Myndigheten för samhällsskydd och beredskap

Inriktning för cyberfysiska system 2021–2022

Inriktning för cyberfysiska system 2021–2022

Foto: Shutterstock
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1588 - juni 2020
ISBN: 978-91-7927-044-5

Inriktning cyberfysiska system 2019–2022

Aldrig tidigare har det historiskt sett varit så viktigt att arbeta med säkerhet i samhället som det är nu. Inte minst när det handlar om cyberfysiska system i samhällsviktig verksamhet. Cyberfysiska system är datorbaserade system avsedda för interaktion med maskiner, fordon och annan utrustning, inklusive sensorer som kan inhämta data från omgivningen. Det innebär att cyberfysiska system omfattar både industriella informations- och styrsystem och Internet of Things (IoT).

Samhället är beroende av cyberfysiska system

Cyberfysiska system är system som ingår i mängder av processer i vårt samhälle. De finns i system som renar vårt dricksvatten, system som gör att avloppsvatten renas för att släppas ut i sjöar och vattendrag. De cyberfysiska systemen används i processer för energiförsörjning, i alla typer av transportsystem; i luften, på land, till sjöss eller på vägar för att möjliggöra kommunikation. I princip allt i vårt samhälle är och blir allt mer beroende av cyberfysiska system.

Då cyberfysiska system kan vara både uppkopplade mot internet samtidigt som de är sammankopplade med andra nätverk, kräver de en högre grad av skydd för att inte bli sårbara eller drabbas av avbrott.

MSB sätter ny inriktning för cyberfysiska system

Cyberfysiska system ägs av statliga, kommunala och privata aktörer, även om merparten av systemen finns i privata företag och organisationer. Eftersom antalet funktioner som är beroende av cyberfysiska system ständigt ökar blir antalet aktörer som behöver skydda systemen också fler. Därför ser vi från Myndigheten för samhällsskydd och beredskap, MSB, ett behov av att skapa en inriktning för cyberfysiska system. Denna inriktning beskriver det arbete MSB kommer att bedriva kommande år fram till och med 2023 avseende på cyberfysiska system. Inriktningen är avsedd för de som arbetar med industriella informations- och styrsystem, Internet of Things och som är intresserade av frågorna.

Gränsen mellan administrativa system och industriella informations- och styrsystem börjar suddas ut

Sett ur ett historiskt perspektiv styrdes industriella processer, transportsystem och liknande system av mekaniska elektromagnetiska maskiner med manuellt handhavande. Dessa system har traditionellt varit fysiskt isolerade och byggt på specialutvecklad teknik. I takt med den tekniska utvecklingen, har gränserna mellan de administrativa systemen och industriella informations- och styrsystem blivit mindre tydliga. Det har resulterat i att de industriella informations- och styrsystemen dels blivit mer automatiserade och dels blivit sammankopplade med organisationernas administrativa system, bland annat för att hämta information för att genom statistik kunna mäta effekten eller nyttjandegrad eller vid fakturering och andra liknande funktioner.

De industriella informations- och styrsystemen är ofta tillgängliga via internet och andra publika nätverk för att uppnå högre flexibilitet och för att kunna styra och övervaka dem från andra platser. Det faktum att de industriella informations- och styrsystemen har tillverkats för att ha mycket lång livstid, och bygger på samma teknik som vanliga it-system, gör att de drabbas av samma säkerhetsproblem som traditionella it-system. För att stödja organisationer som arbetar med industriella informations- och styrsystem har MSB genom åren arbetat med de här frågorna.

MSB, och tidigare KBM (f d Krisberedskapsmyndigheten), har sedan 2005 aktivt arbetat med säkerhet i industriella informations- och styrsystem. Från och med 2007 gavs arbetet en tydlig teknisk dimension genom samarbetet med Totalförsvarets forskningsinstitut. Inledningsvis var arbetet fokuserat på SCADA-system, Supervisory Control And Data Acqusition. Med tiden har perspektivet vidgats till industriella informations- och styrsystem och nu till dagens arbete med cyberfysiska system. Arbetet har bedrivits som ett av flera

program under ett antal år. Från och med 2019 bedrivs arbetet på en enhet hos MSB som fokuserar på säkerhet i cyberfysiska system.

Medvetandehöjande arbete

MSB:s arbete med industriella informations- och styrsystem har fokuserat på att skapa ökad medvetenhet kring frågorna och på fortsatt utveckling av både en nationell och internationell samverkan. Det har bland annat inneburit produktion av vägledningar, faktablad och genomförande av studier inom relevanta områden. MSB deltar också som föreläsare på konferenser, mässor och utbildningar. Målgruppen för det medvetandehöjande arbetet har varit företag, organisationer och myndigheter som bedriver samhällsviktig verksamhet och som är beroende av industriella informations- och styrsystem.

MSB står bakom publikationen ”Vägledning till ökad säkerhet i industriella informations- och styrsystem” som innehåller grund-

läggande rekommendationer för att öka säkerheten i industriella informations- och styrsystem. Den första versionen av vägledningen togs fram 2008, och efter omarbetning har den därefter kommit att bli branschpraxis och fått stor spridning såväl nationellt som internationellt.

Nationell och internationell samverkan

MSB har arbetat med samverkan både nationellt och internationellt. Den nationella samverkan har skett med myndigheter med sektorsansvar, ägare, operatörer och leverantörer. Sedan 2005 leder MSB forum för privatoffentlig samverkan, FIDI-SCADA (Forum för Informationsdelning inom informationssäkerhetsområdet på SCADA-området), där deltagarna representerar verksamheter som förvaltar och driver samhällsviktiga informations- och styrsystem. FIDI-SCADA genomför fyra till sex möten per år och gruppens arbete regleras av formella medlemsriktlinjer.

Den internationella samverkan har under åren skett genom deltagande i internationella forum, men även bilateralt med myndigheter i ett flertal länder. MSB har bland annat medverkat i ICSJWG – US ICS-CERT:s verksamhet för privatoffentlig samverkan och i Europeiska nät- och informationssäkerhetsbyrån ENISA:s möten och arbetsgrupper.

NCS3 och CRATE

Sedan 2007 stöttar MSB Totalförsvarets forskningsinstitut (FOI) i uppbyggnaden av kompetens och en teknisk samverkansplattform, Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3), som myndigheterna inrättade 2012. NCS3 är ett gemensamt kompetenscentrum för MSB och FOI som har till uppgift att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Inom NCS3 sker även forskning, utbildning och övningar för myndigheter och företag som äger och/eller arbetar med samhällsviktig verksamhet där industriella informations- och styrsystem ingår. Inom ramen för NCS3 har även ett flertal demonstratorer utvecklats. Den största demonstratorn är det så kallade miniatyrlandskapet. Det är en miniatyrmodell över ett samhälle som är framtagen för att pedagogiskt visa effekten vid övningar och demonstrationer av hur angrepp kan slå över hela samhället.

MSB har i samverkan med försvarsmakten och FOI utvecklat en nationell övnings- och utbildningsplattform på FOI:s anläggning i Linköping. Denna övnings- och utbildningsplattform CRATE, Cyber Range And Training Environment är en teknisk infrastruktur som skapar tydliga pedagogiska effekter, kopplat till fysiska kontrollsystem och det tidigare beskrivna miniatyrlandskapet.

Forskningsprogram

MSB utlyste och beviljade år 2015 medel för två forskningsprogram inom industriella informations- och styrsystem som pågår under fem år. Dessa är Center for Resilient Critical Infrastructures (CERCES) och Resilient Industrial Control Systems (RICS). Båda forskningsprogrammen är knutna till MSB:s arbete för ökad säkerhet i industriella informations- och styrsystem.

Strategi för ökad förmåga att motstå störningar och angrepp

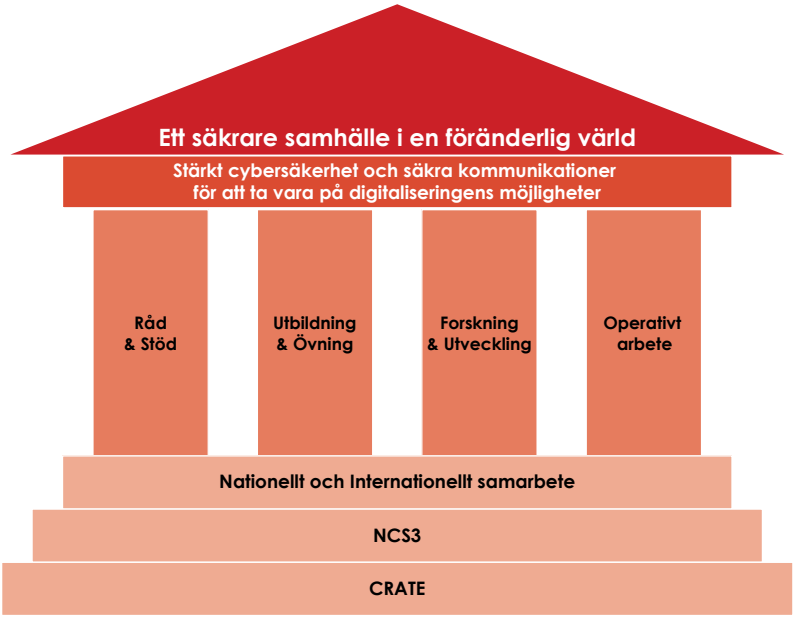
MSB stödjer aktörer inom samhällsviktig verksamhet att öka förmågan att motstå störningar och angrepp. Detta sker genom att myndighetens förebyggande och operativa arbete anpassas till aktörens aktuella behov att skydda systemen och göra dem säkra. Grunden

till arbetet utgörs av MSB:s vision: Ett säkrare samhälle i en föränderlig värld. Målet är stärkt cybersäkerhet och säkra kommunikationer för att ta vara på digitaliseringens möjligheter.

Verksamheten fokuserar på:

- Rådgivning och stöd
- Utbildning och övning
- Forskning och utveckling
- Operativt arbete

Ett säkrare samhälle i en föränderlig värld



Skräddarsydd rådgivning och stöd till NIS-aktörer genom samverkan

MSB har identifierat elva samhällsviktiga sektorer där sju av dessa sammanfaller med de sektorer som omfattas av NIS-lagstiftningen. Dessa sektorer är Energi, Bankverksamhet, Finansmarknadsinfrastruktur, Hälso- och sjukvårdssektorn, Digital infrastruktur, Leverans och distribution av dricksvatten samt Transporter.

När det gäller cyberfysiska system kommer arbetet inledningsvis vara fokuserat på de sju sektorer som omfattas av NIS-lagstiftningen, för att successivt omfatta fler sektorer i framtiden.

Det gör det möjligt att anpassa innehållet för var och en av samhällets sektorer och skapar en flexibilitet att erbjuda det stöd som aktörerna inom respektive sektor behöver och efterfrågar. På så sätt kan skräddarsydda paket erbjudas aktörer inom de olika sektorerna.

Anpassning av de olika sektorspaketen förutsätter samverkan med andra myndigheter, bland annat de myndigheter som har ett tillsynsansvar enligt NIS-lagstiftningen.

Rådgivning och stöd

Det första arbetsområdet, rådgivning och stöd, består av medvetandehöjande material och stödjande verktyg för att öka säkerheten i dessa samhällsviktiga system. Området kommer att erbjuda produkter som vägledningar, faktablad, nyhetsblad, filmer och stöd till aktörerna. Det innebär även genomförande av föreläsningar, deltagande vid mässor och seminarier. Tekniska verktyg och installationsanvisningar kommer också att finnas tillgängliga. Som exempel på sådana verktyg är skyddspaket för ICS/SCADA och nätverksanalys. MSB avser även att erbjuda operativt stöd för att detektera, identifiera, analysera och hantera hot och sårbarheter i industriella informations- och styrsystem.

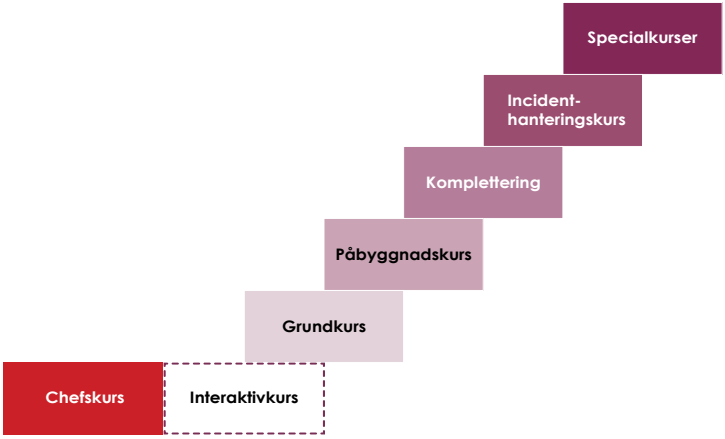
Utbildning och övning

Det andra området, utbildning och övning, består av utbildningar i flera nivåer. Där varje nivå är baserat på de behov och den kunskapsnivå som mottagaren befinner sig på.

Utbildningarna kommer att utgå från en basnivå som består av en kortare utbildning för chefer och en grundläggande interaktiv utbildning som förutsättningskrav för fortsatta utbildningsnivåer. Nästa nivå består av en grundutbildning för tekniker, vilken är en förutsättning för påföljande nivå som är en påbyggnadskurs. Nivån efter det är kompletteringsutbildning till grundkursen och påbyggnadskursen. Ytterligare nivåer är specialkurser som till exempel utbildning i verktyg och metoder att genomföra hotbildsanalys och hantering av hotbilder samt incidenthanteringsutbildning vilken även kan tillhandahållas på distans. Området omfattar även övningar. Genomförande av övningar är viktigt för att identifiera brister och öka förståelsen för hur olika typer av händelser kan påverka den

ordinarie verksamheten och hur den kan skyddas. Som grund för dessa övningar kommer CRATE att användas.

CRATE har en unik förmåga att kunna återanvända erfarenheter från tidigare övningar och utbildningar. CRATE kan även användas för att testa produkter och i forskningssammanhang. Dessa fyra delar bildar en helhet som gör det möjligt att anpassa blocken för samhällets sektorer.



Forskning och utveckling

Det tredje området, forskning och utveckling, innebär att det ska finnas en teknisk infrastruktur som möjliggör tester och akademisk forskning i syfte att skapa nya metoder eller sätt att skydda cyber-fysiska system.

Operativt arbete

Det fjärde området, operativt arbete, innebär att det ska finnas stöd för aktörer att kontakta MSB när en incident eller händelse inträffar i cyberfysiska system. Detta stöd sker inom ramen för CERT.SE som är Sveriges nationella CSIRT (Computer Security Incident Respons Team) en verksamhet som bedrivs inom MSB för att stödja samhället i arbetet med att hantera och förebygga

it-incidenter. MSB:s operativa process innebär att en analys görs av den inrapporterade händelsen, som resulterar i åtgärdsförslag till den drabbade aktören. Det operativa arbetet består även i att stödja aktörer i arbetet med att identifiera sårbarheter och hot i den egna miljön samt att genomföra en hotbildsanalys och identifiera vilka åtgärder som behöver vidtas och att vidta åtgärderna. Syftet är att skapa förutsättningar för aktörerna att på egen hand utföra dessa åtgärder.

Inom ramen för det operativa arbetet kommer även tester att genomföras för att identifiera sårbarheter och brister samt hur det går att skydda system mot sådana händelser. Detta kan i sin tur resultera i åtgärder som vidtas inom området Rådgivning och stöd.

MSB:s arbetsområde ökar i omfattning

Den strategiska inriktningen för MSB:s arbete med cyberfysiska system innebär en högre ambitionsnivå än tidigare. Cyberfysiska system är it-system. MSB:s arbete består i att utifrån identifierat behov hos aktörerna ta fram produkter i form av rådgivning och stöd, kommunicera detta med aktörerna och göra uppföljningar för att verifiera att målet uppnåtts. Inträffade händelser leder till att skapa underlag för det förebyggande arbetet vilket i sin tur innebär att nya verktyg och stöd kan tas fram. Det innebär även att händelser eller företeelser som identifieras i det förebyggande arbetet kan återföras till det operativa arbetet för analys och förslag till åtgärder. På detta sätt kan de två processerna kopplas ihop och skapa en högre effektivitet i arbetet. Allt för att öka den samhälleliga förmågan att stå emot störningar.

MSB:s förmåga att stödja aktörerna ökar

MSB:s arbetsområde vidgas till att omfatta fler system och aktörer samt intressenter. Information överförs idag alltmer via satelliter vilket gör att även de cyberfysiska systemen får ett större beroende till rymdsäkerhetsfrågor vilket i sin tur gör att även dessa frågor behöver beaktas i det framtida arbetet med cyberfysiska system.

Arbetet kommer fortsättningsvis att bedrivas i nära samverkan

med bland andra FOI, Försvarsmakten, Rymdstyrelsen, Energimyndigheten, Svenska Kraftnät, Transportstyrelsen, Post och Telestyrelsen, Livsmedelsverket, kommunala bolag och privata aktörer. Likaså kommer en nationell satsning för ökad säkerhet inom området och fortsatt utveckling av Nationell Cyber Range, NCR, att ske. Internationellt kommer samarbete att ske med andra länder som till exempel Norge, Danmark, Finland, USA, Tyskland, Nederländerna och Frankrike. Att sammanfoga det operativa och det förebyggande arbetet ökar MSB:s förmåga att stödja aktörerna i att höja säkerheten vilket bland annat sker genom systematiskt informationssäkerhetsarbete.

MSB:s arbete med cyberfysiska system kommer i huvudsak att inriktas mot samhällsviktig verksamhet även om annan verksamhet också omfattas. Detta bidrar i sin tur till att totalförsvarsförmågan hos de aktörer som tillhandahåller dessa system också ökar.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1588 - juni 2020 ISBN 978-91-7927-044-5