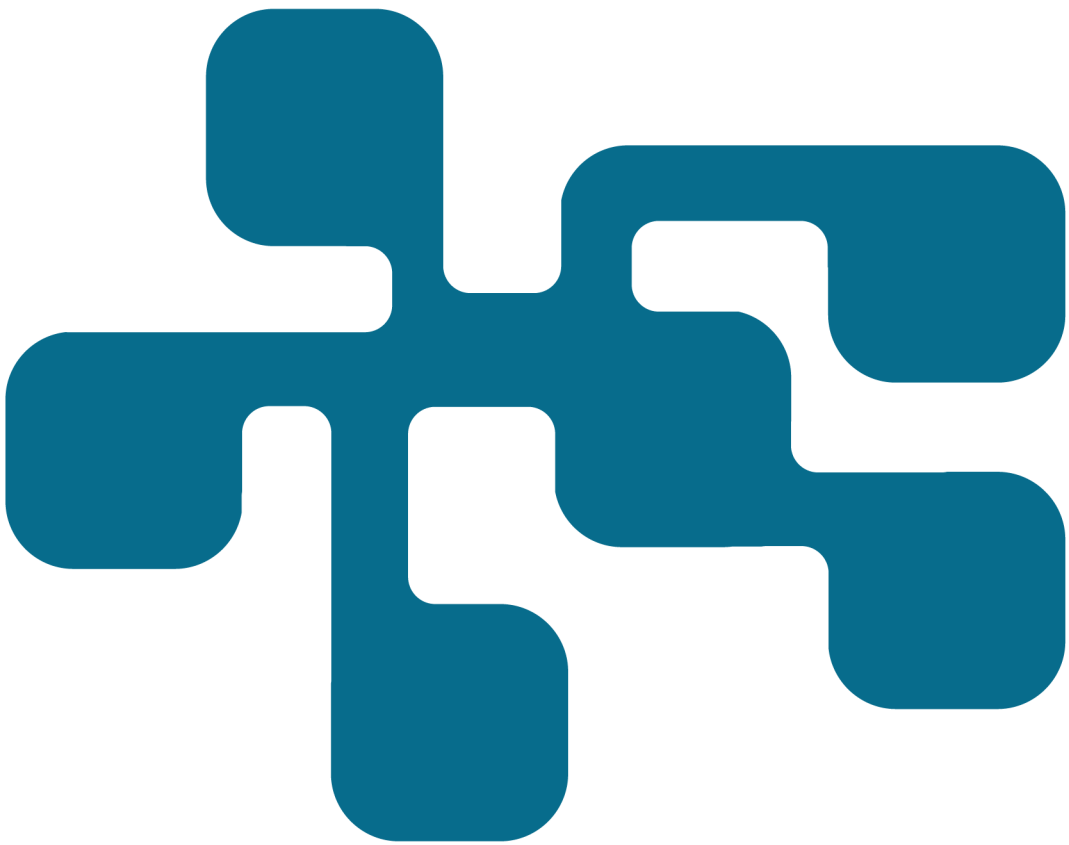
NCS3 2016 - verksamhetsrapport

Lars Westerdahl

FOI
MSB



FOI-R--4575--SE
MSB 2016-1329
ISSN 1650-1942

Februari 2018

Lars Westerdahl

NCS3 2016 - verksamhetsrapport

Titel	NCS3 2016 - verksamhetsrapport
Title	NCS3 2016 - Activity Report
Rapportnr/Report no	FOI-R--4575--SE
Månad/Month	Februari
Utgivningsår/Year	2018
Antal sidor/Pages	25
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ej FoT
Projektnr/Project no	E72017
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är en del av ett program hos *Myndigheten för samhällsskydd och beredskap* (MSB) för att stärka säkerheten i de system som utgör kritisk infrastruktur. Det arbete som utförs inom NCS3 regleras via uppdrag från MSB. I denna rapport sammanfattas de uppdrag som överenskommits under 2016.

Genom 2016 års överenskommelser har 16 uppdrag utförts under perioden 2016–2017. Dessa uppdrag har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på *Totalförsvarets forskningsinstitut* (FOI). Uppdragen omfattade bland annat fem studier och fem kurstillfällen, samt medvetandehöjande aktiviteter såsom föredrag.

Nyckelord: NCS3, industriella informations- och styrsystem, industriella kontrollsystem, kritisk infrastruktur.

Summary

The National Center for Security in Control Systems for Critical Infrastructure (NCS3) is part of a program at the *Swedish Contingencies Agency* (MSB) for enhancing security in those systems that constitutes critical infrastructure. The work that is conducted within NCS3 is regulated through assignments from MSB. In this report, the assignments that were agreed upon in 2016 are summarized.

In 2016, 16 assignments were agreed upon and carried out during the period 2016–2017. These assignments were carried out at the *Swedish Defence Research Agency* (FOI), by the division of Defence Analysis and C4ISR respectively. The assignments included five studies and five course offerings, as well as awareness increasing activities such as talks.

Keywords: NCS3, Industrial Control System, Critical Infrastructure

Innehållsförteckning

1 Inledning

I denna rapport sammanfattas det arbete som utförts inom de överenskommelser som ingåtts under 2016 rörande arbetet inom *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3). Arbetet har utförts av avdelningarna Försvarsanalys respektive Ledningssystem på *Totalförsvarets forskningsinstitut* (FOI).

För 2016 års verksamhet upprättades 16 separata överenskommelser. Kunskaps-uppbyggnad har varit ett tydligt tema i arbetet, vilket märks genom att fler studier har genomförts jämfört med tidigare. Arbetet inom dessa överenskommelser har genomförts under perioden 2016–2017.

1.1 Om NCS3

NCS3 är ett kunskapscentrum som startades 2007 med fokus på IT-säkerhet relaterad till industriella informations- och styrsystem inom samhällsviktig verksamhet. Mycket av centrumets verksamhet är centrerad kring en teknisk laborativ miljö och dess kringverksamhet som finns vid FOI i Linköping, men en del av arbetet utförs även vid FOI i Stockholm.

NCS3 och dess verksamhet syftar till att minska de risker som nyttjandet av digitala system för styrning av samhällsviktig infrastruktur medför, speciellt med avseende på avsiktlig störning. Vidare syftar kunskapscentrumet till att bibehålla en hög statlig kompetens inom området. Uppdragen har bestått av såväl stöd till *Myndigheten för samhällsskydd och beredskaps* (MSB) nationella program (från 2009 och framåt) som tekniskt inriktad verksamhet avseende IT-säkerhet. Namnet NCS3 etablerades 2010.

Det långsiktiga målet med NCS3:s verksamhet är att öka säkerheten i industriella informations- och styrsystem och därigenom öka förmågan att förebygga och hantera störningar i samhällsviktig verksamhet och kritisk infrastruktur i Sverige. För att uppnå detta mål krävs ett långsiktigt säkerhetsarbete som inkluderar:

- medvetenhet om sårbarheter, risker och möjliga åtgärder
- kompetens avseende säkerhet i industriella informations- och styrsystem
- förmåga att analysera aktuella risker och brister
- förmåga att kravställa säkerhet i industriella informations- och styrsystem.

NCS3:s vision och strategi återfinns i sin helhet i dokumentet *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017*[1].

De viktigaste målgrupperna för NCS3:s verksamhet är

- aktörer som äger och driver samhällsviktig verksamhet och kritisk infrastruktur som är beroende av industriella informations- och styrsystem
- sektors- och tillsynsmyndigheter (bland annat inom Samverkansområde teknisk infrastruktur, SOTI)
- myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI).

All verksamhet inom centrumet bygger på en nära samverkan mellan FOI och MSB. Samarbetet regleras genom överenskommelser vilka ingås under varje budgetår.

1.2 Slutrapportens uppbyggnad

I kapitel 2 presenteras de leveranser som NCS3 har producerat under 2016 års överenskommelser. Kapitel 3 sammanfattar den verksamhet som kategoriseras som medvetandehöjande aktiviteter. I kapitel 4 beskrivs de kunskaps- och förmågehöjande aktiviteter som utförts. Utvecklingen av NCS3:s tekniska och pedagogiska plattform presenteras i kapitel 5. De studier som genomförts sammanfattas i kapitel 6. Avslutningsvis beskrivs den övriga verksamhet som kallas för *centrumverksamhet* i kapitel 7.

[1] Wedlin, M. & Hallberg, J. (2012). *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017* (FOI Memo 4166).

2 Leveranser

Leveranser från NCS3 utgörs av rapporter och memon samt olika typer av aktiviteter.

2.1 Skriftliga leveranser

Nedan redovisas NCS3:s skriftliga leveranser sorterat under de överenskommelser som efterfrågat leveranserna.

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016 NCS3 - Delbeställning: **Deltagande i övergripande arbete för FOI Ledningssystem** (FOI-2016-485, MSB 2016-407)

- Westerdahl, L. (2016). *Statusrapport för ÖK Deltagande i övergripande arbete för FOI Ledningssystem* (FOI Memo 5927).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, Delbeställning: **Projektkoordinering och centrumverksamhet vid NCS3s tekniska plattform i Linköping** (FOI-2016-486, MSB-2016-1329)

- Westerdahl, L. (2016). *Statusrapport NCS3 2016 – kvartal 1* (FOI Memo 5674).
- Westerdahl, L. (2016). *Statusrapport NCS3 2016 – kvartal 2* (FOI Memo 5755).
- Westerdahl, L. (2016). *Statusrapport NCS3 2016 – kvartal 3* (FOI Memo 5808).
- Westerdahl, L. (2017). *Statusrapport NCS3 2016 – kvartal 4* (FOI Memo 5990).
- Westerdahl, L. (2018). *NCS3 2016 – Verksamhetsrapport* (FOI-R--4575--SE).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av grundläggande kurs – SI3S** (FOI-2016-410, MSB-2016-1323)

- Lindahl, D. (2016). *Kursredovisning SI3S VT 2016* (FOI Memo 5773).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, NCS3 - Delbeställning: **Distansvisning av miniatyrlandskapet steg 1 och steg 2** (FOI-2016-677, MSB-2016-2429)

- Andersson, P. (2016). *Distansvisning av miniatyrlandskap* (FOI Memo 5727).
- Andersson, P. (2016). *Teknisk lösning för distansvisning av miniatyrlandskap* (FOI Memo 5943).
- Andersson, P. (2016). *Användarinstruktion för distansvisning av miniatyrlandskap* (FOI Memo 5944).
- Westerdahl, L. (2016). *Dokumentation av scenario och presentationsmaterial – elscenario* (FOI Memo 5934).
- Andersson, P. (2016). *Dokumentation av aktiv komponent eldistribution* (FOI Memo 5942).
- [Bildspel] Möjliga konsekvenser av ett elsabotage (FOI-2016-677:7).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, NCS3 - Delbeställning: **Utveckling av kursverksamhet** (FOI-2016-1080, MSB-2016-3563)

- Andersson, P. (2017). *Ångmaskinsdemonstratorn* (FOI Memo 6098).
- Westring, E. & Westerdahl, L. (2017). *Automatisering av angrepp* (FOI Memo 6016).
- Westerdahl, L. (2016). *Utveckling av övningsdokumentation* (FOI Memo 5960).
- Lindahl, D. (2016). *Utveckling av I4S målbildsövning* (FOI Memo 5961).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, NCS3 - Delbeställning: **Industriella protokoll i Sverige** (FOI-2016-1078, MSB-2016-3717)

- Eidenskog, D. & Lindahl, B. (2017). *NCS3 – Industriella protokoll i Sverige* (FOI-R--4438--SE).
- Bildspel med presentation.

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, NCS3 - Delbeställning: **Monitorering- och övervakningssystem** (FOI-2016-1082, MSB-2016-3718)

- Hunstad, A.G. & Karresand, M. (2017). *Monitorerings- och övervakningssystem – En kategorisering och översikt av IDS-teknik inom IIS* (FOI-R--4420--SE).
- Bildspel med presentation.

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, NCS3 - Delbeställning: **Kursmodul forensik** (FOI-2016-1079, MSB-2016-3719)

- Karresand, M. (2016). *Slutleverabel NCS3 Kursmodul forensik* (FOI Memo 5962).
- Bildspel med presentation.

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av kurs – I4S** (FOI-2016-1332, MSB-2016-2587)

- Westerdahl, L. (2016). *Kursutvärdering I4S NCC* (FOI Memo 5973).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av grundläggande kurs – SI3S** (FOI-2016-1333, MSB-2016-5100)

- Lindahl, D. (2016). *Utvärdering av kursen SI3S 16-17 november 2016* (FOI Memo 5916).

NCS3-studie - **Styrsystem anslutna till Internet** (FOI-2016-1334, MSB-2016-5134)

- Holm, H. (2017). *NCS3: Internetanslutna styrsystem i Sverige – En studie av Censys och Shodan* (FOI-R--4415--SE).
- Bildspel med presentation.

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av förkortad grundläggande kurs – SI3S och deltagande på leverantörsmöte** (FOI-2016-1584, MSB-2016-5830)

- Westerdahl, L. (2016). *Utvärdering av leverantörsworkshop och kortkurs SI3S* (FOI Memo 5926).

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016 Delbeställning: **Deltagande i övergripande arbete** (FOI-2016-235, MSB 2016-407)

- Inga leveranskrav.

NCS3 Förstudie – **beroendekedjor till ICS och cyberfysiska system** (FOI-2015-345, MSB 2015-1075)

- Hedtjärn Swaling, V. (2016). *NCS3 Förstudie – Beroenden till industriella informations- och styrsystem* (FOI Memo 5588:2).

- Hedtjärn Swaling, V. & Mossberg Sonnek, K. (2016). *NCS3 – Beroenden till industriella informations- och styrsystem – En förstudie* (FOI-R--4280--SE).

NCS3 Studie: **Kursverksamhetens påverkan på organisationers säkerhetsarbete** (FOI-2016-631, MSB 2016-2331)

- Stenérus Dover, A-S. & Trané, C. (2016). *NCS3-studie: Påverkan på organisationers säkerhetsarbete av kursverksamhet inom området säkerhet i industriella informations- och styrsystem* (FOI Memo 5920).
- Bildspel med presentation.

NCS3 Studie: **Översikt över samhällsviktiga cyberfysiska system på kommunal nivå** (FOI-2016-292, MSB 2016-1196)

- Malmberg Andersson, F. & Stenérus Dover, A-S. (2016). *NCS3 – Översikt över arbetet med cyberfysiska system på kommunal nivå* (FOI-R--4370--SE).

Studie NCS3: **Åldrande informations- och styrsystem** (FOI-2015-1990, MSB 2015-6559)

- Hedtjärn Swaling, V., Malmberg Andersson, F. & Mork, J.C. (2016). *NCS3 – Gammal är inte äldst* (FOI-R--4292--SE).
- Hedtjärn Swaling, V. (2016). *Ageing ICS – What's the Deal* (FOI Memo 5821).

2.2 Övriga leveranser

Utöver skriftliga rapporter och memon har även nedanstående aktiviteter genomförts under 2016.

2.2.1 Föredrag, presentationer och deltagande

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016 NCS3 - Delbeställning: **Deltagande i övergripande arbete för FOI Ledningssystem** (FOI-2016-485, MSB 2016-407)

Datum	Aktivitet
17 juni	Trafikverksworkshop
26–27 oktober	4SICS

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016 Delbeställning: **Deltagande i övergripande arbete** (FOI-2016-235, MSB 2016-407)

Datum	Aktivitet
24–25 augusti	ICS-CSR

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av förkortad grundläggande kurs – SI3S och deltagande på leverantörsmöte** (FOI-2016-1584, MSB 2016-5830)

Datum	Aktivitet
15 november	Leverantörsworkshop

2.2.2 Kurser

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av grundläggande kurs – SI3S** (FOI-2016-410, MSB-2016-1323)

Datum	Kurs	Målgrupp
18–19 maj	SI3S	Transportsektorn
24–25 maj	SI3S	Kommuner

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av kurs – I4S** (FOI-2016-1332, MSB-2016-2587)

Datum	Kurs	Målgrupp
22–25 november	I4S	Nordiska Certarbetet

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av grundläggande kurs – SI3S** (FOI-2016-1333, MSB-2016-5100)

Datum	Kurs	Målgrupp
16-17 november	SI3S	Kommuner

Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2016, **Genomförande av förkortad grundläggande kurs – SI3S och deltagande på leverantörsmöte** (FOI-2016-1584, MSB-2016-5830)

Datum	**Kurs**	**Målgrupp**
15 november	SI3S (kortkurs)	Leverantörer

3 Medvetandehöjande aktiviteter

En stor del av arbetet inom NCS3 har under året varit kopplat mot att stärka de produkter som NCS3 har samt att öka kunskapen inom området bland NCS3:s medarbetare. Detta innebär att färre föreläsningar har genomförts under 2016 jämfört med tidigare år. En viss föreläsningsverksamhet genomfördes dock.

Flera medarbetare deltog på konferensen 4SICS i Stockholm den 26–27 oktober. Två medarbetare höll ett föredrag om samhällskonsekvenser vid en längre tids elavbrott och illustrerade detta bland annat genom att visa konsekvenser i miniatyrlandskapet CRATE City. Visningen av CRATE City skedde på distans via internetanslutna kameror. Ytterligare en medarbetare föreläste vid detta tillfälle om resultat från studien om åldrande industriella informations- och styrsystem.

Inom ramen för NCS3 genomfördes även en föreläsning om ryskt militärt tänkande under ett av FIDI-SCADA:s möten.

4 Kurser – kunskaps- och förmågehöjande aktiviteter

Den kursverksamhet som sker inom NCS3 baseras på två kurser: *Säkerhet i industriella informations- och styrsystem* (SI3S) samt *Praktisk incidenthantering i industriella informations- och styrsystem* (I4S). Under 2016 genomfördes fem kurstillfällen.

Kursen SI3S är en grundläggande IT-säkerhetskurs som riktar sig till tekniker och annan personal som arbetar med, eller i anslutning till, industriella informations- och styrsystem. Syftet med kursen är att deltagarna ska kunna arbeta aktivt med säkerhetsfrågor i sina egna system och få ett stöd för att kunna göra detta. Kursen genomförs oftast med inriktning mot en specifik sektor. De tre ordinarie SI3S-kurserna genomfördes enligt följande:

Inriktning	**Datum**
Transportsektorn	18–19 maj
Kommuner	24–25 maj
Kommuner	16–17 november

I samband med en leverantörsworkshop genomfördes även en förkortad version av SI3S-kursen under en dag. Kursen inriktades mot leverantörer, vilket här avser företag som levererar komponenter och färdiga kontrollsystem till operatörer. Denna grupp ligger bredvid den huvudsakliga målgrupp som kursen normalt riktar sig till.

Inriktning	**Datum**
Leverantörer	15 november

Kursen I4S genomfördes genom det nordiska CERT-samarbetet.[2] Nio deltagare från Danmark, Finland, Norge och Sverige övade incidenthantering i tre och en halv dagar. Kursen hade inför detta tillfälle uppdaterats för att ta hand om de återkopplingar som inkommit under de tidigare pilotkurserna. De främsta förändringarna var en anpassning av de förberedande övningarna samt införandet av en målbildsövning i syfte att förtydliga kursens genomförandeidé. Vid årets tillfälle hade även kursens innehåll breddats genom införandet av en kursmodul om IT-forensik.

[2] Nordic CERT Cooperation (NCC)

Kursen genomfördes under samma kursperiod som SI3S och leverantörs-workshopen.

Inriktning	Datum
Nordiska CERT-samarbetet	22–25 november

5 Teknisk utveckling

Inom NCS3 genomfördes en vidareutveckling av både den tekniska och den pedagogiska plattformen som ligger till grund för bland annat kursverksamheten. Utvecklingen syftade dels till att stärka plattformarna i syfte att öka leverans-säkerhet, dels till att stärka kursernas innehåll.

5.1 Utveckling av CRATE City

Miniatyrlandskapet CRATE City har tagits fram i syfte att tydligare kunna visa och lättare kunna diskutera samhällspåverkan av angrepp mot industriella informations- och styrsystem. I modellen finns en stad och ett omgivande landskap. För att visualisera effekter av angrepp finns det aktiva komponenter vilka påverkas när ett scenario spelas upp.

I årets arbete skapades ett sammansatt scenario för angrepp mot eldistributionen samt en berättelse över konsekvenserna av ett elavbrott placerat över en tidslinje. Angreppet följer i stora drag händelseförloppet som orsakade ett strömavbrott i Ukraina i december 2015, medans berättelsen är en sammanställning av uppgifter om samhällets påverkan av ett avbrott. När elsystemet angrips släcks belysningen ned i modellen, men startar igen för de delar som har en reservkraftslösning. Även reservkraftslösningarna släcks ned efter hand, beroende på vad de har för energikälla. Berättelsen kompletteras av ett bildspel där specifika konsekvenser visas.

Miniatyrlandskapet i sig är 4,5x1,5 meter vilket inte gör modellen flyttbar i någon praktisk mening. För att öka tillgängligheten till CRATE City har därför en distansvisningslösning tagits fram. Med hjälp av webbkameror kan landskapet vissas upp på en godtycklig skärm utanför FOI och genom samma kanal kan förberedda angrepp utföras, exempelvis vid en presentation.

I de fall då det inte är möjligt med en internetkoppling till CRATE, eller då bandbredden inte är tillräcklig, har även filmklipp över händelser i landskapet tagits fram. Filmklippen fångar samma scenario och berättelse som för en direkt eller fjärruppkopplad presentation.

5.2 Kursstöd

Ångmaskinsdemonstratorn utgör en central del i kursen SI3S och ingår numera även som ett delmoment i kursen I4S. Dokumentation om demonstratorn finns delvis sedan tidigare, men det fanns behov av att uppdatera denna samt komplettera dokumentationen över hur demonstratorn används inom NCS3. Den nya dokumentationen omfattar en övergripande beskrivning, ingående komponenter samt den virtuella organisation som är implementerad i CRATE.

Under övningsdagen i kursen I4S genomförs ett antal angrepp mot de system som deltagarna skyddar. Dessa angrepp är dels förberedda och schemalagda angrepp, dels manuella angrepp. De manuella angreppen förutsätter att angriparen är insatt i vad som ska göras. men utgör även en stressfaktor för övningsledningen då angriparen är mer eller mindre låst till denna uppgift. För att avlasta övningsledningen automatiserades fem angrepp genom att de implementerades i verktyget SVED.[3] Med SVED-stöd blir den person som har angriparrollen mer tillgänglig för att stödja övningen.

5.3 Kursförbättringar

Kursen I4S har tidigare genomförts som ett antal pilottillfällen i syfte att få återkoppling på kursupplägg och genomförande. Det har varit tydligt vid dessa tillfällen att deltagarna har haft svårt att ta till sig idén med hur övningen är tänkt att genomföras. För att förbättra deltagarnas förståelse för övningsupplägget skapades därför ett kursmoment i form av en målbildsövning. Målet med målbildsövningen är att deltagarna ska få se hur ett angrepp ser ut i de verktyg som används i kursen samt rapportera detta i rapporteringsverktyget CRATE Exercise Control (CEC).

En annan svårighet för deltagarna har varit att skapa en fungerande organisation och bemanna de roller som behövs för att genomföra övningen. Ett antal roller har föreslagits i kursdokumentationen, men dessa har inte varit utförligt beskrivna. En uppdaterad rollbeskrivning har tagits fram vilken, utöver för de obligatoriska rollerna, även ger en mer tydlig beskrivning av vilka roller som är lämpliga att bemanna för varje lag.

Inför årets I4S-kurs gjordes även en nyanskaffning av kursdatorer så att alla deltagare skulle få likvärdiga datorer med avseende på prestanda och skärmstorlek. 18 bärbara datorer med 15”-skärm införskaffades för detta ändamål.

[3] Scanning, Vulnerabilities, Exploits and Detection (SVED).

6 Studier

Under 2016 genomfördes fyra studier. Ytterligare tre studier påbörjades och genomfördes i huvudsak under 2016, men avslutas under våren 2017. En åttonde studie, *Bortom sakernas internet*, kommer huvudsakligen att utföras under 2017.

6.1 Beroendekedjor

Industriella informations- och styrsystem är idag en viktig del av samhällets funktionalitet. Dessa system kopplas samman allt mer med IT-system och andra nätverk, vilket kan medföra oanade konsekvenser då beroenden skapas mellan system. Målet med denna studie var att kartlägga vilka krav industriella informations- och styrsystem ställer på begrepp och metoder som används inom beroendeanalyser. I studien framgick att det är möjligt att identifiera beroenden, men att dessa ofta är komplexa.

6.2 Effekten av kurser inom ICS-säkerhet

Utbildning framhävs som en viktig komponent i säkerhetsarbete i de flesta rekommendationer som finns, och så även i MSB:s vägledning. NCS3 ger kurserna SI3S och I4S, vilka hittills har haft cirka 400 respektive 60 deltagare. En studie har genomförts för att undersöka vilken effekt kurserna har haft på deltagaren och den organisation de arbetar inom.

Kursdeltagarna beskriver sammantaget med flera exempel på att deras deltagande lett till ett förbättrat säkerhetsarbete inom respektive organisation. Även om den största påverkan av kurserna är på individnivå, exempelvis ökad medvetenhet, ges även exempel på där kurserna bidragit till faktiska förändringar på organisationsnivå.

6.3 Översikt över samhällsviktiga cyberfysiska system på kommunal nivå

Det finns en stor mängd industriella informations- och styrsystem i Sveriges kommuner som levererar grundläggande funktionalitet till kommunens invånare. Dessa system var tidigare huvudsakligen kommunalt ägda men numera kan de även vara privatägda. I denna studie var målet att uppskatta kunskapsnivån inom kommuner avseende industriella informations- och styrsystem, i syfte att få ett underlag för relevant stöd.

Resultatet från studien visar på en varierande grad av överblick och kontroll inom området. Typiska önskemål om stöd utgörs av guider, checklistor och mallar. Även konkreta exempel bedöms som värdefullt.

6.4 Åldrande system

Industriella informations- och styrsystem har långa livslängder vilket medför att de åldras på ett annat sätt än vanliga IT-baserade kontorssystem. Industriella system följer oftare ett underhållsschema vilket sätts utifrån verksamhetens behov, snarare än de ingående IT-baserade systemen. Stegvis utveckling och uppdatering kan även medföra att ett system kan ha flera generationer av samma komponenter i drift samtidigt. I denna studie undersöktes hur industriella informations- och styrsystem hanteras över systemets livslängd.

Resultat från studien visar att ett relativt åldrande kan vara problematiskt, genom att IT-baserade komponenter utvecklas snabbare än vad huvudsystem kan göra. Nyare industriella informations- och styrsystem går också mot mer generiska lösningar av kostnadsskäl, men även för att minska mängden speciallösningar. Mångfalden av generiska lösningar kan dock medföra lägre detaljkunskap, vilket försvårar ett säkerhetsarbete.

6.5 Monitorerings- och övervakningssystem

Det blir allt mer vanligt förekommande att industriella informations- och styrsystem ansluts till tredjepartssystem och även direkt till internet. Det är dock inte alltid möjligt att skydda dessa system på likande sätt som kan göras med traditionella IT-system, då dessa tekniker kan ha en negativ inverkan på kontrollsystemens funktion. I denna rapport presenteras ett ramverk för övervakningssystem för industriella informations- och styrsystem samt även exempel på forskning och kommersiella system inom området.

Resultat från studien visar på ett antal specifika förutsättningar som gäller för industriella informations- och styrsystem och dess möjlighet till övervakning. Exempelvis är möjligheten till autentisering ofta sämre i kontrollsystem vilket tillsammans med varierande grad av separation gör det svårt att skilja på legitim och avvikande sessioner.

6.6 Industriella protokoll i Sverige

Datorsystem kommunicerar enligt förutbestämda protokoll. Det finns ett stort antal publika protokoll, men även flera proprietära, särskilt inom industriella informations- och styrsystem. I denna studie har en undersökning genomförts i

syfte att klarlägga vilka protokoll som är vanligast förekommande inom kritisk infrastruktur, samt vilka egenskaper dessa protokoll har.

Genom en serie intervjuer framkom det att det är flera olika protokoll som används inom system för kritisk infrastruktur. Vilket protokoll som används verkar dock inte vara ett medvetet val vid en kravställning eller upphandling, utan påverkas mest av den funktionalitet som efterfrågas samt leverantörens preferenser.

6.7 Internetanslutna styrsystem i Sverige - En studie av Censys och Shodan

Industriella informations- och styrsystem blir allt mer beroende av komponenter och system från vanliga IT-system i sin dagliga funktion. Tillsammans med en ökad exponering mot internet leder detta dock till en ökad exponering mot antagonistiska aktörer som vill påverka systemens funktion. Det finns även system som är exponerade mot internet utan att ansvariga för systemen är medvetna om detta.

I denna studie identifierades internetanslutna system genom att använda databaserna Shodan och Censys. Även geodata för identifierade system undersöktes för att ge en bild av vilka samhällssektorer i Sverige som har system som är nåbara från internet. Resultatet visar att det finns internetanslutna komponenter inom flera sektorer, och att elkraft är den klart mest exponerade sektorn. Exponeringsgraden kan dock kopplas till att elkraftsbolag ibland agerar som internetleverantör själva vilket ger dem ett större antal egna IP-adresser. Det är sannolikt att det inom andra sektorer i större utsträckning anlitas internet-leverantörer för kommunikationen, vilket gör att det är internetleverantörernas adresser som exponeras.

7 Centrumverksamhet

Verksamhetsåret inleddes formellt med en kick-off, vilken MSB organiserade i Nyköping den 27–28 januari. Vid detta tillfälle deltog sex medarbetare från FOI och två från MSB. Under kick-offen presenterade MSB inriktningen för årets verksamhet och FOI presenterade resultat från 2015 års verksamhet.

En workshop genomfördes med FOI, MSB och Trafikverket. Syftet med workshopen var att presentera NCS3:s verksamhet för Trafikverket och diskutera hur NCS3 skulle kunna stödja Trafikverket i framtiden. Workshopen genomfördes den 16 juni.

Under året genomfördes ett par samverkansmöten mellan FOI och MSB i syfte att effektivisera samarbetet mellan myndigheterna. Det första mötet genomfördes den 12 april och var ett informationsmöte där beställningar och tankar om framtiden diskuterades. Ett andra möte i denna anda genomfördes den 20 september, där idéer och uppslag för uppdrag för 2017 diskuterades.

En medarbetare deltog på konferensen ICS-CSR[4] i Belfast den 24–25 augusti. Konferensen var den fjärde i ordningen och fokuserar på akademisk forskning med inriktningen mot säkerhet inom industriella informations- och styrsystem.

I slutet av året genomfördes en kortare workshop med leverantörer av industriella informations- och styrsystem. Deltagarna kom från nio företag av olika storlek, vissa med enbart en nationell marknad andra med en internationell. Syftet med workshopen var att få ett leverantörsperspektiv på säkerhetsfrågor rörande industriella informations- och styrsystem. I samband med workshopen, som genomfördes den 15 november, gavs även en kortversion av kursen SI3S för tekniker från deltagande företag.

[4] Industrial Control System – Cyber Security Research, https://www.ics-csr.com/ (besökt 2017-10-28).

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

MSB Swedish Civil Contingencies Agency

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se