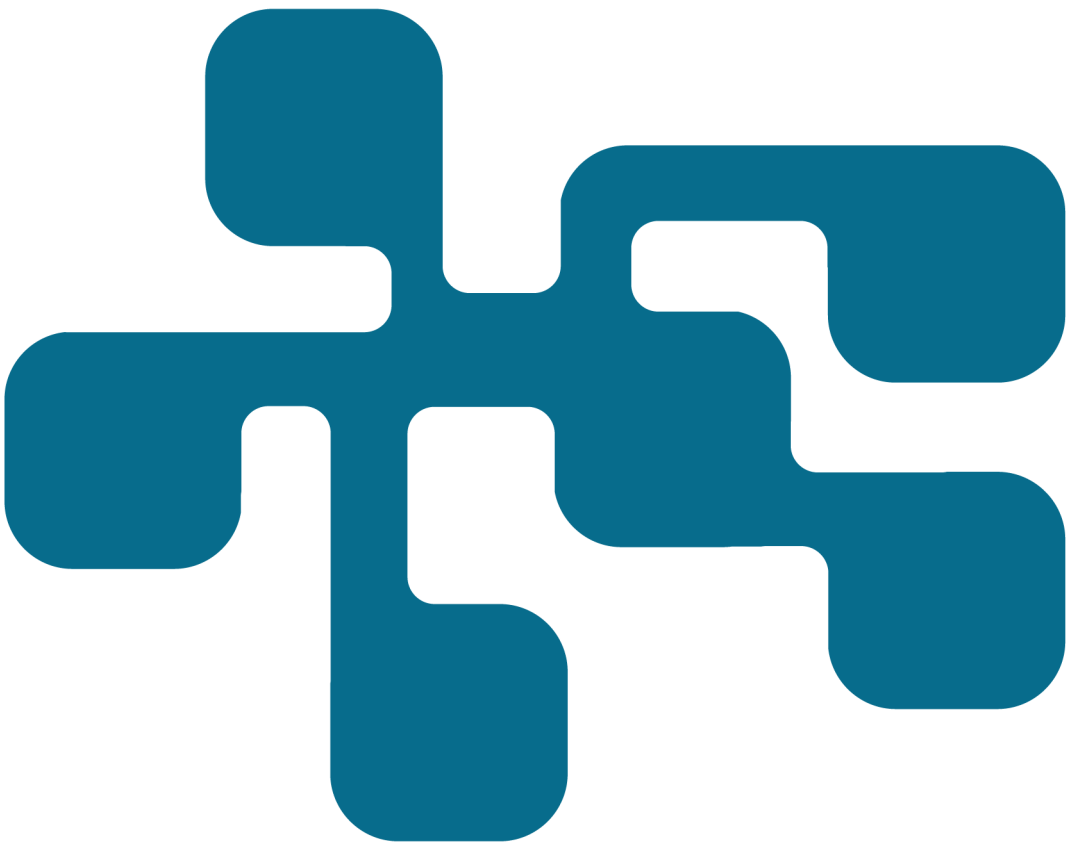
NCS3 - Molntjänster inom industriella informations- och styrsystem

En översikt av säkerhetsaspekter

AMUND GUDMUNDSON HUNSTAD
MARTIN KARRESAND

FOI
MSB



FOI-R--4597--SE
MSB 2017-1620
ISSN 1650-1942

Juni 2018

Amund Gudmundson Hunstad
Martin Karresand

Molntjänster inom industriella informations- och styrsystem

En översikt av säkerhetsaspekter

Titel	Molntjänster inom industriella informations- och styrsystem
Title	Cloud services for ICS
Rapportnr/Report no	FOI-R--4597--SE
Månad/Month	Juni
Utgivningsår/Year	2018
Antal sidor/Pages	37
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ej FoT
Projektnr/Project no	E72184
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Molntjänster framträder i ökande grad som smidiga och attraktiva för industriella informations- och styrsystem. Säkerhetsmässiga avvägningar är dock nödvändiga rörande vilka delar av system som det kan vara tänkbart att utlokalisera.

Denna rapport redovisar en kategoriindelning av molntjänster, deras tillhandahållna servicenivåer och relaterade säkerhetsutmaningar. Med detta som utgångspunkt formuleras en uppsättning säkerhetsrelaterade råd för systemägare och operatörer av industriella informations- och styrsystem.

Studien drar som slutsats att det är av vikt att säkerställa egen kompetens inom IT-säkerhetsområdet och incidenthanteringsresurser även vid en övergång till molntjänster.

Nyckelord: Industriella informations- och styrsystem, molntjänster, säkerhetsaspekter

Summary

Cloud services are emerging as convenient and attractive for the industrial control system community. There are however a need for security related considerations regarding what parts of a system that can be transferred to the cloud.

This report presents a categorization of cloud services, their service levels and related security challenges. With that in mind, a number of security related advices aimed at system owners and operators of industrial control systems are formulated.

The conclusions of the study stress the importance of having access to IT security competence in-house, as well as resources to cope with IT security related incidents when transferring parts of industrial control systems to the cloud.

Keywords: Industrial control systems, cloud services, security aspects

Innehållsförteckning

1 Inledning

Allt fler leverantörer av industriella informations- och styrsystem erbjuder även molntjänster med olika innehåll och servicenivå. Ett vanligt sätt att använda molntjänster är att lägga de administrativa delarna med statistik, rapportgenerering och historian[1] i molnet. Det finns även mer långtgående lösningar där i stort sett allt utom den processintegrerade hårdvaran läggs i molnet.

Den snabba utvecklingen och stora variationen mellan olika molntjänster gör att det kan vara svårt för systemägarna att få en överblick över de specifika utmaningar som användning av molntjänster inom industriella informations- och styrsystem medför. Övergången till molntjänster har precis börjat och det finns därför inte någon erfarenhetsbank att utnyttja hos nytillkommande systemägare eller tjänsteleverantörer. Därför har MSB initierat en kunskapsuppbyggande studie som ska kartlägga säkerhetsaspekter vid användning av molntjänster för industriella informations- och styrsystem, vilken denna rapport utgör en del av. Studien utförs inom Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3).

1.1 Syfte, mål och avgränsningar

Syftet med studien är att stärka systemägarnas kunskapsnivå om säkerhetsaspekter relaterade till molnlösningar för industriella informations- och styrsystem genom att presentera en översikt av de typer av molntjänster som erbjuds inom området för tillfället och inom en nära framtid. Vidare ska studien översiktligt beskriva de säkerhetsaspekter som är relevanta för dylika system, kunskap som sedan kan användas vid till exempel upphandling av molntjänster för industriella informations- och styrsystem. Av särskilt intresse är system inom vatten- och avloppssektorn (VA), vilket delvis färgat urvalet av respondenter, men rapporten är utformad för att vara generellt applicerbar. Rapporten är också tänkt att kunna ligga till grund för framtida fördjupande studier inom till exempel kravställning, möjligheter och risker inom området.

Rapporten som utgör resultatet av studien beskriver ett urval av typiska molntjänster, men utgör inte en fullständig genomlysning av området. I stället är den tänkt att visa läsaren på några olika tjänster som erbjuds.

[1] Generellt använd term för det system som lagrar historisk driftdata under längre tid.

1.2 Målgrupp

Rapporten riktar sig till beslutsfattare, ingenjörer och andra befattningar med behov av kunskap kring säkerhetsaspekter vid användning av molntjänster inom verksamhet kring industriella informations- och styrsystem.

1.3 Läsanvisningar

Kapitel 2 presenterar de metodiker som använts för att inhämta den information som ligger till grund för rapporten. I kapitel 3 förklaras molntjänstkonceptet. Kapitel 4 beskriver säkerhetsaspekter kring användning av molntjänster. I kapitel 5 diskuteras resultaten och de slutsatser som har dragits baserat på det insamlade underlaget. I det avslutande kapitel 6 ges råd kring hur molntjänster för industriella informations- och styrsystem kan kravställas för att bli säkrare.

2 Metodik

I det här kapitlet 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 aktörer inom området.

2.1 Litteratur

Översiktliga sökningar har gjorts i databasen Scopus för de vetenskapliga artiklar inom området *molntjänster för industriella informations- och styrsystem* som presenteras i rapporten. För den leverantörsspecifika informationen har istället sökmotorn Google 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.

2.2 Intervjuer

För att intervjuer skall resultera i relevant datainsamling och på bästa möjligt sätt bidra till studiens slutresultat, är det av vikt att använda en tydlig och enkel intervjumetodik. Huvuddragen av den av Eidenskog [DE15] redovisade metodiken används i denna studie. Inom NCS3 genomförs parallellt en studie om virtualisering av industriella informations- och styrsystem. I båda fallen är fokus på IT-säkerhet i komplexa system- och organisationssammanhang. Likartade förutsättningar, mål och syften innebar att det var synnerligen lämpligt att använda samma metodik för studierna, vilket också har gjorts.

Metodiken som Eidenskog [DE15] presenterar baserar sig på semistrukturerade intervjuer där en intervjuguide används som utgångspunkt för intervjugenomförandet. Metodiken tar sin planeringsmässiga utgångspunkt i tre av Kvale [SK97] påpekade viktiga frågeställningar inför en intervjustudie. När intervjuguiden (se Bilaga A) formulerades för de fem intervjuer som har genomförts inom projektet användes följande grundläggande frågeställning:

- *Vad*: Vilka förkunskaper krävs inför intervjuerna, avseende allmän forskarkompetens, domänkunskap avseende studiens fokus och intervjuteknik.
- *Varför*: Vikten av att formulera ett tydligt syfte med intervjustudien.
- *Hur*: Genomförande av intervjuerna respektive bearbetning och analys av intervjumaterialet.

Intervjuerna förväntades bidra, relativt litteraturen, med mera operativa kunskaper och erfarenheter av molntjänster i industriella informations- och styrsystem. Dessa kunskaper och erfarenheter torde vara värdefulla för syftet att

ta fram en marknadsöversikt och beskrivning av säkerhetsaspekter avseende sådana molntjänster. Dock kom intervjuerna i sin slutliga utformning bara att omfatta en leverantör, vilket gjorde att tyngdpunkten på marknadsöversikten hamnade i litteraturstudien istället.

I valet mellan individuella intervjuer och gruppintervjuer valdes individuella intervjuer för att minska risken att någon enskild respondent styrde svaren och att grupptänkande uppstod. Om vi märkte att någon av respondenterna var stel och nervös lät vi den inledande delen av intervjun vara helt öppen.

Ansvaret för intervjuerna delades upp så att en person huvudsakligen ställde frågor och en annan person förde anteckningar. För att underlätta arbete med renskrivning av intervjun gjordes inspelning av intervjuer, om inte respondenten motsatte sig detta. Anteckningar var dock den primära dokumentationen och inspelningarna fungerade endast som referens om anteckningarna i efterhand visade sig oklara. Istället eftersträvades att kunna identifiera påståenden, utsagor och observationer av vikt för studiens fokus och forskningsfrågor direkt vid intervjutillfället, vilket var den antecknandes ansvar. Denne ansvarade även för att ställa eventuella följdfrågor om någonting var oklart.

3 Molntjänster för industriella informations- och styrsystem

Begreppet *molntjänst* är en generell term som används inom ett flertal områden och inte bara inom industriella informations- och styrsystem. Kapitlet börjar därför med en definition och förklaring av molntjänstbegreppet.

3.1 Vad är molnet?

Molnet är ett samlingsbegrepp för en stor mängd olika tjänster och lösningar inom IT-området som nu också påverkar industriella informations- och styrsystem. Denna studie fokuserar på de molntjänster som erbjuds av en extern leverantör och där tjänsterna tillhandahålls med hjälp av servrar placerade utanför systemägarens lokaler. Där erbjuds behovsstyrd beräknings- och lagringskapacitet och kunden betalar bara för den kapacitet som faktiskt används, ungefär som för el och vatten. Molnkonceptet bygger på att det ska vara enkelt för kunden att själva öka eller minska den kapacitet som används utan att behöva interagera med personalen hos tjänsteleverantören och skalbarhet och virtualisering är två nyckelbegrepp som används[HK12, NIST11, MSA17].

En molntjänst har några specifika egenskaper som karaktäriserar dem enligt NIST[2] [NIST11]:

1. *Självbetjäning för att anpassa kapacitet:* Kunden kontrollerar själv hur mycket resurser som används och när. Detta görs utan krav på att personal hos leverantören behöver hjälpa till.
2. *Åtkomst via nätverk:* Tjänsterna är tillgängliga via internet och anpassade för generell användning av olika klienter via webbläsaren, till exempel smarta telefoner, surfplattor och datorer.
3. *Delade resurser:* De resurser som kunden utnyttjar delas med andra kunder hos tjänsteleverantören, men på ett sådant sätt att kunden upplever sig ha exklusiv tillgång till resurserna. Dessa kan vara spridda över världen och kunden har vanligtvis vare sig kontroll eller kunskap om var i världen de nyttjade resurserna finns. Tilldelningen är dessutom dynamisk vilket gör att de fysiska resurserna som används kan växla utan att kunden märker det. Exempel på resurser inkluderar lagringskapacitet, processorkraft, arbetsminne och bandbredd.
4. *Snabb kapacitetsanpassning:* I och med den dynamiska tilldelningen av resurser utifrån aktuellt behov upplever kunden att resurserna är

[2] National Institute of Standard and Technology, U.S. Department of Commerce

oändliga, även om de inte är det i praktiken. Skulle det samlade behovet från kunderna vid någon tidpunkt överstiga den totala kapaciteten hos leverantören begränsas resurserna för alla eller delar av kunderna enligt regler som leverantören sätter upp.

5. *Betala för utnyttjad kapacitet:* Molntjänster inkluderar funktioner som kontinuerligt mäter resursutnyttjande och vilket gör det möjligt för leverantören att ta betalt för den utnyttjade kapaciteten. Det ger också i de flesta fall köparen en möjlighet att se nyttjandegrad och öka eller minska resurstilldelningen för att anpassa kostnaden för tjänsten.

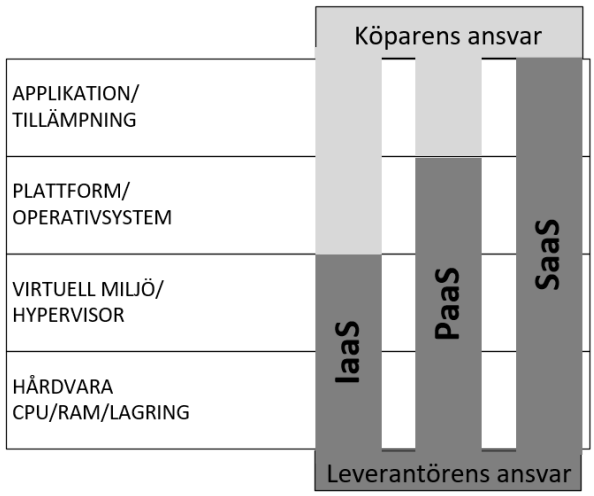
Ovanstående egenskaper beskrevs av NIST 2011 och beskriver endast delvis de molntjänster som är aktuella för industriella informations- och styrsystem 2018. Detta resonemang utvecklas vidare under diskussionskapitlet.

3.2 Typer av molntjänster

NIST beskrev 2011 tre olika typer av molntjänster där indelningen baseras på leveransmodellen för den levererade tjänsten [NIST11]. De tre huvudtyperna är:

- *Infrastructure as a Service (IaaS):* Den minst programvaruutrustade nivån av molntjänster. Leverantören står för den fysiska hårdvaran och en virtuell miljö men tillhandahåller inte operativsystem. Även sådant som brandväggar och annan säkerhetsfunktionalitet som skyddar de virtuella maskinerna ingår. Kunden installerar och ansvarar själv för det operativsystem den vill ha och eventuella användarprogram [NIST11, MSA17].
- *Platform as a Service (PaaS):* Mellannivån av molntjänster. Leverantören står för allt upp till och med operativsystem och där tillhörande säkerhetsfunktioner. Användaren installerar och ansvarar för de användarprogram den vill ha. [NIST11, MSA17].
- *Software as a Service (SaaS)* är den mest omfattande nivån av molntjänster. Leverantören står för ett färdigt paket där all användarprogramvara ingår. Kunden kan i princip börja använda systemet direkt i sin dagliga verksamhet [NIST11, MSA17].

Figur 1 beskriver leverantörens respektive köparens ansvar i förhållande till IT-tekniken på en övergripande nivå. Om vi liknar molntjänster med att hyra olika typer av lokaler så skulle IaaS motsvara att hyra en tom lokal, PaaS med att hyra en lägenhet inklusive värmesystem och vitvaror och SaaS att hyra en fullt möblerad lägenhet eller ett hotellrum.



Figur 1: Beskrivning av leverantörens och köparens ansvar för respektive typ av molntjänst.

Ovanstående kategorisering av molntjänsttyper ska ses som fingervisningar om vad leverantören har för avsikt med den levererade tjänsten, än en bokstavlig utfästelse av vad som ingår. Det är också värt att notera att det sedan NIST:s beskrivningar av begreppen 2011 har det tillkommit flera olika typer av molntjänster.

Några av de nivåer som förekommer är Data as a Service (DaaS) [QFH11], där kunden köper ett färdigt databasmoln och bara matar in sina egna data, och Mobile Backend as a Service (MBaaS, BaaS) [MBAAS17], som är inriktad på utveckling av programvara för smarta telefoner. Det finns också exempel där aktörer inom industriella informations- och styrsystem tillhandahåller egna molntjänster som SCADA-as-a-Service [SIEMENS18].

En annan utveckling som har skett är att SaaS-leverantörer i sin tur emellanåt kan placera sina mjukvaror hos IaaS-leverantörer.

3.3 Leveransformer för molntjänster

NIST har delat in molntjänster i tre övergripande leveransformer utifrån vem som kan använda dem. Till viss del ligger även placeringen av hårdvaran som molntjänsterna körs på till grund för gruppindelningen [NIST11]. De tre grupperna är:

- Ett *publikt* moln, vilket innebär att hårdvara och övriga delar av systemet kontrolleras av leverantören och nås via internet, även om upp-kopplingen kan skyddas av olika säkerhetslösningar. Ett publikt moln är

tillgängligt för alla som har köpt en tjänst av leverantören [NIST11, MSA17].

- Ett *privat* moln är ett molntjänstsystem där en kund har exklusiv tillgång till systemet. Många gånger är det fysiskt placerat i kundens lokaler, men det är inte nödvändigt. Likaså kan fortfarande leverantören sköta om driften av systemet och hårdvaran [NIST11, MSA17].
- Ett *hybridmoln* är en blandning av ett privat och publikt moln, där de två typerna utgör separata enheter, men är sammanbundna nätverks- och funktionsmässigt för att till exempel erbjuda lastbalansering vid enstaka toppar i utnyttjandegraden [NIST11, MSA17].

Det finns även indelningar i fler grupper utifrån användning. NIST tar också upp något de kallar gruppmoln (eng. community cloud) i sin uppräkning. Gruppmoln är som ett privat moln för en grupp eller sammanslutning av användare, det vill säga det är fler än ett företag eller organisation som har tillgång till molnet, men det har fortfarande en begränsning i tillgången och är alltså inte öppet för alla [NIST11].

Ovan nämna arkitekturer för molntjänster påverkar i hög grad vilka risker som molntjänsten medför. Om det till exempel är ett privat moln så kan ägaren av molntjänsten och de industriella informations- och styrsystemen vara samma organisation och då riskerar inte data att hamna utanför organisationen. Och i så fall behöver molntjänsten i sig inte heller medföra någon högre exponering mot internet som är fallet med ett publikt moln. Om inget annat nämns kommer rapporten fortsättningsvis anta att det rör sig om ett publikt moln.

För industriella informations- och styrsystem är det också viktigt vilken typ av funktion som molntjänsten används för. Ett exempel på en molntjänst är att all styr- och kontrollfunktionalitet finns kvar lokalt hos systemägaren och att molnet enbart används för lagring av data (exempelvis loggar och historik). Det innebär dock att systemägaren inte längre har kontroll över lagrad data, utan att det är molntjänstleverantören som har det. Data kan då läcka över till andra kunder i samma moln och om det sker ett intrång i molntjänsten, kan angriparen få tillgång till ett stort antal användarkonton och -data på samma gång [WTM13].

Det är möjligt att molntjänstleverantören har tillgång till alla data som lagras om inte särskilda säkerhetsåtgärder vidtas som förhindrar detta. Och även om det juridiskt går att skriva avtal som säkerställer tillgång till data så är detta inte detsamma som att tekniskt garantera systemägarens tillgång till sina data. Med andra ord är det viktigt att göra en korrekt riskanalys med avseende på data-tillgång och datasekretess innan denna molntjänst utnyttjas.

Ett annat exempel på användning av molntjänster för industriella informations- och styrsystem innebär att även styr- och kontrollfunktionalitet har flyttats ut i molnet. Ett exempel på detta är Microsoft IoT Central [MIC18], där en operatör

via molnet kan kommunicera direkt med utrustningen och ändra parametrar för att åtgärda problem som sensorerna varnar för. Kvar hos systemägaren finns bara själva processkontrollutrustningen. Innan en sådan molntjänst används är det viktigt att analysera hur detta påverkar tillgängligheten till styr- och kontroll-funktionerna då tjänsten är beroende av att den externa kommunikationen fungerar. Det kan också vara ett problem att trafiken till och från utrustningen passerar internet på sin väg till molntjänstleverantören, vilket medför en större attackyta och fler säkerhetsutmaningar. Trafiken kan bland annat bli avlyssnad, modifierad eller förhindrad [WTM13].

4 Säkerhet

En förflyttning av styr- och kontrollfunktioner för industriella informations- och styrsystem till molnet medför att säkerheten kan öka inom vissa områden, men det förutsätter att kunden ställer rätt krav på leverantören. Exempel på områden som behöver kravställas är hur den levererade tjänsten ska uppdateras, skyddas mot intrång och tillgängligheten garanteras via avtal[3]. Varje fall är dock unikt och kräver en grundlig analys innan beslut fattas i frågan.

4.1 Utmaningar

Det finns dock ett antal områden där skyddet och säkerheten påverkas negativt och där en noggrann analys av vilka negativa säkerhets- och tillförlitlighets-effekter en flytt till en molntjänst skulle ha. Utmaningarna täcker hela spannet från strategi och avtal till tekniska detaljer som kommunikationsutrustning och konfigurering av lagring i molnet. I kapitel 6 ges råd om hur dessa utmaningar kan hanteras.

4.1.1 Styrning utlokaliserad till extern part och via internet

Att fullt ut utlokalisera styrningen av ett system är riskfyllt och kostnaderna för och konsekvenserna av ett eventuellt fel eller intrång kan vara mycket stora. Vid utlokalisering av styrande funktioner till en extern part ges utomstående full kontroll över processen och kommer att hantera detta i enlighet med de till-gänglighetsavtal och de driftinstruktioner som upprättas. Det är endast för små processenheter utan strategisk betydelse där det inte är möjligt att upprätthålla nödvändig kompetens och resurser för fortsatt drift som det kan vara tänkbara att utlokalisera även styrning till en molntjänst [INT1, INT2, INT4].

4.1.2 Lagring av data hos extern part

Lagring av data hos extern part medför att informationsägaren inte längre har kontroll över vem som har tillgång till data. Även om molntjänstleverantören använder alla till buds stående medel för att separera olika kunders data från varandra lagras och hanteras de i ett gemensamt system. Avgränsningarna mellan datamängderna är bara logiska, det vill säga det kan räcka med en bugg i den underliggande virtualiseringsprogramvaran eller ett administrativt fel för att information ska kunna läcka. Det är också möjligt att personal hos molntjänst-leverantören kan läsa kundernas data i och med att de är systemadministratörer

[3] Ett tillgänglighetsavtal motsvarar vad som på engelska benämns Service Level Agreement (SLA).

på underliggande system. En presumtiv kund bör fråga sig om det är acceptabelt att de data som lagras i molnet riskerar att bli publika [WTM13]?

En annan utmaning med att lagra data hos extern part är risken för att tillgängligheten till data tillfälligt eller varaktigt går förlorad. Även om detta kan hanteras i avtal med leverantören så måste det i så fall vara möjligt att vidmakthålla processen under den tid som data är otillgängliga.

4.1.3 Angrepp på webbgränssnitt

Många molntjänster använder någon form av webbgränssnitt för leverans eller konfiguration och angrepp på webbgränssnitt är fortfarande den vanligaste typen av angrepp mot molntjänster [AB18, MIC16]. Även om molntjänstleverantörerna ser till att deras webbgränssnitt är så säkra som möjligt motverkas åtgärderna till viss del av att leverantörerna utgör lockande mål i och med sin storlek. Dessutom omfattas även kundens egna webbgränssnitt av det utökade hotet eftersom IP-adresser och DNS-uppslagningar pekar mot tjänsteleverantörens nät. En presumtiv kund bör fråga sig om det är acceptabelt att möjligen dra till sig extra uppmärksamhet genom att använda en välkänd tjänst och vad som kan göras för att minska exponeringen [WTM13]?

4.1.4 Förlorad kontroll över systemens omgivning

Vid användning av en molntjänst kommer kontrollen över omgivningen till de utlokaliserade industriella informations- och styrsystemen att försämras. Molntjänstleverantören kan till exempel ta in nya kunder som medför en förändrad hotbild mot de utlokaliserade systemen. Ett annat exempel är att molntjänstleverantören kan skapa anslutningar mellan sina system och system i utlandet eller helt enkelt flytta servrarna som huserar tjänsterna till andra länder. Andra exempel är att molntjänstleverantören kan bli föremål för myndighetsagerande baserat på andra kunder som utnyttjar samma plattform. Sammantaget kan detta dels öppna nya vägar in för angripare eller leda till att systemen blir otillgängliga vilket därmed äventyrar säkerheten i det utlokaliserade informations- och styrsystemet.

En presumtiv kund bör fråga sig om det är acceptabelt att inte ha kontroll över vilka kopplingar eller övriga omgivningar och omständigheter som kan påverka det egna systemet [WTM13]?

4.1.5 Skyddad kommunikation

Många kommunikationsprotokoll som används inom industriella informations- och styrsystem saknar säkerhetsmekanismer såsom autentisering och kryptering. Detta är inte heller något som molntjänstleverantören ansvarar för utan är något

som kunden måste säkerställa [DEBL17]. Det är därför viktigt att kunden säkerställer säker kommunikation mellan molntjänstleverantören och de egna systemen innan ett system utlokaliseras.

Ett annat problem avseende kommunikation som behöver hanteras innan utlokalisering av industriella informations- och styrsystem genomförs är att säkerställa relevanta tillgänglighetsavtal för kommunikationen. Detta eftersom tillgången i sig är helt eller delvis beroende av tillgången på kommunikation. Egenskaper som behöver vägas in är bandbredd, svarstider och serviceavtal. Det är också viktigt att det finns kontinuitetsplanering för verksamheten som hanterar kommunikationsbortfall under den tid som föreskrivs i serviceavtal med kommunikationsleverantören [INT5].

4.1.6 Säkerställa korrekt loggning

Loggning är en viktig funktion för att kunna utreda incidenter och spåra orsaken till problem och system som utlokaliseras till molntjänster kommer helt eller delvis att logga händelser i system utanför kundens kontroll. Det kommer också att bli ett komplext system som inbegriper åtminstone tre aktörer, molntjänstleverantören, kommunikationsleverantören och systemägaren. Detta medför att det är svårt att säkerställa att alla relevanta loggar som behövs för felsökning och incidenthantering är nåbara [INT5, WTM13].

En presumtiv kund bör fråga sig om det är acceptabelt att möjligen förlora tillgången till systemloggar och om det skulle innebära en säkerhetsrisk.

4.1.7 Molntjänstleverantörens stabilitet

Molntjänstleverantörens (och eventuella underleverantörers) stabilitet som företag, både finansiellt och juridiskt kan hastigt påverka tillgången till både tjänsten och de data som lagras i molnet. I och med att nyttjande av molntjänster kan innebära en ny affärsmodell för kunden finns det även risk att de avtal som skrivs inte motsvarar kundens behov fullt ut [HK12].

En presumtiv kund måste tillse att verksamhetens kontinuitetsplan kan hantera de avbrott som kan uppstå. Detta måste även inkludera tiden som en eventuell juridisk konflikt kan pågå och inte enbart begränsas till ett traditionellt tillgänglighetsavtal [INT5].

4.1.8 Kontroll av avtalsefterlevnad

Det är svårt att kontrollera molntjänstleverantörens avtalsefterlevnad i och med att kunden inte har tillgång till det underliggande molnsystemet. Det är även nödvändigt att vara uppmärksam på vilka delar av verksamheten som omfattas av olika avtal och har olika leverantörer. Det finns annars en risk att ansvaret för en

kritisk funktion visar sig falla mellan stolarna i ett skarp läge. Det kan till exempel handla om att kund och leverantör använder olika internetleverantörer, vilka sedan hänvisar till varandra vid fel på anslutningen [INT1].

4.1.9 Avveckling och byte av molntjänstleverantör

Avveckling och byte av molntjänstleverantör kan innebära en del problem och utmaningar. För det första går det inte att tillförlitligt radera data från molnservrarna eftersom det inte kan göras fysiskt i och med att flera kunder delar på samma hårdvara (lagringsmedia). Vid byte av molntjänstleverantör kan det även uppstå problem med att flytta data på grund av att leverantörerna använder olika molnsystem som i sin tur använder olika dataformat. Det finns en formatstandard som heter Open Virtual Format (OVF) och som underlättar flytt mellan olika virtualiseringsmiljöer och som skulle kunna användas även vid byte av molntjänster. [HK12]. Men industriella informations- och styrsystem är så komplexa att flytta att det troligen är bättre att genomföra en nyinstallation hos den nya molntjänstleverantören än att flytta befintliga system [INT5].

4.1.10 Oförutsedda kaskadeffekter

Att dela infrastruktur med okända aktörer ökar risken för oförutsedda kaskadeffekter från både andra kunders system och från olika typer av cyberincidenter. Det kan till exempel röra sig om att en molntjänstleverantörs plattform utsätts för en DoS-attack på grund av en annan kund eller att ett fel i en annans kund system också påverkar virtualiseringsmiljön.

Det har under senare år förekommit flera fall där molntjänstleverantörer har utsatts för IT-angrepp med allvarliga konsekvenser för stora kundgrupper som följd. Ett exempel är angreppet mot Dropbox 2012 där cirka 60 miljoner inloggningsuppgifter stals. 2014 publicerade sedan en anonym källa flera miljoner lösenord och inloggningsnamn och krävde betalt för att inte publicera fler. Företaget genomförde därför en återställning av lösenorden för de påverkade användarna [AG16]. Ett annat exempel är den bugg i Cloudflares programvara för hantering och spridning av webbplatser som under tiden oktober 2016 till februari 2017 orsakade att potentiellt känslig data läckte och i sällsynta fall lades till i slutet på visade webbsidor [IT17, CERT-SE17]. CloudHopper var ett världsomfattande IT-angrepp mot företag som hade utlokaliserat sin IT-drift till externa bolag och där hela eller delar av IT-systemen flyttats till molnet. Molntjänstsystemen användes för att hoppa vidare in i de enskilda företagens lokala nätverk och system, vilket möjliggjordes av kommunikationsvägarna mellan molnet och de lokala nätverken. Angreppet upptäcktes i slutet på 2016, men misstänks ha pågått sedan åtminstone början på 2014 [MSB17, PWC17].

Det förs också resonemang om huruvida placering av många industriella informations- och styrsystem hos samma molntjänstleverantör kan ge upphov till

att det specifika molnet eller tjänsteleverantörens värde för en angripare ökar. Det skulle i så fall innebära att en incident skulle få större konsekvenser för samhället än om antalet kunder varit mindre [INT1, INT2].

En kontinuitetsplan som verifierats genom tester bör användas för att kartlägga och hantera verksamhetens beroende av molntjänsten och -leverantören. Tänk även på att störningar i andra kringliggande system kan ge effekter även på processverksamheten och molntjänsten [INT1].

4.1.11 Systemkomplexitet

Att placera system hos en molntjänstleverantör kan i vissa fall öka komplexiteten vid felsökning och kan också ge upphov till kaskadfel. Ofta är industriella informations- och styrsystem beroende av egna kommunikationsprotokoll som inte är så robusta som de kommunikationsprotokoll som används över internet. Det är därför viktigt att kunden säkerställer att molntjänstleverantören kan hantera de förutsättningar som de industriella informations- och styrsystemen kräver innan utlokalisering sker [INT5].

4.1.12 Licenshantering

En utmaning som specifikt behöver beaktas vid utlokalisering av industriella informations- och styrsystem är hanteringen av licenser då det inte är ovanligt med hårdvaruberoende licenser inom dessa system. Då kan det till exempel bli stora problem om molntjänstleverantören startar om sina fysiska servrar [INT5]. Säkerställ därför att licenshanteringen stödjer de tekniker som molntjänst-leverantören använder och verifiera att efterfrågad tillgänglighet kan tillhanda-hållas.

4.1.13 Larmhantering och incidenthantering

När styrning och övervakning av en process läggs ut på en molntjänst är det viktigt att först tänka igenom hur larmhanteringen skall hanteras vid uppkomna incidenter. Molnleverantörer har inte samma kännedom om processen som personal på plats och kommer endast att följa de rutiner som finns beskrivna Var därför noga med att upprätta fungerande rutiner samt testa att dessa fungerar genom varje steg i kedjan. Rutinerna för larmhantering och incidenthantering behöver också inkludera samtliga intressenter i kedjan, till exempel kommunikationsleverantörer [INT5].

4.2 Nuläget

Det finns ett flertal leverantörer av molntjänster för industriella informations- och styrsystem och antalet kan förväntas öka när molntjänstkonceptet blir mer etablerat i branschen. I många fall är den slutgiltiga molntjänstleverantören i sin tur kund hos någon annan molntjänstleverantör i och med den indelning utifrån servicenivå som används för att klassificera molntjänster. En leverantör av molntjänster på SaaS-nivå köper ofta i sin tur en PaaS eller till och med IaaS-tjänst av någon annan leverantör [INT5]. Många av de tjänster som erbjuds på lägre nivåer är inriktade mot sakernas internet (eng. Internet of Things, IoT), men kan anpassas för att användas med industriella informations- och styrsystem.

4.2.1 Produktexempel

Följande exempel på Iaas, PaaS och SaaS är i vissa fall inte officiellt kategoriserade av leverantörerna och vi har därför själva kategorisera dem utifrån tillgängliga beskrivningar av tjänsterna. Kategoriseringarna kan därför i vissa fall skilja sig från leverantörernas.

På IaaS-nivå levererar till exempel Amazon Web Services (AWS) IoT Core [AWS18] och Microsoft Azure [MA18] molntjänster. Dessa är inte specifikt framtagna för industriella informations- och styrsystem, men kan mycket väl komma i fråga om det är ett befintligt system som ska flyttas till molnet. AWS erbjuder ett egenproducerat realtidsoperativsystem, Amazon FreeRTOS [AFR18], som körs på gränsenheter (edge devices) och underlättar användning av andra molntjänster som Amazon tillhandahåller. Azure är en molntjänst där system baserade på Microsofts operativsystem och applikationer kan placeras.

På PaaS-nivå återfinns till exempel Microsoft Azure IoT Hub [MAH18], Google Cloud IoT [GCI18], General Electric Predix [GEP18] och Siemens MindSpere [SMS18]. Dessa erbjuder plattformar där kunden kan köra sina egna specifika industriella informations- och styrsystem, det vill säga kunden står för styrlogik med mera. De presenterade PaaS-tjänsterna hanterar främst uppkoppling av enheter, datalagring, och analys.

Vad gäller SaaS har till exempel Rockwell ett systemkoncept som heter FactoryTalk [RFT18]. Det är byggt för att utföra alla delar från kommunikation, datainsamling till analys och presentation. Till hjälp vid dataanalysen använder systemet artificiell intelligens. Även Microsoft erbjuder en SaaS-lösning genom Microsoft IoT Central [MIC18]. Där kan en operatör direkt manipulera styr-parametrar i enskild processutrustning via molntjänsten, vilket placerar systemet i den högre nivån av användning av molntjänster för industriella informations- och styrsystem.

4.2.2 Exempel på säkerhetslösningar i produkt

För att exemplifiera de olika säkerhetsåtgärder som en molntjänst för industriella informations- och styrsystem kan innehålla har vi använt produkter från Siemens. Valet är enbart baserat på det faktum att en av intervjuerna [INT3] gjordes med tekniker från Siemens, vilket medförde tillgång till mer detaljerad information om molntjänstens uppbyggnad än vad annars var fallet. Valet innebär inte någon värdering eller gradering av Siemens produkter relativt andra tillverkare inom branschen.

Siemens tillverkar vad som förenklat kan kallas en säkerhetsbrygga (MindConnect Nano) mellan den processnära hårdvaran och deras molnbaserade styrsystemstjänst (MindSphere). Säkerhetsbryggan skyddar de delar av kommunikationen mellan de servertjänsterna som är placerade i MindSphere och de processnära delarna som går över Internet och kan liknas med en VPN-tjänst. För att bibehålla den säkerhetsnivå som säkerhetsbryggan erbjuder får inte de processnära delarna exponeras separat mot internet. Det krävs därför en brygga per lokal grupp av processkomponenter och all internettrafik måste passera bryggan. Bryggans säkerhetsfunktion [SSW16] bygger enligt Siemens bland annat på

- användning av certifikat för att ge en autentiserad koppling till molntjänsten
- att alla uppkopplingar initieras av bryggan
- användning av HTTPS-protokollet (med TLS v. 1.2) för krypterad kommunikation
- fysiskt separata nätverkskort för koppling till internet respektive det lokala processnätet

Siemens molntjänst är en PaaS som kör styr- och analysprogramvara för industriella informations- och styrsystem. Den använder sig av logisk separering med hjälp av sandlådor för att skilja olika kunders installationer åt. Detta gäller på programvaru- och nätverksnivå [SSW16]. En sandlåda är en logiskt isolerad miljö som saknar kopplingar till andra miljöer som existerar i molnet. Eftersom separationen är enbart logisk kan eventuella fel i det underliggande systemet göra att sandlådornas innehåll sammanblandas eller läcker mellan olika instanser [GF16, JH16].

Standardsättet för inloggning till molntjänsten är med användarnamn och lösenord, men det går att använda tvåfaktorautentisering om högre säkerhet krävs [SSW16]. Delar av de data som lagras är krypterade, men krypteringen sker i molnet, vilket gör att de som har tillgång till Siemens krypteringsnycklar också kan läsa dessa data. Siemens har inrättat en nyckelhanteringsrutin för MindSphere och upprätthåller en förteckning över alla nycklar som används i systemet.

Maskin- och processdata lagras i klartext och skyddas med rättighetshanterings-mekanismer [SSW16]. Kunden är själv ansvarig för att göra backup av de egna data som lagras i systemet. Siemens ansvarar för att göra backup av systemet som sådant, se till att säkerhetsuppdateringar görs, att det finns adekvat logiskt och fysiskt skydd av systemet och att byta ut trasig hårdvara.

Det finns även lösningar som erbjuder enbart säkerhetsbryggor för att ge kunden möjlighet att själv välja molntjänstleverantör, eller behålla egna system som med hjälp av bryggan kan kopplas samman över internet [INT2, INT3, INT4]. Stundtals benämns även användning av enbart en säkerhetsbrygga som en moln-lösning, vilket det i strikt mening inte är enligt den definition som används i denna rapport. En dylik lösning med enbart brygga kan användas för öka skyddet för kommunikationen mellan olika fysiskt åtskilda installationer. Den utgör då ett VPN mellan installationerna, inte en molntjänst.

4.3 Framtiden

Det finns en stor mängd vetenskapliga artiklar som beskriver problematiken med användning av molntjänster för industriella informations- och styrsystem. De beskriver dock sällan hur problemen kan lösas i detalj. De lösningar som föreslås i litteraturen och intervjuerna presenteras i kapitel 6.

Endast ett fåtal artiklar presenterar nya lösningar för att förbättra säkerheten i ICS-moln. En av dessa tar upp bristen på autentiseringsmekanismer i ICS och presenterar en lösning i form av ett Multilevel User Access Control Layer (MLAC) [BMSA15]. Författarnas lösning bygger på att det finns en central åtkomstkontrollfunktion i molnet som skickar ut virtuella polletter (tokens) för varje åtgärd i systemet. Dessa polletter bestämmer sedan vad respektive användare får göra för tillfället. En sådan lösning medför dock att varje funktion i systemet som kan påverkas också kan hantera dessa polletter. Ytterligare ett problem är ägarskapet av den centrala åtkomstkontrollfunktionen. Ägaren måste gå att lita på, för funktionen utgör en kritisk del av åtkomstsystemet och eventuellt missbruk (eller avbrott) kan få stora konsekvenser.

I artikeln har problemet med kravet på pollethantering i flera funktioner lösts genom att hela systemet är tänkt att köras via en webbläsare och åtkomst-kontrollen har därför flyttats från respektive enhet till en eller flera webbservrar som interagerar med det underliggande systemet. Detta löser dock inte hela problemet eftersom webbservern i sig kan angripas. Därför rekommenderar artikelförfattarna användning av privata moln, vilket i flera fall tar bort nyttan med att börja utnyttja en molntjänst.

Ett mer komplett system som är tänkt att lösa flera av säkerhetsproblemen vid användning av molntjänster för industriella informations- och styrsystem presenteras av Goose, Kirsch och Wei [GKW15]. I en artikel från 2015 beskriver

hur de har skapat ett system de kallar SKYDA. Systemet nyttjar ett flertal olika tekniker för att bygga ett molnbaserat system som utan försämrad funktionalitet kan hantera både slumpmässiga och medvetna fel. Teknikerna de använder är välkända och teoretiskt underbyggda. Beroende på vilken säkerhetsnivå som ska uppnås används olika tekniker, vilket dock ökar kostnaderna för systemet i olika grad.

Generellt sett bygger SKYDA på användning av flera molninstanser och i vissa fall till och med flera oberoende molntjänstleverantörer. Dessa kopplas samman och genom att synkronisera dem via ett virtuellt nätverk mellan de inblandade molninstanserna kan det fås att fungera som ett enhetligt system med tillräckligt korta svarstider. En instans som använder SKYDA ska då fungera trots störningar från andra molninstanser, inklusive medvetna sabotageförsök. I den mest feltoleranta konfigurationen behövs det $3f+1$ molninstanser för att kunna hantera upp till f felaktiga instanser.

I den enklaste konfigurationen av SKYDA är ICS Mastern, den del i systemet som styr och övervakar exempelvis en Remote terminal unit (RTU), dubblerad i en primär enhet och en aktiv reserv i varsitt moln (de kan dock hanteras av samma tjänsteleverantör). Konceptet liknar det som för närvarande används i traditionella industriella informations- och styrsystem. Fördelen med moln-lösningen är att det går mycket snabbt att flytta ett virtuellt system till en ny molninstans om den gamla skulle fallera.

Om flera samtidiga molninstanser av primär enhet respektive aktiv reserv körs i två olika moln erhålls ett visst skydd vid intrång, där en eller flera enheter kan vara komprometterade utan att systemet som helhet påverkas ur en till-gänglighetssynvinkel. För det övervakade industriella informations- och styrsystemets del fungerar de olika molninstanserna som ett enda sammanhållet system. För att öka säkerheten ytterligare kan olika molntjänstleverantörer användas, vilket ger redundanta internetkopplingar som skydd mot Distributed Denail of Service (DDOS)-angrepp på molntjänsten Denna lösning i SKYDA utgör ett skydd på mellannivå, men kräver mer hårdvaruresurser och innebär därmed högre kostnader, särskilt om olika molntjänstleverantörer används. Lösningen ökar komplexiteten och därmed också kraven på kompetens hos de som administrerar och underhåller det industriella informations- och styrsystemet.

Den högsta nivån av säkerhet i SKYDA innebär att minst fyra primära enheter körs i olika moln, eventuellt hos olika tjänsteleverantörer. I denna konfiguration behövs inte några aktiva reserver, utan de inblandade primära enheterna är synkroniserade och fungerar som en enda primär enhet ur det industriella informations- och styrsystemet synvinkel. SKYDA skyddar dock primärt mot tillgänglighetsproblem, någon reell ökning av sekretesskyddet ges inte. Likaså räcker det inte med redundans på SKYDA-sidan, även det eller de lokala systemen måste beaktas. Där är det främst kopplingen till internet som är

flaskhalsen och som bör vara redundant genom användning av flera oberoende internetleverantörer.

Utöver dessa exempel, finns det forskning som studerar hur säkerheten i molntjänster kan ökas på en generell nivå, utan att ta hänsyn till de särskilda behov som finns för industriella informations- och styrsystem. Denna forskning är inte direkt tillämpbar på dylika system, men kan ändå vara bra att känna till. Några exempel på sådana forskningsprojekt presenteras av Santos, Gummadi och Rodrigues [SGR09], Lombardi och Di Pietro [LDP11], Subashini och Kavitha [SK11] samt Zissis och Lekkas [ZL12]. De presenterar alla olika sätt att råda bot på problem med till exempel autentisering, skydd av data och tillit mellan noder.

5 Diskussion och slutsatser

Molntjänster för industriella informations- och styrsystem röner ökande intresse hos såväl utvecklare som systemägare. Begreppet molntjänster används om ett brett spektrum av företeelser och ibland även om lösningar som inte strikt följer definitioner av vad som utgör molntjänster. Parallella näraliggande utvecklingstrender, så som utveckling av virtualiseringsteknik och -tjänster inverkar rimligen också på intresset för molntjänster. Begreppsmässiga oklarheter kan därmed härröra från att parallella utvecklingstrender ger samtidiga avtryck i teknikdiskussionen.

Studien inom vilken denna rapport togs fram är begränsad i omfattning. Särskilt är detta fallet vad gäller omfattningen på intervjustudien. Intervjumaterialet ger inget tydligt statistiskt underlag, endast en uppsättning synpunkter från ett urval av aktörer. Urvalet av aktörer för intervjustudien gjordes i samråd mellan Totalförsvarets forskningsinstitut (FOI) och uppdragsgivaren Myndigheten för samhällsskydd och beredskap (MSB). Studien avsågs att vara generellt tillämpbar, men med särskild betoning på VA-sektorns behov och utveckling avseende molntjänster. Synpunkter som framkom från denna sektor var dock inte sektorsspecifika utan generellt tillämpbara.

Ett viktigt syfte med studien är att stärka operatörers kunskapsnivå om molnlösningar för industriella informations- och styrsystem. Studien bidrar till detta med en genomgång av vad molntjänster innebär, vilka typer av molntjänster som erbjuds och hur de övergripande leveransformerna för molntjänster ser ut. Med detta som utgångspunkt presenteras en uppsättning säkerhetsmässiga utmaningar och råd respektive en nulägesbeskrivning och vad som ur forskningsverksamhet på området kan anas inför framtiden.

Affärsmässiga besparingar och ökad tillgänglighet till information så väl som leverantörernas leveransmodeller av tillämpningar är vanliga skäl till varför molnlösningar väljs. Samtidigt behöver dessa fördelar vägas mot vilka risker införande av molnlösningar kan innebära. Denna studie formulerar en uppsättning generella råd utifrån identifierade säkerhetsrelaterade utmaningar rörande molnlösningar, beskrivna i avsnitt 4.1 och med relaterade råd i kapitel 6. Råden pekar på vikten av planering och noggrann riskanalys, av att använda bra säkerhetsmekanismer och protokoll, detaljerad loggning och slutligen att bra avtal med molntjänstleverantören förhandlas fram.

I NIST:s beskrivning av molntjänster från 2011 beskrivs fem egenskaper som karakteriserar molntjänster. Denna beskrivning har åldrats fort och är endast delvis relevant för molntjänster för industriella informations- och styrsystem. Under *Åtkomst via nätverk* beskrivs att åtkomst sker via webbläsaren men det är ofta beroende av vilken funktion som behöver kommas åt. Idag är det till exempel vanligt med viss konfiguration via SSH. Under *Delade resurser*

beskrivs hur tjänster kan vara spridda över världen men behov av korta responstider och framförallt nationell lagstiftning har medfört att det numera är normalt att erbjuda valmöjlighet för var en molntjänst lokaliseras. *Snabb kapacitetsanpassning* och att kunden *betalar för utnyttjad kapacitet* är framförallt vanligt för de mer infrastrukturnära molntjänsterna (Iaas och delvis Paas). Inom SaaS har tjänsterna utvecklats mot användning av licenser för ett visst antal användare eller för att kunna hantera ett visst antal enheter.

En egenskaper som NIST inte nämner i sin lista är de möjligheter som molntjänster tillåter för att tillhandahålla utökad tillgänglighet till centrala system. Det kan till exempel handla om användning av redundanta servrar spridda på flera platser eller att upprättande av en katastrofsite som kan tas i drift vid ett katastrofalt avbrott i den egna datorhallen.

Nuläget inom molntjänster för industriella informations- och styrsystem exemplifieras genom en beskrivning av Siemens säkerhetsbrygga. Det utgör ett aktuellt exempel på hur molntjänstleverantörer också erbjuder säkerhetsmässiga lösningar i gränsområdet mellan processnära hårdvara och molnbaserade styrsystemtjänster. Detta påvisar att leverantörerna är medvetna om de säkerhetsmässiga utmaningar som finns samtidigt som det också visar på en förmåga till återvinning av lösningar från IT-området. I detta fall finns det klara likheter mellan det Siemens kallar en säkerhetsbrygga och det som inom IT-området skulle kallas en VPN-tunnel mellan två brandväggar. Värt att notera är dock skillnaden i terminologi. Genomgången av molntjänster för industriella informations- och styrsystem visar också att det finns andra leverantörer som erbjuder liknande lösningar och fler tillkommer i stadig takt.

Den framtida utvecklingen inom molntjänster för industriella informations- och styrsystem är svår att uppskatta i och med att konceptet är nytt och utvecklingen inom industriella informations- och styrsystem går relativt långsamt jämfört med inom IT-området. Dock ger domänens forskning en indikation om möjlig framtida tekniskt utveckling. Lösningar som samtidigt omfattar flera olika teoretiskt underbyggda och välkända tekniker verkar vara den mest troliga utvecklingsvägen in i framtiden. Samtidigt går det att skönja en utveckling där tekniker som traditionellt används inom IT-området utnyttjas för molntjänster för industriella informations- och styrsystem. Detta medför att den forskning och den utveckling som sker gällande säkerhet i generella molntjänster också kan utnyttjas för att göra molntjänsterna för industriella informations- och styrsystem blir säkrare.

Sammanfattningsvis är i dagsläget molnlösningar för industriella informations- och styrsystem baserade på allmän teknikutveckling inom IT-området. Specifika sektorbehov och branschspecifik teknikutveckling styr molnteknikutvecklingen i liten grad. I studien noteras dock inte några direkta problem med detta. För aktörer inom industriella informations- och styrsystem är det ändå av vikt att identifiera sina allmänna behov och särskilt säkerhetsrelaterade behov för att på

bästa möjliga vis kunna välja bland tillgängliga molntjänster med tillhörande säkerhetsmekanismer. Vidare är det synnerligen viktigt att kritiskt granska och göra avvägningar kring vilka funktioner det kan vara försvarbart att utlokalisera till molntjänstleverantörer. Detta accentuerar även vikten av att fortfarande ha en egen kompetens inom IT-säkerhetsområdet, respektive relevanta och adekvata incidenthanteringsresurser inom organisationen.

6 Råd

För att motverka de säkerhetsproblem som molntjänster för industriella informations- och styrsystem ger upphov till ges följande råd. Observera att behoven varierar mellan olika molntjänstlösningar och att råden därför är generellt hållna. Varje situation måste analyseras för sig och lämpliga lösningar väljas baserat på de rådande förutsättningarna.

- Utför en fullständig riskanalys av den tilltänkta molnlösningen innan den tas i drift. Riskanalysen bör omfatta men inte begränsas till behov av sekretess, tillgänglighet, samt frågor om hur olika säkerhetslösningar i molnet är implementerade. Den ska också analysera hur molntjänsten påverkar exponeringen av de egna systemen och nätverken, hur trafiken flödar samt att inte andra system exponeras mot molnleverantören. Det är viktigt att analysen genomförs med hjälp av expertis inom både IT-säkerhet och industriella informations- och styrsystem och om denna inte finns inom organisationen bör extern kompetens anlitas. [INT1, INT5].
- Upprätta tillgänglighetsavtal (ofta refererade som SLA) med relevanta leverantörer för att säkerställa åtkomst till molntjänsten. Det kan också vara aktuellt att se över tillgänglighetsavtal med internetleverantören innan utlokalisering sker [INT5].
- Kontrollera molntjänstleverantörens avtalsefterlevnad via en extern part som kan ges tillgång till delar även utanför kundens kontroll. Ett annat alternativ är att välja en leverantör som är certifierad enligt någon lämplig standard.
- Ta fram en kontinuitetsplan för verksamheten, inklusive alla berörda processer och intressenter. Planen ska hantera driftstörningar för molntjänsten som täcker de avbrottstider som de tillgänglighetsavtal som tecknats med leverantören [INT1, INT4]. Se också till att det finns en hantering av driftlarm och övervakning av relevanta tjänster som inkluderar alla leverantörer [INT5].
- Utred om det finns behov av en redundant anslutning till molntjänstleverantören för att minska risken för kommunikationsavbrott [INT5].
- Innan en utlokalisering av industriella informations- och styrsystem sker bör det finnas en avvecklingsplan som beskriver hur det går till att lämna tjänsten [INT5].
- Använd säkra kommunikationslösningar för att skydda kommunikationen över öppna nätverk såsom internet genom kryptering. Protokollet IPSec erbjuder både lösningar för autentisering och kryptering av trafik

och kan användas för att skapa virtuella privata nätverk (VPN) mellan geografiskt skilda nätverk. Transport Layer Security (TLS) används för att skapa krypterade sessioner mellan två noder i ett nätverk [WTM13].

- Om inte IPSec används bör protokoll med inbyggd säkerhet [WTM13, BMSA15, SAS16] användas i stället. I en FOI-rapport [DEBL17] görs en genomgång av ett flertal av de protokoll för industriella informations- och styrsystem som används i Sverige.
- Data som är i vila bör krypteras. Detta råd gäller för alla tillfällen när data lagras utanför de egna interna systemen, men är särskilt viktigt i molnsammanhang [WTM13]. Lösningen bör vara konstruerad så att krypteringen sker innan data flyttas ut från det interna nätverket [BMSA15, SAS16]. Om de data som lagras behöver bearbetas av molntjänsten på något sätt måste tjänsten ha tillgång till krypterings-nycklarna, annars fungerar inte tjänsten.
- Aktivera den loggning som erbjuds och använd gärna en centraliserad lösning där så många olika loggar som möjligt sparas. Inkludera system-, säkerhets-, nätverks-, och tillämpningsloggar om möjligt för att kunna ge en så heltäckande bild som möjligt av systemet och händelserna däri om så behövs i efterhand [WTM13, SAS16].
- Se till att dokumentera hela lösningen, inklusive felsökningsmetoder och kontaktvägar [INT5].
- Förhandla fram avtal med molntjänstleverantören som reglerar vem som får åtkomst till de utlokaliserade systemen. [WTM13, SAS16]. Avtalet bör också reglera processen för byte av leverantör, vad som händer om leverantören inte kan tillhandahålla tjänsten längre och leverantörens skyddsåtgärder för att förhindra intrång och dataläckage mellan instanser i molnet.
- Se till att det finns en lokal säkerhetskopia av de system som utlokaliseras som ni kontrollerar. Det har förekommit att data och system som har utlokaliserats har gått förlorade på grund av slarv hos leverantören [INT5].
- Använd de säkerhetslösningar som finns tillgängliga för den valda lösningen. Det kan till exempel handla om att förhindra icke godkänd programvara från att köras i systemet, tillåta rollbaserad administration och rättighetshantering samt att fungerar ihop med andra säkerhetslösningar [WTM13].
- Kontrollera leverantörens kostnadsbild för uppgradering av resurser så att denna inte väsentligt avviker från det tecknade avtalet. Det är viktigt

att inte behöva byta molntjänstleverantör bara för att det är för dyrt att uppgradera plattformen [INT5].

- Kontrollera hur licenshantering sker i förhållande till de komponenter som skall hanteras via molnplattformen. Många industriella informations- och styrsystem är fortfarande beroende av hårdvarulicenser vilket kan bli svårt att implementera i molntjänster [INT5].

Ett generellt råd är att vara mycket noggrann med riskanalysen innan utlokalisering av delar som kan påverka processen sker. Att exponera kontrollfunktionalitet kan ge större konsekvenser än att bara exponera data ur ett system. Även organisationens interna kompetens inom säkerhet för IT-system och industriella informations- och styrsystem samt processens känslighet bör beaktas innan molntjänster används. Notera dock att användandet av en molntjänst inte tar bort behovet av att kunna förstå och kravställa säkerhetsfunktioner, det påverkar bara behovet av att själv kunna konfigurera och underhålla systemen.

Huruvida en molntjänst ska användas eller inte måste dock avgöras från fall till fall och alltid i samråd med oberoende experter med spetskompetens inom IT- och säkerhet inom industriella informations- och styrsystem [INT1].

Litteraturlista

[AB18] A. Bryk (2018), *Cloud Computing: A New Vector for Cyber Attacks*, https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks, läst 2018-04-11

[AFR18] Amazon Web Services (2018), https://aws.amazon.com/freertos/, läst 2018-02-28

[AG16] A. Griffin (2016), *Dropbox Hack: Cloud storage company hacked, potentially revealing over 60 million passwords*, The Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/news/dropbox-hack-cloud-storage-company-hacked-potentially-revealing-over-60-million-passwords-a7218521.html, läst 2017-05-09

[AWS18] Amazon (2018), https://aws.amazon.com/iot-core/, läst 2018-02-28

[BMSA15] T. Baker, M. Mackay, A. Shaheed, B. Aldawsari (2015), *Security-Oriented Cloud Platform for SOA-Based SCADA*, 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Shenzhen, ss. 961-970

[CERT-SE17] CERT-SE (2017), *Cloudflare har läckt data från sin reverse-proxy-tjänst*, https://www.cert.se/2017/02/cloudflare-upptacks-ha-lackt-data-fran-deras-reverse-proxy, läst 2017-05-09

[DE15] D. Eidenskog (2015), *Intervjuguide arkitektur*, Totalförsvarets forskningsinstitut, FOI Memo 5310

[DEBL17] D. Eidenskog, B. Lindahl (2017), *Industriella protokoll i Sverige*, Totalförsvarets forskningsinstitut, FOI-R--4438--SE

[GCI18] Google (2018), https://cloud.google.com/solutions/iot/, läst 2018-03-02

[GEP18] General Electric (2018), https://www.ge.com/digital/predix-platform-foundation-digital-industrial-applications, läst 2018-03-02

[GF16] A. Grattafiori (2016), *Understanding and Hardening Linux Containers,* https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/2016/april/ncc_group_understanding_hardening_linux_containers-1-1.pdf, läst 2018-05-18

[GKW15] S. Goose, J. Kirsch, och D. Wei (2015), *SKYDA: cloud-based, secure SCADA-as-a-service*, Int. Trans. Electr. Energ. Syst., Vol. 25, ss. 3004–3016. doi: 10.1002/etep.2018

[HK12] H. Karlzén (2012), *Molnet – möjligheter och begränsningar*, Totalförsvarets forskningsinstitut, FOI-R--3381--SE

[INT1] intervju med en IT-chef, tillika biträdande säkerhetsskyddschef, på ett stort kommunalt vattenverk i Sverige, utförd 2017-06-12

[INT2] intervju med en konsult specialiserad på trådlös kommunikation i SCADA-system, utförd 2017-06-14

[INT3] intervju med en tekniker och en säljare av säkerhetsbryggor för SCADA-system, utförd 2017-06-14

[INT4] intervju med en konsult inom SCADA-system, utförd 2017-06-14

[INT5] intervju med infrastrukturarkitekt med erfarenhet av SCADA-system, utförd 2018-05-14

[IT17] I. Thomson (2017), *Cloudbleed: Big web brands 'leaked crypto keys, personal secrets' thanks to Cloudflare bug*, The Register, https://www.theregister.co.uk/2017/02/24/cloudbleed_buffer_overflow_bug_spaffs_personal_data/, läst 2017-05-09

[JH16] J. Hertz (2016), *Abusing Privileged and Unprivileged Linux Containers*, https://www.nccgroup.trust/uk/our-research/abusing-privileged-and-unprivileged-linux-containers/, läst 2018-05-18

[LDP11] F. Lombardi, R. Di Pietro (2011), *Secure virtualization for cloud computing*, Journal of Network and Computer Applications, Volume 34, Issue 4, ss. 1113-1122

[MA18] Microsoft (2018), https://azure.microsoft.com/sv-se/, läst 2018-02-28

[MAH18] Microsoft 82018), https://azure.microsoft.com/sv-se/services/iot-hub/, läst 2018-02-28

[MBAAS17] Wikipedia (2017), https://en.wikipedia.org/wiki/Mobile_backend_as_a_service, läst 2017-05-09

[MIC18] Microsoft (2018), https://www.microsoft.com/en-us/iot-central/, läst 2018-02-28

[MIC16] Microsoft (2016), https://partner.microsoft.com/pl-pl/training/azuresalesstarprogram/top-cloud-threats-2017-and-how-vendors-will-respond-with-security, läst 2018-04-11

[MSA17] Microsoft (2017), https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/, läst 2017-05-09

[MSB17] Myndigheten för samhällsskydd och beredskap (2017), *Frågor och svar om Cloud Hopper*, https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Omfattande-cyberangrepp-hos-driftleverantorer/Fragor-och-svar-om-Cloud-Hopper/, läst 2017-05-09

[NIST11] National Institute of Standards and Technology (2011), *The NIST Definition of Cloud Computing*, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, läst 2017-05-09

[PWC17] PwC UK och BAE Systems (2017), *Operation Cloud Hopper*, https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf, läst 2017-05-09

[QFH11] Q. F. Hassan (2011), *Demystifying Cloud Computing*, CrossTalk. http://static1.1.sqspcdn.com/static/f/702523/10181434/1294788395300/201101-Hassan.pdf?token=Yk%2FMAJpZWISljeWSt%2BFhWaHhOFI%3D, läst 2017-05-09

[RFT18] Rockwell Automation (2018), https://www.rockwellautomation.com/rockwellsoftware/overview.page, läst 2018-03-02

[SAS16] A. Sajid, H. Abbas, K. Saleem (2016), *Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges*, IEEE Access, vol. 4, ss. 1375-1384, 2016

[SGR09] N. Santos, K. P. Gummadi, R. Rodrigues (2009), *Towards trusted cloud computing*, Proceedings of the 2009 conference on Hot topics in cloud computing (HotCloud'09). USENIX Association, Berkeley, CA, USA

[SIEMENS18] Siemens (2018), https://w3.usa.siemens.com/smartgrid/us/en/transmission-grid/solutions/Documents/SCADA_Flyer_HiRes.pdf, läst 2018-05-14

[SK11] S. Subashini, V. Kavitha (2011), *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, vol. 34:1, ss. 1-11

[SK97] S. Kvale (1997), *Den kvalitativa forskningsintervjun*, Lund: Studentlitteratur

[SMS18] Siemens (2018), *MindSphere - The Internet of Things (IoT) Solution*, https://www.siemens.com/global/en/home/products/software/mindsphere.html, läst 2018-03-02

[SSW16] Siemens (2016), *MindSphere and MindConnect Elements – Security Whitepaper*, erhållet via mail från MSB 2017-05-23

[WTM13] K. Wilhoit (2013), *SCADA in the Cloud - A Security Conundrum?*, http://www.trendmicro.it/media/misc/scada-in-the-cloud-a-security-conundrum-en.pdf, läst 2017-05-09

[ZL12] D. Zissis, D. Lekkas (2012), *Addressing cloud computing security issues*, Future Generation Computer Systems, vol. 28:3, ss. 583-592

Bilaga A Intervjuguide

Mål

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

1) Vad innebär molntjänster för industriella informations- och styrsystem?
    a. Hur påverkar styrsystemspecifika egenskaper molntjänster?
    b. Vilka omständigheter gör molntjänster lämpligt eller olämpligt som lösning?
    c. Vilka konsekvenser och risker finns med molntjänster för styrsystem?
2) Vilka förväntning har de intervjuade eller deras organisationer haft inför introduktion av molntjänster?
3) Hur har man gått till väga för att genomföra introduktion av molntjänster?
4) Vilka erfarenheter har man gjort under denna process?
5) 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 forsknings-institut (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 molntjänster.

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 under 2017. Rapporten kommer att beskriva vad molntjänster är och hur det relaterar till informationssäkerhet. Rapporten kommer även att belysa ett antal områden som konsekvenser och risker med molntjänster och vilka slutsatser de intervjuade har dragit av sitt arbete med molntjänster.

Intervjuguide

Bakgrundsinformation om den intervjuade

1) Vilka erfarenheter har du/ni av molntjänster i kontexten av styrsystem i ditt arbete?

2) Är informationssäkerhet något du/ni jobbar med regelbundet?

3) Hur länge har du/ni jobbat med molntjänster?

Inför att introducera molntjänster

4) Hur skulle du/ni beskriva vad molntjänster i kontexten av styrsystem innebär?

5) Varför började er organisation med molntjänster?

6) Vilka förväntningar hade du/ni på molntjänster, vilka fördelar förväntade du/ni er?

7) Finns det någon etablerad metod för att introducera molntjänster i styrsystem?

- **a.** Användes den?

8) Hur såg arbetsgången inför att introducera molntjänster ut?

- **a.** Hur tog du/ni reda på vad du/ni ville göra?
- **b.** Hur kom du/ni fram till vilka krav molntjänsten skulle uppfylla?
- **c.** Fanns det specifika krav som tillkom på grund av styrsystemspecifika egenskaper som tillgänglighetskrav eller dylikt? (Ingick det säkerhetsanalyser i denna? Informationssäkerhet?)

Genomförande molntjänster

9) Vem eller vilka var det som genomförde introduktionen av molntjänster (roller)?

10) Fanns det svårigheter? Vad?

11) Fanns det saker som fungerade oväntat väl? Vad?

Slutresultatet

12) Gav molntjänsterna de fördelar du/ni förväntade er? (Se fråga 5)

13) Har du/ni gjort någon informationssäkerhetsanalys av det nya systemet? Resultat? Enligt förväntningar?

14) Vilka erfarenheter har du/ni gjort som du/ni skulle velat veta innan du/ni genomförde introduktionen av molntjänster?

Förbättringsmöjligheter?

15) Har du/ni några konkreta förslag för andra som ska börja ett arbete med molntjänster? [Återkoppla till frågor]

- **a.** Behov, konkreta åtgärder, effekter?
- **b.** Finns det något av dessa som är viktigare än de övriga? Varför?

16) Finns det faktorer som skulle göra en molntjänster olämpliga? 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