Information från programmet för säkerhet i industriella informations- och styrsystem – #2 2016

Inledning

Genom detta blad vill vi på enklaste sätt informera om aktiviteter, rapporter och dylikt med koppling till arbetet för säkerhet i industriella informations- och styrsystem.

Frågor, kommenterar och förslag till innehåll tas tacksamt emot via e-post till scada@msb.se.

Helt färskt medvetandehöjande material

Programmet har producerat tre små broschyrer som i ”serieformat” levandegör några av vägledningens 17 rekommendationer. Broschyrerna kommer senare att gå att beställa via MSB:s hemsida. De finns inom kort även i presentationsformat på www.msb.se/ics och kan med fördel användas som diskussionsunderlag vid möten etc.

Presentation baserad på vägledningen

På programmets hemsida hittar ni numera en presentation som på torraste möjliga sätt går igenom vägledningens 17 punkter. Färdig att använda för interna utbildningar och dylikt!

Vår vägledning

Arbetet med en ny version av vår uppskattade vägledning rullar vidare. Planerat färdigställande har fått skjutas till 2018, men har ni synpunkter eller förslag så kontakta oss gärna.

Vägledningen går att beställa gratis i tryckt format, alternativt hittar ni den på https://www.msb.se/RibData/Filer/pdf/27425.pdf

SI3S-kurser 2017

Den grundläggande kursen om säkerhet i industriella informations- och styrsystem, SI3S, kommer preliminärt finansieras av MSB vid 4 tillfällen - v9, v10, v45 och v46.

Intresseanmälningar kan alltid skickas till scada@msb.se. Kontakta oss även om ni är intresserade av att själva finansiera något tillfälle.

Leverantörsmöte

Den 15 november genomfördes en workshop för leverantörer i Linköping.

MSB, FOI, NCS3 och programmet för säkerhet i industriella informations- och styrsystem vill framföra sina varma tack till alla leverantörer som ställde upp med sin tid och kunskap (i bokstavsordning):

ABB, Bombardier Transportation, Cactus Rail, Cactus Utilities, HMS, Malthe Winje Automation AB, Modio, Netcontrol, Schneider Electric, Siemens Turbomachinery, Siemens

Frågor som diskuterades under workshopen var: Vad ser ni för utmaningar inom arbetet med ökad cybersäkerhet? Vad är era erfarenheter av att arbeta med säkerhetsaspekter tillsammans med kunder? Hur ser ni på utvecklingen framöver kopplat till säkerhetsfrågan? Vad har ni för önskemål gällande stöd, vägledning etc. från myndighetshåll? Var har ni för erfarenhet av eget eller kunders arbete med IEC-62443 eller andra standarder och vägledningar?

Parallellt med workshopen genomfördes en komprimerad version av SI3S och I4S.

Möte för integratörer och tekniska konsulter

Under 2017 hoppas vi kunna anordna en workshop för integratörer och tekniska konsulter inom området. Kontakta oss om du är intresserad. Preliminärt datum för mötet är den 5 april.

Workshop med CERCES och RICS

Den 22 februari kommer de MSB-bekostade forskningsprogrammen CERCES och RICS presentera och diskutera sin forskning hos MSB i Stockholm under några timmar. Ta chansen att påverka nationell forskning inom området! Anmäl intresse via scada@msb.se med ”forskningsworkshop” i ämnesraden.

Utredningar och årsrapporter visar på vikten av säkerhet i industriella informations- och styrsystem

Såväl informationssäkerhetsutredningen (SOU 2015:23) som utredningen om en ny säkerhetskyddslag (SOU 2015:25) betonar samhällsviktiga verksamheters beroende av industriella informations- och styrsystem och vikten av att upprätthålla en stark nationell kompetens inom området. I Myndigheten för Samhällssydd och beredskaps Nationell risk- och förmågebedömning 2016 görs bedömningen att arbetet med informations- och cybersäkerhet behöver utvecklas ytterligare. I Svenska Kraftnäts risk- och sårbarhetsanalys 2016 redovisas hotbildsanalyser, baserade till stor del på öppna källor i form av rapporter från Försvarsmakten och Säkerhetspolisen samt det senaste årets nyhetsflöde. En av bedömningarna som görs är att resursstarka aktörer med stor förmågebredd utgör det dimensionerade hotet när ansvariga för viktiga elinfrastrukturer utformar och kravställer informations- och IT-säkerhetsfunktioner.

I de senaste årens årsöversikter från Säkerhetspolisen och Militära Underrättelsetjänsten framgår att främmande makt arbetar med kartläggning av både civil och militär svensk

Information från programmet för säkerhet i industriella informations- och styrsystem – #2 2016

infrastruktur, bl.a. genom elektroniska angrepp. Enligt Säkerhetspolisen kan sådan kartläggning av olika former av sårbarheter ligga till grund för planläggning av bland annat sabotage där syftet i slutändan kan vara att lamslå viktiga samhällsfunktioner. Militära Underrättelsetjänsten beskriver hur så kallad hybridkrigföring har fått ökad betydelse i hotbilden mot Sverige. Med hybridkrigföring avses att en bred pallet av militära, irreguljära och civila metoder används, inklusive angrepp mot t.ex. elförsörjning. FRA noterar i sin årsrapport för 2015 att de har sett en accelererande utveckling av avancerade cyberangrepp i det globala nätet och att de under 2015 upptäckt angrepp mot forskningsinstitutioner, industri, myndigheter och andra mål i Sverige.

NIS-direktivet

EU-direktivet om en hög gemensam nivå av nät- och informationssäkerhet i hela unionen, det så kallade NIS-direktivet, kommer bland annat att innebära obligatorisk incidentrapportering för såväl offentliga som privata aktörer inom sektorerna energi, transporter, bank, finans, hälso- och sjukvård och vattenförsörjning. Regeringen har tillsatt en genomförandekommitté för att se hur direktivet kan införlivas i svensk rätt. Regeringsbeslut om utredare togs 31 mars och de ska lämna sitt förslag senast den 1 maj 2017. 2018 ska direktivet implementeras.

Osäkra implementationer av protokollet MQTT

CERT-SE har skrivit en informationstext om osäkra implementationer av protokollet MQTT, som bland annat används IoT-applikationer, där sensorer sänder mätdata till en server som skickar datat vidare till styr- och reglersystem, webbservrar eller direkt till datorer eller mobiltelefoner. Se https://www.cert.se/2016/09/mqtt-i-sverige

NCS3-studier 2017

NCS3, Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (det av MSB bekostade samarbetet mellan MSB och Totalförsvarets forskningsinstitut, FOI), kommer under 2017 bland annat arbeta med projekt inom:

Molntjänster och viritualisering inom ICS, användningen av trådlös teknik inom ICS och tillämpningen av regelverk och krav inom området.

Hör gärna av er vid intresse av att delge erfarenheter och idéer.

Informations- och cybersäkerhet inom transportområdet

MSB genomför varje år en fördjupad analys av informationssäkerheten inom minst en av sex särskilt utpekade samhällssektorer. Under 2016 undersöktes transportsektorn. 188 företag svarade på en enkät som skickades ut. Några av slutsatserna från enkäten är att:

- Vikten av informations- och cybersäkerhet undervärderas inom den svenska transportsektorn,
- El, elektroniska kommunikationer och it-system och tjänster är stora beroendeområden som växer i betydelse,
- Icke-antagonistiska incidenter påverkar företagen både värst och oftast, och
- kortare avbrott i tillgången till information ses som den troligaste informationssäkerhetsrisken under det kommande året.

NCS3-studie om åldrande klar för nerladdning

I studien undersöks synen på, och hanteringen av, åldrande industriella informations- och styrsystem (ICS) inom några samhällsviktiga verksamheter i Sverige. Resultatet visar att det inte är åldrande i den traditionella meningen, dvs. att något degenererar tills det slutar fungera, som utgör den stora utmaningen. Utmaningarna är i stället kopplade till relativt åldrande, dvs. att tekniska lösningar åldras relativt omgivningens krav.

Kraven kommer i första hand från de snabbt evolverande övergripande informations- och övervakningssystemen, med resultat att automationsutrustning snabbt uppfattas som omodern. I första hand är det leverantörernas allt kortare supporthorisont som är gränssättande. Rapporten hittas på www.msb.se/ics.

Cyberfysiska system i kommuner

Hösten 2016 genomfördes en studie i syfte att undersöka vilket stöd som kommuner ser som relevant i sitt arbete med cyberfysiska system. Resultaten visar önskemål om stöd i form av guider, checklistor, mallar och konkreta exempel på hur man strukturerar och kartlägger sina systemstrukturer. I rapporten listas identifierade typer av cybersfysiska system som kan användas vid en inventering i den egna kommunen. Dessutom listas diskussionspunkter som stöd för tankearbete, kartläggning och strukturarbete med de cyberfysiska systemen. Studien visar att det finns kommuner som kommit noterbart längre i sitt arbete. Dessa har också signalerat att de gärna stödjer andra kommuner i deras arbete. Rapporten kommer att publiceras på www.msb.se/ics efter årsskiftet.

Programmet för säkerhet i industriella informations- och styrsystem är ett MSB-program som arbetar sektorsövergripande med frågor om säkerhet i samhällsviktiga informations- och styrsystem. För mer information, se www.msb.se/ics. Nyhetsbladet är producerat november-december 2016.

Information från programmet för säkerhet i industriella informations- och styrsystem – #2 2016

ICSJWG

I mitten av september genomfördes höstens ICSJWG-konferens. ICSJWG står för Industrial Control Systems Joint Working Group och är, i första hand, amerikanska ICS-CERTs sätt att nå ut till privata och icke-federala målgrupper.

Ett tema som återkom under septembermötet var diskussioner relaterade till om RISK-begreppet, såsom: Vad får säkerhets kosta? Omöjligheten i att sätta siffror på ngt som har med intention att göra – svårigheterna att då göra jämförelser och motivera satsningar på säkerhet/security.

Vidare rapporterades resultat från undersökningar och utvärderingar. Representanter från Storbritannien (från det som nu är NCSC, National Cyber Security Centre) berättade att oavsiktlig bruten separation såsom fjärraccess/tredjepartsaccess/dåligt konfigurerade brandväggar var något det ofta stötte på inom industrialla informations- och styrsystem. Det var också mycket vanligt att man inte visste hur ens system såg ut och vilken mjuk- och hårdvara man hade implementerat.

Inom VA-sektorn i USA konstaterade en konsult som gjort en större genomgång att man ofta hade väldigt platta nätverk, med avsaknad av grundläggande säkerhet.

En rekommendation som gavs var att kontinuerligt se över sina zoner och sin zonindelning och att plocka bort till exempel arbetsstationer som inte används mer än då och då.

Rapporter från ENISA

ENISA, EU:s byrå för nät- och informationssäkerhet har under hästen publicerat ett antal rapporter, bland annat: *Cyber security and resilience for Smart Hospitals*, *Cyber Insurance: Recent Advances, Good Practices and Challenges* och *The cost of incidents affecting CIIs*. Rapporterna finns att ladda ner på: https://www.enisa.europa.eu/publications#c5=2006&c5=2016&c5=false&c2=publicationDate&reversed=on&b_start=0

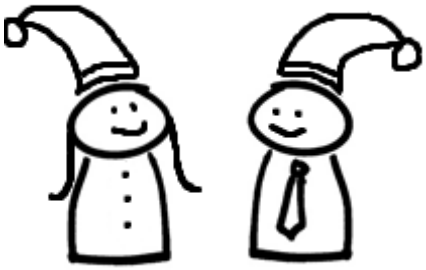
Trendrapport från NCSC-NL

Det Nederländska cybersäkerhetscentret NCSC-NL publicerar årligen sin Cyber Security Assessment Netherlands (CSAN). I årets rapport lyfter man fram fyra trender: att professionella kriminella genomför långlivade och högkvalitativa attacker, att digitalt industrispionage från utlänska säkerhetstjänster påverkar Nederländernas konkurrenskraft, att ransomware har blivit vardag och allt mer avancerad och att ”skadliga annonser” fortfarande är ett problem.

Siemens först ut att certifiera produktutvecklingen

Siemens blir världens första företag som blir certifierade enligt standarden för industriell it-säkerhet IEC 62443. Certifieringen som utfördes av TÜV SÜD gäller IEC 62443-4-1, säkerhet i produktutvecklingsprocessen och omfattar Siemens driv- och automationsprodukter. Säker produktutveckling är en viktig del i djupförsvarskonceptet.

God Jul och gott nytt år!



Programmet för säkerhet i industriella informations- och styrsystem är ett MSB-program som arbetar sektorsövergripande med frågor om säkerhet i samhällsviktiga informations- och styrsystem. För mer information, se www.msb.se/ics. Nyhetsbladet är producerat november-december 2016.