Information från programmet för säkerhet i industriella informations- och styrsystem – #1 2017

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.

Under andra halvåret 2017 kommer våra möjligheter att omhänderta frågor och uppslag vara begränsade på grund av flera samtidiga föräldraledigheter.

Presentation baserad på vägledningen – nu på engelska

Efter önskemål har den presentation som på torraste möjliga sätt går igenom vägledningens 17 punkter översatts till engelska. Även denna finns nu att hämta på www.msb.se/ics.

Lärdomar från elavbrottet i Ukraina

Elavbrotten i Ukraina 2015 och 2016 aktualiserar ett antal åtgärder gällande skyddet av industriella informations- och styrsystem. Vi har nu samlat dessa lärdomar i ett FAKTA-blad. Faktabladet hittas här: https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-programmet-for-industriella-informations--och-styrsystem/Alla-sektorer-har-nagot-att-lara-av-ukrainska-elavbrott/

Kurser 2017

Vi genomförde två grundläggande kurser, SI3S, under v9 och v10. Deltagarna kom från energi- samt vattensektorn.

Vi planerar att hålla den avancerade incident-hanteringskursen I4S under v45 (tisdag-fredag). Den kommer i första hand vända sig till operatörer inom energisektorn men det finns även möjlighet för deltagare från andra sektorer att delta. Kursen vänder sig främst till de som har relativt mycket erfarenhet av IT-system och vill lära sig mer om förutsättningarna att arbeta med incidenter i IT-system där det finns ett stort beroende till de produktionsnära systemen.

Skicka intresseanmälan till scada@msb.se så får ni inbjudan när denna är klar. Kontakta oss även om ni är intresserade av att själva finansiera något tillfälle av SI3S eller I4S.

Eventuellt kommer ytterligare tillfällen av den grundläggande kursen SI3S att annonseras under hösten vid 3 tillfällen. Preliminärt blir det i så fall vecka 44, 46 och 47.

Möte för integratörer

Den 5 april anordnades en workshop för integratörer och tekniska konsulter inom automationsområdet. Vi vill rikta ett mycket stort tack till de medverkande företagen ÅF, Rejlers och Eitech och deras visade intresse av att bidra till att höja säkerheten i Sverige. Under mötet diskuterades frågan om standarder och certifieringar, grundläggande branschetik och hur förmågan att arbeta säkerhet ska få mer genomslag i upphandlingar.

Vi söker samtidigt kontakt med fler integratörer inom automations- och styrsystemsområdet och uppmanar intresserade av att höra av sig.

Rejlers satsar på IT-säkerhet

Som en del i sitt arbete med IT-säkerhet och ökad kvalitet gentemot sina kunder kommer Rejlers att dela ut MSB:s *Vägledning till ökad säkerhet i industriella informations och styrsystem* till alla anställda. Alla kontor kommer därtill att få en genomgång av de av MSB framtagna *"Sedelärande Berättelser".*

Inom Rejlers pågår ett implementationsprojekt med LIS med utgångspunkt i ISO-27000. Arbetet med en internrevision för att uppfylla kraven enligt ISO-27001 för ledningen, centrala IT-funktionen samt för avdelningen automation inom affärsområdet Technology, är även det påbörjat. Som del i detta tas det fram en metodik för leveranser via externa medier, för hantering för att se till att minimera riskerna för att skadlig kod sprids samt kryptering av känslig information.

MSB:s program för säkerhet i industriella informations- och styrsystem uppmuntrar initiativet och uppmanar fler integratörer att följa Rejlers exempel. Kontakta oss om intresse finns – vi kan bidra med material och idéer.

Översikt över monitorerings- och övervakningssystem

En studie om monitorerings- och övervakningssystem har publicerats på www.msb.se/ics

I rapporten kan läsaren bland annat lära sig mer om olika principer för intrångsdetektion samt aktuella trender för forskningen inom området och var marknadens fokus för området ligger. Studien kan fungera som stöd tidigt i en införskaffningsprocess av intrångsdetektionssystem för att visa på de tekniska möjligheter som finns.

Studie om kursers påverkan

Att kurser inom säkerhet ger resultat för den enskilde individens kunskapsnivå kan i många fall vara uppenbart – men hur påverkar en säkerhetskurs individens beteende inom en organisation och framförallt hur påverkas resultatet

Information från programmet för säkerhet i industriella informations- och styrsystem – #1 2017

av säkerhetsarbetet i slutänden? Svar på detta söks i en studie där bland annat effekterna av de kurser som ges vid NCS3 beskrivs. Resultaten visar på attitydförändringar uttryckt i handlingar som ökat intresse för information, interna riktlinjer och kompetens kring säkerhetsfrågor. Det finns även indikationer på att kurserna påverkar på en organisatorisk nivå i form av exempelvis ökad separering av system, framtagande av sårbarhetsanalys och bidragande till att förena olika synsätt på säkerhet inom IT och OT. Studien, som även går igenom vad olika standarder och vägledningar säger om utbildning kommer att publiceras på www.msb.se/ics.

Uppkopplade styrsystem i Sverige

FOI har på uppdrag av MSB utvecklat en metod för att via öppna databaser (Censys och Shodan) identifiera vilka industriella informations- och styrsystem och andra komponenter som samhällskritiska verksamheter i Sverige har anslutna till Internet. Rapporten kommer inom kort publiceras på www.msb.se/ics.

Årsrapport om obligatorisk incidentrapportering

Den första årsrapporten har nu tagits fram i nära samarbete med Säkerhetspolisen och Försvarsmakten och lämnats till regeringen. Arbetet med it-incidentrapportering är i sin linda och rapporteringsprocessen kommer att utvecklas.

Från rapportering framkommer bland annat att det finns brister i loggningen av it-system, exempelvis brister på dedikerade loggservrar vilket är en viktig komponent för övervakning av och för att i efterhand ha möjlighet att klargöra vad som hänt i systemet.

https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Forsta-arsrapporten-inlamnad-till-regeringen-om-arbetet-med-allvarliga-it-incidenter/

Rapport om OPC UA från tyska BSI

Den tyska säkerhetsmyndigheten BSI har publicerat en analys om säkerheten i OPC-UA (Open Platform Communications Unified Architecture). Rapporten, som tidigare bara funnits tillgänglig på tyska finns nu även på engelska:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA.html

Övervakning av system baserad på fysikaliska egenskaper

Amerikanska NIST har publicerat en artikel om övervakning av system baserad på fysikaliska egenskaper hos kontrollsystem där CERCES-projektledaren professor Henrik Sandberg medverkat. Artikeln går igenom tidigare forskning inom området och presenterar ett sätt på hur resultat kan jämföras och vilka utmaningar som återstår.
https://www.nist.gov/publications/survey-and-new-directions-physics-based-attack-detection-control-systems.
CERCES är ett av två MSB-finansierade forskningsprojekt inom området säkerhet i industriella informations- och styrsystem.

Artikel om cyberförsäkringsmarknaden i Sverige

Ulrik Franke, forskare på RISE/SICS, har som en del av ett MSB-finansierat forskningsprojekt publicerat en första artikel om cyberförsäkringsmarknaden i Sverige. Artikeln, *The cyber insurance market in Sweden*, som publiceras i tidskriften Computers & Security är fritt tillgänglig för alla och hittas här: http://dx.doi.org/10.1016/j.cose.2017.04.010

ITS

Dagens fordon är i hög grad uppkopplade, men i närtid förväntas än högre uppkopplingsgrad, bl.a. mot varandra och mot väginfrastrukturen. Europeiska kommissionen är starkt pådrivande i arbetet med ” Cooperative Intelligent Transport Systems” (C-ITS), se bl.a. COM(2016)76, vilket kommer att öka trafiksäkerheten och bana vägen för självkörande fordon. Cybersäkerhet är en nyckelkomponent för fungerande C-ITS och kommissionen avser därför publicera en vägledning rörande en EU gemensam säkerhets och certifikat policy under 2017. MSB deltar med expertkompetens i den arbetsgrupp som tar fram de båda dokumenten.

NIS-utredningen

Förslaget finns nu att läsa på:
http://www.regeringen.se/498cec/contentassets/9330610dab214a40a23730d2ef75d274/informationssakerhet-for-samhallsviktiga-och-digitala-tjanster-sou-201736

ICSJWG

MSB var med på vårens ICSJWG-möte i Minneapolis v11 och bidrog med en föreläsning om hur utbildning förstärker resultatet av en organisation säkerhetsarbete – baserat bland annat på erfarenheter från de grundläggande kurser MSB tillhandahåller tillsammans med FOI. Andra ämnen som diskuterades på konferensen var bland annat ransomware inom ICS och vikten av att identifiera de allra viktigaste styrsystemen och skydda dessa från logiska problem genom exempelvis extra robusta lösningar eller genomtänka fysiska begränsningar.

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. Informationsbladet är producerat april-maj 2017.