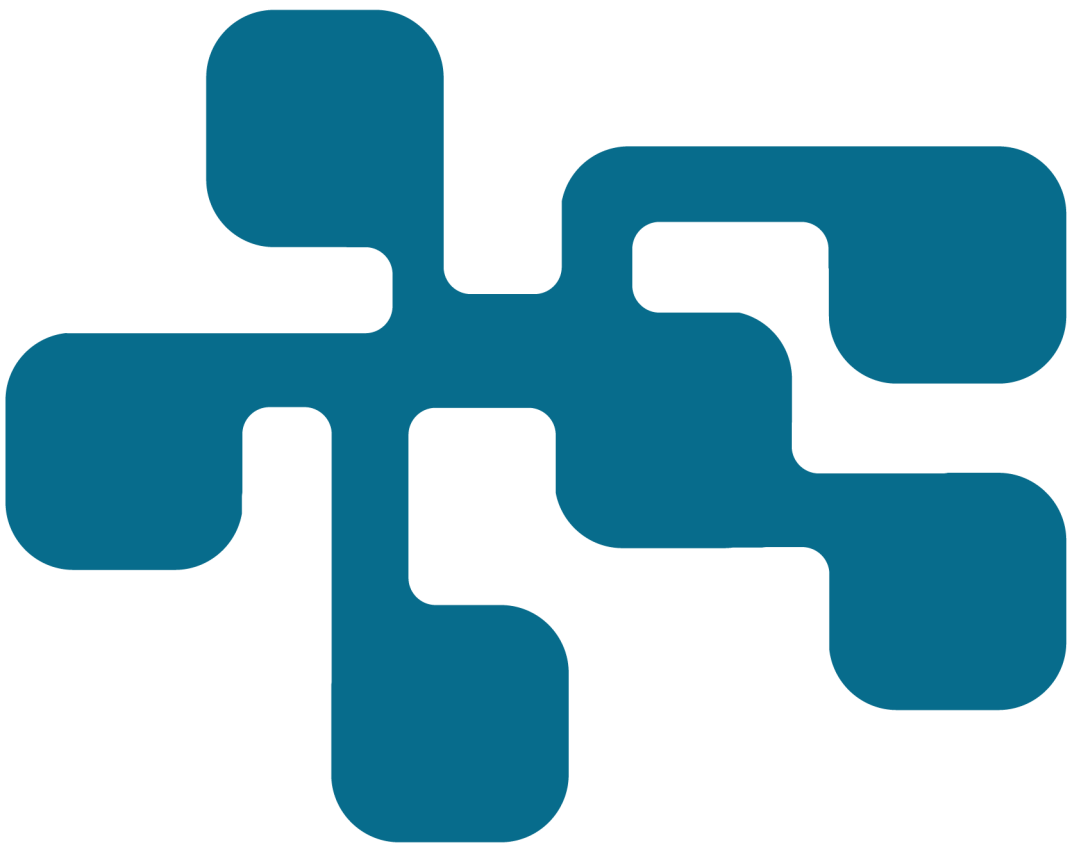
NCS3 - Virtualisering inom industriella informations- och styrsystem

En översikt

AMUND GUDMUNDSON HUNSTAD
CHRISTIAN VALASSI
DAVID LINDAHL

FOI
MSB



FOI-R--4603--SE
MSB 2017-1624
ISSN 1650-1942

Juni 2018

FOI-R--4603--SE

Amund Gudmundson Hunstad
Christian Valassi
David Lindahl

Virtualisering inom industriella informations- och styrsystem

En översikt

Titel	Virtualisering inom industriella informations- och styrsystem
Title	Virtualisation in ICS
Rapportnr/Report no	FOI-R--4603--SE
Månad/Month	Juni
Utgivningsår/Year	2018
Antal sidor/Pages	28
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72185
Godkänd av/Approved by	Chrstian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Virtualisering framträder i ökande grad som smidigt och attraktivt för industriella informations- och styrsystem. Säkerhetsmässiga avvägningar är dock nödvändiga vid övergång från traditionell till virtualiserad datordrift.

Denna rapport redovisar huvudtyper av virtualiseringslösningar och relaterade säkerhetsutmaningar. Med detta som utgångspunkt formuleras säkerhetsrelaterade rekommendationer för systemägare och operatörer av industriella informations- och styrsystem.

Studien drar som slutsats att virtualisering implicerar organisatoriska såväl som tekniska utmaningar och att leverantörsberoenden kräver noggranna överväganden. Detta indikerar vidare behov av planering avseende ansvarsfrågor, incidenthantering respektive risk- och sårbarhetsanalys.

Nyckelord: Industriella informations- och styrsystem, virtualisering, säkerhetsaspekter

Summary

Virtualization is emerging as convenient and attractive for the industrial control system community. There are however, a need for security related considerations regarding the transition from a traditional to virtualized operation of a computing environment.

This report presents the main types of virtualization and their related security challenges. With that in mind, a number of security related recommendations aimed at system owners and operators of industrial control systems are formulated.

The study concludes that virtualization implicates organizational, as well as technological challenges and that supplier dependencies requires careful considerations. This further indicates the need of planning regarding issues of liability, incident handling respectively risk and vulnerability analysis.

Keywords: Industrial control systems, virtualization, security aspects

Innehåll

1 Inledning

Virtualisering i en kontext av industriella informations- och styrsystem innebär att man skapar en virtuell kopia av ett fysiskt system. Detta kan vara ett mindre system som en enskild dator eller stora miljöer som serverhallar eller hela styrsystem för industriprocesser.

Virtualisering av tjänster, servrar och hårdvara öppnar för möjligheter att spara resurser som till exempel pengar och personal samtidigt som man kan behålla funktionalitetsnivåer och öka tillgängligheten i systemen. Denna kombination av fördelar gör det troligt att en överväldigande majoritet av framtida systemlösningar kommer att utnyttja virtualisering.

För industriella informations- och styrsystem kan detta, beroende på hur framtida lösningar ser ut, komma att innebära stora förändringar och säkerhetsutmaningar. Till exempel medför troligen virtualisering av servrar centralisering av IT-resurser. Centralisering underlättar uppbyggande av skalskydd, men samtidigt ökar beroendet av tillförlitlig kommunikation mellan centraliserade IT-resurser och verksamhetens olika delar.

Det förefaller därför viktigt att säkerhetsanalyser blir korrekt utförda när man fattar beslut om virtualiseringsåtgärder.

1.1 Bakgrund

Myndigheten för samhällsberedskap, MSB har gett FOI i uppdrag att studera konsekvenserna av virtualisering i styrsystem. Virtualisering är en teknik som kan användas för att separera hårdvara från mjukvara och bidra till effektivare förvaltning av system. Motiven bakom virtualisering har oftast varit ekonomiska vinster genom mer effektivt utnyttjad hårdvara, men kan även vara säkerhetsmässiga med avseende på tillgänglighet/driftsäkerhet och funktionalitet. Den ökande användningen av virtualisering inom området industriella styrsystem har lett till ett behov av att belysa virtualiseringens säkerhetsimplikationer.

1.2 Syfte, mål och avgränsningar

Syftet med studien är att beskriva förutsättningarna för virtualisering i kontexten industriella informations- och styrsystem och vad virtualisering innebär för praktisk verksamhet idag.

Målet med studien är att ta fram ett stöd som förtydligar området virtualisering för industriella informations- och styrsystem avseende fördelar, nackdelar, hot och risker, samt speglar erfarenheter inom området. Stödet ska kunna ligga som

underlag för hur en operatör inom industriella informations- och styrsystem väljer att arbeta med virtualisering.

Studien är avgränsad i och med att den främst avser virtualisering av servrar och nätverk, *inte PLC:er eller motsvarande komponenter.*

1.3 Målgrupp

Rapporten riktar sig till ingenjörer, arkitekter, beslutsfattare och liknande roller inom verksamhet kring industriella informations- och styrsystem.

1.4 Läsanvisningar

Kapitel 2 presenterar de metodiker som använts för att inhämta den information som ligger till grund för rapporten. Kapitel 3 redovisar vad virtualisering innebär och för dess säkerhetsmässiga implikationer. I kapitel 4 förs en diskussion kring virtualiseringens utmaningar och möjligheter, vilket leder fram till grundläggande rekommendationer för implementation av virtualisering i industriella informations- och styrsystem.

2 Metodik

Här presenteras den metodik som använts vid framtagning av den information som rapporten bygger på. Informationen är hämtad från öppna källor på internet och genom intervjuer med några aktörer inom området.

2.1 Litteratur

Översiktliga sökningar har gjorts i Scopus och Google Scholar för att finna vetenskapliga artiklar inom området. Även material från tidigare FOI-rapporter inom området har använts. Ingen av sökningarna har haft som mål att vara uttömmande, utan har använts för att skapa en översikt av det tillgängliga materialet inom området inför eventuella fördjupade studier. Specifikt har FOI-rapporten *Risker med virtualisering av IT-system* (Eidenskog & Karresand, 2017) och *Molntjänster inom industriella informations- och styrsystem* (Hunstad & Karresand, 2018) varit användbara då dessa författare utförde litteraturstudier inom områden som överlappar denna studie.

2.2 Intervjuer

För att intervjuer skall resultera i relevant datainsamling och på bästa möjliga sätt bidra till studiens slutresultat, är det av vikt att använda en tydlig och enkel intervjumetodik. Vi valde att utgå från *Intervjuguide arkitektur,* av Daniel Eidenskog (2015) och tillämpa huvuddragen av den metodik som redovisas i denna. I båda fallen ligger studiernas fokus på IT-säkerhet i komplexa system- och organisationssammanhang. Inom NCS3 genomförs parallellt med denna studie om virtualisering en studie om molntjänster, också inom industriella informations- och styrsystem och även i denna har det fungerat väl att använda metodiken från (Eidenskog, 2015). Likartade förutsättningar, mål och syften innebär att det är synnerligen lämpligt att använda samma metodik.

Metodiken i (Eidenskog, 2015) baserar sig på semistrukturerade intervjuer där en intervjuguide[1] används som utgångspunkt för intervjugenomförandet. Metodiken tar sin planeringsmässiga utgångspunkt i tre av (Kvale, 1997) påpekade viktiga frågeställningar inför en intervjustudie:

- *Vad*: Vilka förkunskaper som krävs inför intervjuerna, avseende allmän forskarkompetens, domänkunskap avseende studiens fokus och intervjuteknik

[1] Intervjuguiden återfinns i bilaga A.

- *Varför*: Vikten av att formulera ett tydligt syfte med intervjustudien.
- *Hur*: Genomförande av intervjuerna respektive bearbetning och analys av intervjumaterialet

Aktuell studie har fokus på virtualisering i industriella informations- och styrsystem, vilket därmed ställer krav på nödvändig domänkunskap vid intervjuerna. Intervjustudiens syfte framgår i avsnitt 1.2: Intervjuerna förväntas bidra, relativt litteraturen, med mera operativa kunskaper och erfarenheter av virtualisering i industriella informations- och styrsystem. Dessa kunskaper och erfarenheter torde vara värdefulla för syftet att beskriva förutsättningarna för virtualisering i kontexten industriella informations- och styrsystem, klargöra vad virtualisering innebär för praktisk verksamhet idag och att lyfta fram fördelar, nackdelar, hot och risker, samt spegla erfarenheter inom området.

Eidenskog (2015) påpekar vikten av att få respondenten att känna sig bekväm i intervjusituationen, genom att orientera om syftet med intervjun, stämma av huruvida inspelning av intervjun får göras och fråga om respondenten har funderingar inför intervjun. Inledningsvis är det bra att mjukstarta intervjun med enklare frågor om respondentens bakgrund och roll inom sin organisation. Vid intervjuns avslutning är det bra att mycket kort rekapitulera intervjuns observationer och öppna för kompletterande frågor och tankar från respondenten.

Förtroende mellan intervjuare och respondent är av betydande vikt för att lyckas med intervjuerna. Bra planering och struktur bidrar till detta, men även att avdramatisera intervjusituationen genom exempelvis inledande social konversation i samband med fika.

I valet mellan individuella intervjuer och gruppintervjuer har individuella intervjuer valts för att minska risken att någon respondent styr svaren och att grupptänkande uppstår.

Ansvaret på intervjuarsidan delas upp så att en person huvudsakligen ställer frågor och en annan person för anteckningar. För att underlätta arbete med renskrivning av intervjun görs inspelning av intervjuer, om inte respondenten motsätter sig detta. Anteckningar är dock den primära dokumentationen. Ingen fullständig transkribering av intervjuer genomförs. Istället eftersträvas att kunna identifiera påståenden, utsagor och observationer av vikt för studiens fokus och forskningsfrågor.

3 Virtualisering för ICS

3.1 Vad är virtualisering?

Virtualisering i IT-kontext innebär att man skapar en virtuell miljö, en mjukvarusimulering eller –emulering[2] av en datorresurs på vilken annan mjukvara kan köras som om simuleringen/emuleringen vore ett verkligt IT-system. (Scarfone, Souppaya & Hoffman, 2011). Datorresurs i den här kontexten ska förstås som hårdvara med eventuell mjukvara, till exempel en fysisk dator med ett operativsystem, eller enbart emulering av datorserverns fysiska egenskaper.

Tillämpningsvirtualisering innebär att man simulerar det programmerings-gränssnitt (API[3]) som ett tillämpningsprogram skrivits för på en annan typ av operativsystem eller omgivning.[4] Systemvirtualisering innebär att mjukvara för hela servrar körs i en virtualiseringsmiljö (Eidenskog & Karresand, 2017). Detta är den typ av virtualisering som oftast avses i kontexten industriella informations- och styrsystem och är den som kommer att avses i denna rapport om inget annat anges.

I Figur 1 visas de olika komponenter som ingår i en virtualiseringsserver. I ett serverrack med fysisk hårdvara, en server, körs ett program kallat hypervisor (eventuellt med ett mellanliggande värdoperativsystem). Överst i figuren ser vi de olika virtualiserade datorresurserna (i blått). Var och en av dessa är en emulering av en fysisk dator med eget operativsystem och egna tillämpnings-program.

Hypervisorn (även kallad Virtual Machine Monitor) sköter de simuleringar eller emuleringar som krävs för att en virtualiserad miljö ska skapas på vilken de olika gästoperativsystemen ska kunna köras. De olika virtuella maskinerna delar på de faktiska fysiska resurserna som finns tillgängliga. (NIST, 2011)

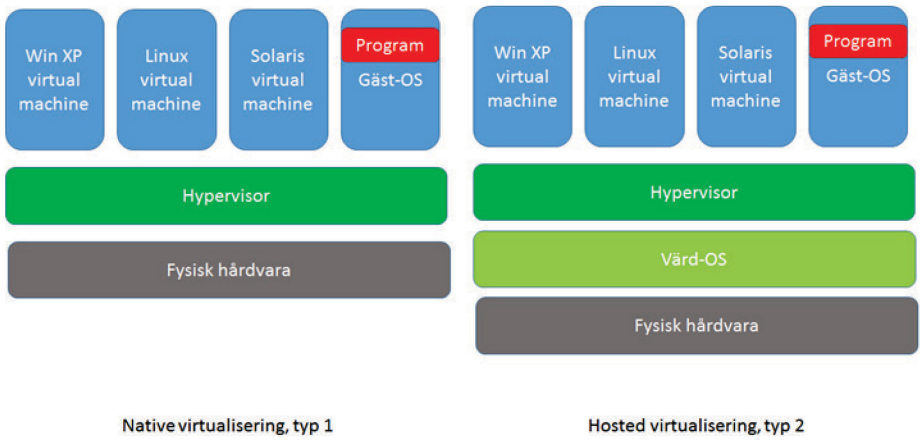
Det är även möjligt att köra en hypervisor direkt på hårdvara utan något annat operativsystem som mellanmjukvara. Denna typ av virtualisering kallas Typ 1, eller Native, medan den andra kallas typ 2, eller Hosted virtualisering. Svenska

[2] Skillnaden mellan simulering och emulering beskrivs enklast som att en simulering används om det inte behövs en översättning mellan de instruktioner som skickas mellan den fysiska hårdvaran och programmen som körs i den virtuella miljön. En emulering sker om en översättning är nödvändig.

[3] Application Programming Interface – Specificerar hur applikationer kan kommunicera och interagera med en specifik programvara

[4] Ett exempel skulle kunna vara Javas Virtuella Maskin

termer för denna uppdelning används i praktiken inte. (Eidenskog & Karresand, 2017)



Figur 1 Virtualiseringstyper

Den praktiska skillnaden är att typ 1 är mer effektiv eftersom inga hårdvaru-resurser behöver allokeras för värdoperativsystemet, men å andra sidan måste alla I/O-enheter hanteras i hypervisorn vilket kan vara lämpligare att sköta med ett dedikerat operativsystem.

3.2 Varför är virtualisering viktigt för ICS?

En virtualiserad miljö har ett antal stora fördelar jämfört med fysiska IT-system. För det mesta behövs inte en dators fulla kapacitet hela tiden. Genom att abstrahera det fysiska lagret kan ett större antal tillämpningar köras på en enskild dator och när extra datorresurser krävs kan tillämpningar dynamiskt flyttas till lediga maskiner, vilket gör att den totala mängden fysiska maskiner kan hållas mindre vilket i sin tur minskar kostnader. Virtualisering ger även möjlighet att i högre grad automatisera underhåll och uppdateringar.

En stor fördel med virtualisering är att det virtualiserade systemet/servern i praktiken bara blir en fil som kan säkerhetskopieras och flyttas med enkelhet. Detta gör det möjligt att få systemen mer driftsäkra genom att spara undan kopior av systemet, vilket innebär att om en fysisk maskin eller den virtuella instansen av någon anledning stängs ner eller fallerar kan en ny virtuell instans startas upp utan märkbar fördröjning.

Dessutom kan virtualisering användas för att göra systemen avsevärt mer flexibla. Om en del av verksamheten behöver fler servrar kan man skapa dessa

dynamiskt och på samma sätt ta bort maskiner som inte längre behövs, vilket frigör resurser.

Virtualisering gör det också betydligt enklare att verifiera systemuppdateringar och att återställa system om en förändring går fel, i och med att det då bara är att återställa en ögonblicksbild av systemet[5] eller i värsta fall att återläsa en säkerhetskopia. Det är också enklare att utveckla sina miljöer eftersom man kan testa i en identisk miljö.

Virtualisering är redan idag standard i IT-leveranser. Enskild hårdvara tenderar att inte längre vara ett alternativ, om man inte har specifika skäl.

Virtualisering gör ICS-systemen hårdvaruoberoende vilket gör att man kan byta fysisk hårdvara tre eller fyra gånger under gäst-serverns livslängd. Detta gör det möjligt att underhålla ICS-miljön längre och löser mer eller mindre problemet med att hålla liv i samma server i tjugo år.

Kortsiktigt kan det vara dyrare att implementera en virtualiserad miljö än en traditionell, men i längden kan besparingarna bli avsevärda. Det finns alltså många skäl att anta att virtualiserade miljöer kommer att bli framtidens standard inom industriella informations- och styrsystem.

3.3 Informationssäkerhet i ICS

Myndigheten för samhällsskydd och beredskap (MSB) beskriver i *Vägledning till ökad säkerhet i industriella informations- och styrsystem* hotbilden enligt följande:

> *Gränserna mellan traditionella/administrativa IT-system och industriella informations- och styrsystem håller på att suddas ut i och med en ökad integrering mellan dessa olika system. För att uppnå hög flexibilitet och effektivitet görs industriella informations- och styrsystem även i allt högre grad tillgängliga via Internet och andra publika nätverk. Dagens industriella informations- och styrsystem bygger dessutom allt mer på samma teknik som vanliga IT-system och drabbas därmed av samma säkerhetsproblem. Resultatet av denna utveckling är en ökad attackyta och radikalt förändrad riskbild*. (MSB, 2014)

Det är rimligt att anta att den information som används för att styra kritisk infrastruktur måste skyddas mot angrepp. Men vad ska skyddas, hur ska det skyddas och vad är hoten?

[5] Så kallad återställningspunkt eller snapshot.

I *Terminologi för informationssäkerhet* beskrivs informationssäkerhet som ”bevarande av konfidentialitet, riktighet och tillgänglighet hos information” (SIS, 2015). Denna triad av egenskaper benämns generellt CIA[6].

Konfidentialitet kan beskrivas som att den information som obehöriga inte bör känna till, inte ska göras tillgänglig eller avslöjas. **Riktighet** som att information som sänds, eller lagras i systemet inte har ändrats av någon obehörig. **Tillgänglighet** innebär att information ska finnas tillgänglig för ett system eller en användare när den behövs.

Olika branscher har historiskt sett fokuserat på olika delar av triaden. De normala kontorsmiljöerna hanterar affärsinformation som inte bör spridas, och som absolut inte får förändras. Exempelvis personregister, kontrakt och verksamhetskritisk information. Däremot är tidsaspekten relativt oviktig. Om något går fel och ett epostmeddelande kommer fram några minuter försenat, eller om datorn måste startas om för en uppdatering spelar för det mesta mindre roll eftersom människor arbetar i en långsam takt jämfört med datorer. Här är alltså riktighet och konfidentialitet prioriterade.

Industriella produktionsmiljöer har haft helt andra prioriteringar. Om ett styrkommando inte kommer fram, eller kommer fram för sent kan resultaten bli katastrofala. På samma sätt kan ett larm som missas, eller tolkas fel leda till allvarliga problem inom mycket kort tid. Tillgänglighetsaspekten är alltså traditionellt den viktigaste för industristyrning.

Det finns en faktor till som är viktig för informationssäkerheten. Det svenska språket har bara ett ord för det som på engelska kallas *security* respektive *safety*. Förenklat kan man säga att safety innebär att systemet inte ska kunna skada någon. Security innebär att ingen ska kunna skada systemet och dess information.

Inom den svenska industrin har, historiskt sett, säkerhet varit synonymt med safety. Denna syn på säkerhet är inte begränsad till Sverige. Sökmotorn Shodan[7] visar tusentals industriella system som är uppkopplade direkt mot Internet, i många fall utan säkerhetsåtgärder.

Den klassiska bilden av industriella informations- och styrsystem är att de finns på fysiskt isolerade platser där skalskydd förhindrar yttre påverkan. Men i och med centralisering och fjärrstyrning är det numera snarare regel än undantag att det finns fjärrkommunikation i form av 3G/4G- eller Internetuppkopplingar till och från systemen. I och med det ökande beroendet av kommunikationsteknik

[6] Efter den engelska förkortningen för Confidentiality, Integrity, Availability
[7] https://www.shodan.io/

har också hotbilden förändrats. Där man tidigare kunde klara sig med bra skalskydd för att skydda lokalt lagrad data och trafik måste nu även hela kedjan av informationsflöde genom tredjepartsmiljöer skyddas mot påverkan.

3.3.1 Hotbild och trender

Nedan följer en kort genomgång av några av de mest framträdande angreppen som utförts mot industriella informations- och styrsystem de senaste åren.

Exemplen är inte utvalda för att specifikt visa hot eller risker med virtualisering utan är tänkta att illustrera en mångårig trend; hot och angrepp mot industriella styrsystem inte bara pågår, utan utvecklas och blir mer sofistikerade över tid.

Energetic Bear/Dragonfly 2013

Från åtminstone början av 2013 utförde hackergruppen Dragonfly, också kallad Energetic Bear[8], datorintrång och spionage mot företag i energisektorn i Europa och USA (Symantec, 2014). De hade tidigare (åtminstone sedan 2011) riktat sig mot försvars- och flygsektorn i USA och Kanada. Angreppen verkade syfta till att hämta ut data om företagen, men också till förberedelse för framtida sabotage.

Black Energy 3 2015

Den 23 december 2015 orsakade ett datorintrång strömavbrott för kunderna till tre[9] olika energibolag i Ukraina (IR-ALERT-H-16-056-01, 2016). Angriparna hade under en period på mer än sex månader infiltrerat flera elkraftleverantörers organisationer och tagit kontroll över den datorstyrning som användes för att distribuera el till kunder. Strömavbrottet varade ungefär tre timmar för hälften av de 230 000 drabbade abonnenterna och upp till sex timmar för resterande. Men då angriparna sabotagerat många datorer med raderingsprogram kunde stora delar av nätverken inte styras automatiskt igen förrän nästan ett år senare (DRAGOS, 2017)

CRASHOVERRIDE 2016

Den 17 december 2016, alltså nästan exakt ett år efter det föregående angreppet mot de tre företagen i Black Energy 3-incidenten, anfölls ett ukrainskt kraftbolag[10] på nytt. Denna gång ledde angreppet till ett elavbrott i norra delen av Kiev, under ungefär en timme.

[8] Namnen kommer från de olika säkerhetsföretag som kartlagt attackerna. Vad angriparna själva kallar sig är inte känt.
[9] Prykarpattyaoblenergo i Ivano-Frankivsk Oblast, Chernivtsioblenergo i Chernitvtsi Oblast och Kyivoblenergo i Kiev Oblast
[10] Ukrenergo

Angreppet mot kraftstationen föregicks som i det förra el-angreppet av flera månaders oupptäckt tillträde till offrens nätverk (Polityuk, Vukmanovic & Jewkes, 2017).

Det som skiljer mellan angreppen 2015 och 2016 är att angriparna denna gång använde sig av skadlig kod för att direkt ta över kommunikationen med de olika delarna av styrsystemet. Detta är en markant kompetensökning jämfört med det tidigare infrastrukturangreppet (Kushner, 2013).

3.3.2 Sårbarheter, risker och exponering

Detta avsnitt diskuterar sårbarheter och exponeringsytor hos industriella informations- och styrsystem med avseende på virtualisering. Vissa av dessa sårbarheter och exponeringsytor är inte direkt relaterade till virtualisering, men de är även i detta sammanhang av vikt att beakta.

Alla anslutningar in till och ut från det industriella nätverket är en exponeringsyta som kan utnyttjas av en angripare. För att skydda sig är det därför viktigt att man är medveten om alla möjliga anslutningar som finns och tillåts i detta nätverk.

Fjärranslutningar är en populär attackvektor som nyttjas av angripare. Dessa anslutningar är ofta nödvändiga i anläggningar för att leverantörer skall kunna utföra uppdateringar och underhåll av sina produkter samt hämta diagnostik, vilket även gäller virtualisering. För att upprätta en säker anslutning krävs inte enbart att kommunikationen är skyddad, utan även att operatörens eller leverantörens lokala system är skyddade. Detta är speciellt viktigt om den fysiska virtualiseringsmiljön ligger hos en leverantör, då säkerheten hos leverantören kommer påverka det egna nätverkets säkerhet.

Trådlösa lokala nätverk så som Wi-Fi bör även kontrolleras och skyddas noggrant då detta nätverk kan sträcka sig utanför den fysiska plats där det är tänkt att användas. En potentiell antagonist kan även använda sig av en signalförstärkare för att få tillgång till nätverket från en avlägsen plats. Det är därför viktigt att nätverket har ett minimiskydd av ett lösenord. Beroende på vad för typ av kommunikation som flödar på nätverket så kan det även vara aktuellt att kryptera trafiken så att obehörig part inte kan läsa meddelandeinnehåll.

De incidenter som inträffar i industriella system och nätverk är långt ifrån alltid relaterade till en antagonist. Faktum är att en majoritet av de incidenter som inträffar beror på operatörmisstag, mjukvarufel och hårdvarufel (Kaspersky, 2014). För virtualisering är det därför viktigt att man utför implementation och testning korrekt och fullständigt för att undvika att man introducerar nya sårbarheter, mjukvarufel och hårdvarufel. Hur detta görs på bästa sätt kommer att skilja sig från installation till installation, men två viktiga moment för att säkerställa implementationen är här att rigoröst testa virtualiseringsmiljön och att utbilda personal.

Introduktionen av en sårbarhet på virtuella maskiner har potential att få väsentligt större konsekvenser än på en fysisk maskin. En ny version av fysisk maskin kommer att införas gradvis i takt med att gamla maskiner behöver ersättas, men en ny serverversion kommer att användas för att uppdatera en mycket stor del av alla befintliga virtuella maskiner förutom de nya som startas upp i framtiden. Eftersom endast ett fåtal företags produkter de facto används för att driva virtualiseringscenter kan alltså en uppdatering från dessa företag propageras till en signifikant andel av världens infrastrukturservrar inom några dygn. Samtidigt är det av vikt att notera att enkelheten i att byta ut en hypervisor har betydande fördelar gentemot att hantera fel i fysisk hårdvara.

Hypervisorn är en annan viktig aspekt att ta hänsyn till då denna i sig kan vara sårbar för angrepp. Under de genomförda intervjuerna anmärktes att en viss sådan programvara används för majoriteten av alla virtuella maskiner i världen och är dessutom konfigurerad på samma eller liknande sätt på de allra flesta maskiner. Om denna programvara på ett eller annat sätt skulle visa sig sårbar för angrepp skulle detta kunna innebära katastrofala konsekvenser.

Det kan även vara svårt att förutse komplex interaktion mellan virtualiserade och fysiska systemdelar. Detta kan i sin tur innebära skapande av oavsiktlig extra funktionalitet eller förminskad funktionalitet hos den virtuella maskinen. Ett exempel på detta är hanteringen av licenser då industriella informations- och styrsystem inte sällan förlitar sig på fysiska licensnycklar. Ett annat exempel är om en automatisk migrering mellan olika värdservrar sker och som i sin tur bryter kommunikationen via vlan.

Återanvändning av säkerhetsrelevanta tillstånd, som exempelvis kryptografiska nycklar eller aktivitetsdata, innebär en sårbarhet i den virtuella maskinen. Mer specifikt gäller dessa säkerhetsrelevanta tillstånd kryptografiska nycklar, loggar, slumptalsgeneratorer, raderade filer, aktivitetsdata och initialvektorer. Återanvändande av dessa tillstånd bör i största grad undvikas för att försvåra ett möjligt angrepp och undvika problem i normal drift.

Resursbrist hos den fysiska hårdvaran är ytterligare ett problem för virtuella maskiner. Detta problem kan leda till att en säkerhetsåtgärd eller reaktion på en incident resulterar i att en eller flera av de virtualiserade komponenterna förbrukar sin allokerade resurs och effektivt stjäl resurser från andra komponenter. Detta i sin tur påverkar funktionaliteten hos dessa komponenter och kan få en negativ effekt på både prestanda och tillgänglighet. Det finns också exempel på värdövergripande system såsom brandväggar och virusskydd som kan slå ut alla gästsystem på en värdserver.

Två nyligen publicerade sårbarheter, Meltdown & Spectre[11], är även väldigt relevanta att diskutera ur virtualiseringssynpunkt. Båda dessa sårbarheter rör

[11] https://meltdownattack.com/

informationsläckage från processorer, främst Intel och ARM[12]. Meltdown bryter ner barriären för minnesisolering mellan applikationer och ger otillbörliga processer tillgång till privilegierad information hos andra applikationer och operativsystemet. Spectre utnyttjar en funktionalitet hos moderna processorer kallat spekulativ exekvering[13]. Denna funktionalitet förekommer när processorn försöker förutspå resultatet av en grenexekvering och då exekverar flera möjliga grenar för att sedan förkasta de som inte nyttjas. Spectre utnyttjar detta för att få processorn att läcka konfidentiell information via sidokanaler från dessa spekulativa exekveringar. Spectre är svårare att utföra än Meltdown men också svårare att försvara sig mot.

För virtualisering innebär dessa sårbarheter ett större problem än för enskilda användare. Virtualisering sker ofta i kombination med en centralisering där ett stort antal separata datorer virtualiseras och placeras som processer i ett datacenter. I händelse av ett dataintrång kan sårbarheterna ovan medföra att data, som tillhör en viss process, går att nå från andra processer, och eftersom det stora antalet processer som finns ’inom räckhåll’ i datacentret kan läckan av information bli omfattande. Situationen kan förvärras om man som lösning på detta stänger av spekulativ grenexekvering då det markant kan försämra prestandan hos en processor. Det innebär att den förmåga som systemet har att snabbt växla mellan olika virtuella processer kan komma att fallera då realtidskraven inte kan uppfyllas.

Centraliseringen är alltså ett exempel på en felkritisk systemdel (i form av en Single point of failure, SPOF)[14] där en likriktad och allt mindre mängd hårdvara blir en flaskhals om fel skulle uppstå och med större konsekvenser. Samtidigt är det betydligt enklare att skapa system utan SPOF-problematik med virtualisering.

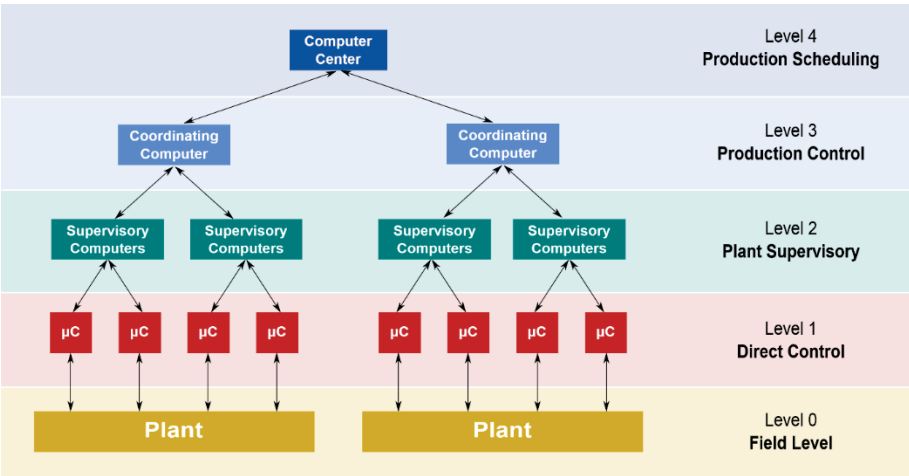
En annan sårbarhet som uppstår med virtualisering är att åtkomst till hanteringssystemet för hypervisorn också medger åtkomst till de gästsystem som exekveras på värdserverna . Det är därför mycket viktigt att man dels tillser att åtkomsten till hanteringssystemet endast kan ske från skyddade platser samt att man implementerar god autentisering av administratörerna. Inloggning ska endast vara möjlig via konton i en annan kontodatabas än vad som används för övriga IT-system.

3.3.3 Tredjepartsberoende

Det finns en långvarig trend inom all industriell verksamhet att fokusera på kärnverksamhet och hyra in tjänster för övrig verksamhet från tredje part. Detta gäller även den kritiska infrastrukturen. Resonemanget i detta avsnitt berör även

[12] Advanced RISC Machine
[13] Eng. Speculative Execution
[14] Eng. Single point of failure (SPOF)

frågor kring molntjänster, men som här diskuteras utifrån den relevans och påverkan de har i samband med virtualisering. FOI-rapporten *Molntjänster inom industriella informations- och styrsystem* (Hunstad & Karresand, 2018) analyserar utmaningar med molntjänster närmare.



Figur 2 Logiska nivåer i ett DCS-system (Pugliese, 2014)

Ett exempel på denna trend är SaaS eller SCADA-as-a-Service. Detta är lösningar där ett företag tillhandahåller datorcenter, programvara och kommunikation via internet för att köra styrsystem (SCADA-lösningar). Det som finns fysiskt hos operatören är maskinerna för industriprocessen, styrdatorer direkt monterade på maskinerna, samt någon form av utrustning för att övervaka driften, till exempel ett kontrollrum eller kontorsmiljö (Lager 0, 1 och delar av 4 i Figur 2). Allt annat, historian[15], kontrollservrar och så vidare finns virtualiserade hos SaaS-leverantören (Lager 2, 3 samt delar av lager 4 i Figur 2).

Säkerhetskonsekvenserna av denna typ av lösningar är blandade. På plussidan har vi att de som sätter upp och underhåller servrar och kommunikation troligen blir skickligare och mer säkerhetsmedvetna eftersom de är specialister. Samtidigt torde den centralisering som virtualisering leder till, medföra att datorcentra blir allt mer attraktiva mål för en angripare som vill orsaka skada.

Till detta kommer att många olika organisationer kommer att dela lagringsutrymme, minne och processorkraft på de fysiska servrar som finns i datorcentret. Det innebär att en ny säkerhetsfråga uppstår: att varje organisation ska kunna nå sina virtuella servrar, men inte någon annans och utomstående ska

[15] Detta är termen för den databas som lagrar historik, driftdata, under en längre tid.

inte komma åt systemet alls. Det har inträffat situationer, i laboratorier (Savage, 2017) och i verkligheten (McMillan, 2013; Wilts, 2017) där denna separation inte fungerat som avsett på grund av misstag från administratörer eller användare.

3.3.4 Utmaningar

Virtualisering innebär en rad nya utmaningar för de industrier och organisationer som applicerar denna teknik. De utmaningar som diskuteras i detta avsnitt är förankrade, delvis i de intervjuer som genomförts under studien och delvis i tidigare studier och utveckling inom virtualisering för industrisektorn.

När det kommer till administrativa utmaningar så uppkommer en hel del av dessa på grund av kulturskillnader mellan operativ teknologi (OT) i industriella processer och IT så som det används inom kontors- och servermiljöer. Som tidigare nämnt i avsnitt 3.3, präglas industriella styrsystem historisk av en fysisk isolering från omvärlden. Detta skapar problem då OT-system idag allt mer liknar IT-system, samtidigt som den interna kulturen bland beslutsfattare ligger kvar i bilden av från omvärlden isolerade system. Som respondent [INT A] uttryckte i sin intervju, så vill beslutsfattare sällan byta ut hårdvara och system innan de faktiskt går sönder, vilket enligt respondenten inte lämpar sig väl för system som blir allt mer lika IT-system och som har väldigt stora krav på tillgänglighet.

Yttranden från intervjuerna indikerar även ett större upplevt beroende av leverantörer än tidigare då en del som inte har den interna kunskapen eller medlen för att utföra virtualisering internt, förlitar sig på leverantörer i allt högre grad. Detta beroende beskriver respondent [INT A] som oroande då en allt större del av den interna arkitekturen hamnar utanför den interna möjligheten för kontroll. Samma problem upplevs dock inte av respondent [INT B] och [INT C] som innehar mycket av den kompetens och de medel som krävs internt i organisationen och då också en stor del av den infrastruktur som krävs för virtualisering.

Organisationer som implementerar virtualisering utsätts även för diverse tekniska utmaningar. Exakt vilka dessa är och hur de påverkar varierar från installation till installation. Exempelvis upplever respondent [INT A] att dennes organisation har fått sämre prestanda på en del av de maskiner som virtualiseras, vilket kan bero på en rad olika faktorer, som för många instanser per virtualiseringsvärd.

Ett annat problem är den monokultur som uppstår när en handfull av programvarutillverkare har den absoluta majoriteten av marknaden. Om en sårbarhet skulle finnas i den virtuella standardserver som någon av de största aktörerna tillhandahåller, kommer en angripare att kunna påverka en signifikant andel av all infrastruktur i världen.

Till detta kommer även att användare tenderar att betrakta en programvaru-uppdatering som säker när den använts ett par dygn, eftersom man antar att eventuella fel kommer att ha kommit fram vid det laget givet den totala mängd timmar som uppdateringen då har kört i alla virtuella maskiner i hela världen. Detta är ett rimligt antagande om man ser till oavsiktliga fel. Avseende avsiktligt introducerade fel från en illasinnad aktör kan läget vara annorlunda, vilket pekar på vikten av noggranna och strikta kontroller.

4 Diskussion och rekommendationer

Virtualisering av industriella informations- och styrsystem skapar både nya problem och möjligheter. Det är en synnerligen viktig teknik för hantering av servrar som troligen kommer att bli den helt dominerande modellen för dator-administration inom en nära framtid. Vinsterna i effektivitet, besparingar och driftsäkerhet kan bli avsevärda, vilket poängteras i aktuell forskningslitteratur men även i intervjuer genomförda inom denna studie.

Viktiga fördelar virtualisering möjliggör är

- högre grad av hårdvaruoberoende och redundans
- flexibilitet i resursutnyttjande
- förenklad licenshantering
- förenklad återställning.

Virtualisering innebär även vissa nackdelar:

- Licenshantering knyts till hårdvara
- Virtuella system på samma hårdvara påverkar varandra
- IT-kulturen inom organisationer tenderar att få företräde, till exempel vid kontinuitetsplanering.

Det finns dock ett antal nya säkerhetsrisker med virtualisering som en organisation måste ta hänsyn till inför och under övergången från traditionell datordrift till virtualiserad drift. Organisationen bör ha klart för sig vilka förändringar som måste göras i organisationen om organisationens fysiska servrar flyttas till ett centralt datacenter; rörande personal, driftkostnader, ansvar, felrapportering, debitering och så vidare. En utredning kring hur organisationen måste förändras och hur slutresultatet förväntas bli, bör finnas redo innan den första servern migreras. Om organisationen väljer att lägga uppgifter på entreprenad till en leverantör är det viktigt att man har klart för sig vilka säkerhetsmässiga konsekvenser det kan innebära och hur man hanterar detta. En plan rörande ansvar, incidenthantering och risk- och sårbarhetsanalys bör därför tas fram innan något beslut rörande entreprenad tas.

Ytterligare problem involverar den monokultur som skapas av att en handfull programvarutillverkare innehar den absoluta majoriteten av marknaden för virtualiseringsmiljöer. En sårbarhet i den virtuella standardserver som erbjuds av någon av de största aktörerna, kan innebära att en angripare får möjlighet att påverka en betydande andel av världens totala infrastruktur. Detta för även med sig att användare kan se en programvaruuppdatering som säker när denna har använts i ett par dygn, då man antar att eventuella fel eller sårbarheter kommer

att ha upptäckts vid det laget. Detta eftersom att den totala mängd användnings-timmar över alla användare i världen är väldigt stor. För implementationsfel eller kodrelaterade fel är detta rimligt att anta, men i fallet av avsiktliga fel behöver detta antagande inte stämma.

Denna rapport har beskrivit förutsättningar, fördelar, nackdelar hot och risker med virtualisering inom ramen för industriella informations- och styrsystem. Rapporten har dock en begränsning i att den inte speglar några misslyckade implementationsförsök av virtualisering inom denna kontext. Detta innebär att rapporten inte visar några direkta fallgropar som en organisation måste undvika för att lyckas med en implementation av virtualisering.

Litteraturförteckning

Cyber-Attack against Ukrainian Critical Infrastructure (IR-ALERT-H-16-056-01) (2016). *ICS-CERT*, 25 februari. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [2018-02-19]

DRAGOS (2017). *CRASHOVERRIDE Analysis of the threat to Electric grid Operations.* DRAGOS.

Eidenskog, D. (2015). *Intervjuguide arkitektur (FOI Memo 5310)*. Stockholm: Totalförsvarets forskningsinstitut, FOI.

Eidenskog, D., Karresand, M. (2017). *Risker med virtualisering av IT-system* (FOI-R--4448--SE). Stockholm: Totalförsvarets forskningsinstitut, FOI.

Hunstad, G. A., Karresand, M. (2018). *Molntjänster inom industriella informations- och styrsystem* (FOI-R--4597--SE). Stockholm: FOI.

[INT A] Intervju med automationsingenjör

[INT B] Intervju med IT-utvecklare

[INT C] Intervju med systemförvaltare för SCADA-system

Kaspersky (2014). *Industrial Security 2014. Cyberthreats to ICS systems - You Don't Have to be a Target to Become a Victim.* Kaspersky Labs. https://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf

Kushner, D. (2013). *The Real Story of Stuxnet.* IEEE Spectrum, 26 februari. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet [2018-03-12]

Kvale, S. (1997). *Den kvalitativa forskningsintervjun*. Lund: Studentlitteratur.

McMillan, R. (2013). Cloud Computing Snafu Shares Private Data Between Users. *Wired*, 2 april. https://www.wired.com/2013/04/digitalocean/ [2018-03-12]

Myndigheten för samhällsskydd och beredskap (MSB) (2014). *Vägledning till ökad säkerhet i industriella informations- och styrsystem.* Stockholm: MSB.

Scarfone, K., Souppaya, M. & Hoffman, P. (2011). *Guide to Security for Full Virtualization Technologies* (SP 800-125). National Institute of Standards and Technology (NIST). Gaithersburg: NIST

Pugliese, D. (2014) Functional Leveles of a Distributed Control System (DCS) (bild). *Wikimedia.* https://commons.wikimedia.org/wiki/File:Functional_levels_of_a_Distributed_Control_System.svg

Savage, N. (2017). *Keeping the Clouds from Leaking*. Worcester Polytechnic Institute. https://www.wpi.edu/news/keeping-clouds-leaking [2018-03-12]

Swedish Standards Institute (SIS) (2015). *Terminologi för informationssäkerhet* SIS-TR 50:2015. Stockholm: SIS.

Symantec (2014). Dragonfly: Western Energy Companies Under Sabotage Threat. *Symantec Official Blog* [blogg] 30 juni https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat [2018-03-12]

Wilts, A. (2017). US Data Leak: 198 million Americans' Personal Information Accidentally Released. *The Independent*, 19 juni. http://www.independent.co.uk/news/world/americas/us-politics/us-leak-data-americans-personal-information-deep-root-analytics-republican-national-committee-a7798251.html [2018-03-12]

Polityuk, P., Vukmanovic, O. & Jewkes, S. (2017). Ukraine's power outage was a cyber attack: Ukrenergo. *Reuters*, 18 januari. http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA [2018-05-13]

Bilaga A: Intervjuguide

Mål

Att få en bild av hur aktörer inom industriella styrsystem använt virtualisering. Mer specifikt

a) Vad innebär virtualisering för industriella informations- och styrsystem?
    - Hur påverkar styrsystemspecifika egenskaper virtualisering?
    - Vilka omständigheter gör virtualisering lämpligt eller olämpligt som lösning?
    - Vilka konsekvenser och risker finns med virtualiserings-lösningar för styrsystem?

b) Vilka förväntning har de intervjuade eller deras organisationer haft inför virtualisering

c) Hur har man gått till väga för att genomföra virtualisering

d) Vilka erfarenheter har man gjort under denna process

e) Hur förhåller sig resultatet till förväntningarna?

Bakgrund

Myndigheten för samhällsberedskap (MSB) har som ett led i sitt arbete inom säkerhet i industriella styrsystem gett i uppdrag till Totalförsvarets forskningsinstitut (FOI) att göra en mindre studie i form av intervjuer. Studien ska resultera i ett underlag som aktörer inom industriella styrsystemområdet kan ha som stöd när de väljer hur de ska arbeta med virtualisering.

Om intervjuerna och hur materialet kommer att användas

Intervjuerna genomförs som ett samtal mellan den intervjuade och forskare från FOI. Vid intervjuerna kommer en intervjuguide med en uppsättning frågor att användas som grund. Detta för att alla de områden som är intressanta för studien ska beaktas under intervjun. Intervjuarna kommer att ställa i huvudsak öppna frågor och vid behov avvika från guiden för att få ytterligare svar eller förtydliganden.

Intervjuerna kommer att spelas in och dokumenteras i form av de intervjuande forskarnas anteckningar. Efter intervjun kommer dessa anteckningar att sammanställas och kommer sedan att skickas till de intervjuade för kommentarer, detta för att säkerställa att inga missförstånd skett vid själva intervjun. De intervjuade ges således chansen att ändra eventuella felaktigheter samt att lägga till information som kanske missats under intervjuerna.

Resultaten från intervjuerna kommer att sammanställas och ligga till grund för en öppen FOI-rapport. Rapporten kommer att beskriva vad virtualisering är och hur det relaterar till informationssäkerhet. Rapporten kommer även att belysa ett antal områden som konsekvenser och risker med virtualisering och vilka slutsatser de intervjuade har dragit av sitt arbete med virtualisering.

Bakgrundsinformation om den intervjuade

1. Vilka erfarenheter har du/ni av virtualisering av styrsystem i ditt arbete?
2. Är informationssäkerhet något du/ni jobbar med regelbundet?
3. Hur länge har du/ni jobbat med virtualisering?

Inför virtualisering

4. Hur skulle du/ni beskriva vad virtualisering av styrsystem innebär?
5. Varför började er organisation med virtualisering?
6. Vilka förväntningar hade du/ni på virtualiseringen, vilka fördelar förväntade du/ni er?
7. Finns det någon etablerad metod för att virtualisera styrsystem? Användes den?
8. Hur såg arbetsgången inför virtualiseringen ut?
9. Hur tog du/ni reda på vad du/ni ville göra?
10. Hur kom du/ni fram till vilka krav virtualiseringlösningen skulle uppfylla?
11. Fanns det specifika krav som tillkom på grund av styrsystemspecifika egenskaper som tillgänglighetskrav el dyl?

    (Ingick det säkerhetsanalyser i denna? Informationssäkerhet?)

Genomförande virtualisering

12. Vem eller vilka var det som genomförde virtualiseringen? (roller)
13. Fanns det svårigheter? Vad?
14. Fanns det saker som fungerade oväntat väl? Vad?

Slutresultatet

15. Gav virtualisering de fördelar du/ni förväntade er? (Se fråga 5)
16. Har du/ni gjort någon informationssäkerhetsanalys av det nya systemet?

    (Resultat? Enligt förväntningar?)

17. Vilka erfarenheter har du/ni gjort som du/ni skulle velat veta innan du/ni genomförde virtualiseringen?

Förbättringsmöjligheter?

18. Har du/ni några konkreta förslag för andra som ska börja ett virtualiseringsarbete? [Återkoppla till frågor]
    (Behov, konkreta åtgärder, effekter)
    Finns det något av dessa som är viktigare än de övriga? Varför?
19. Finns det faktorer som skulle göra en virtualiseringslösning olämplig? Vilka?

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
Swedish Defence Research Agency
SE-164 90 Stockholm

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

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

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

www.msb.se