för att skydda systemet eller bäraren.
Sårbarhet	Brist i skyddet av en tillgång eller av en säkerhetsåtgärd som kan utnyttjas av ett eller flera hot.
Säkerhetsperimeter	Logiskt eller fysiskt skalskydd. Logiskt skalskydd utgörs av segment eller domän som avgränsar område, exempelvis åtskiljer OT-från it-arkitektur.
Säkerhet på djupet	Ett omfattande försvar som utgörs av flera lager av säkerhetsmekanismer. Detta innebär att flera samverkande eller kompletterande skyddsmekanismer existerar och därmed motverkar att fel i- eller manipulation av enstaka skydd får omfattande konsekvenser.
TCP/IP	(Eng. *Transmission Control Protocol/Internet Protocol.*) Standardiserat datakommunikationsprotokoll som används som bärartjänster såväl på internet som inom industriella lösningar.
Teknisk säkerhet	Säkerhetsåtgärder som införs i it-miljön och den cyberfysiska miljön, till exempel autentisering, nätverkssegmentering, kryptering, filtrering av nätverkstrafik.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1880 - december 2021 ISBN 978-91-7927-213-5