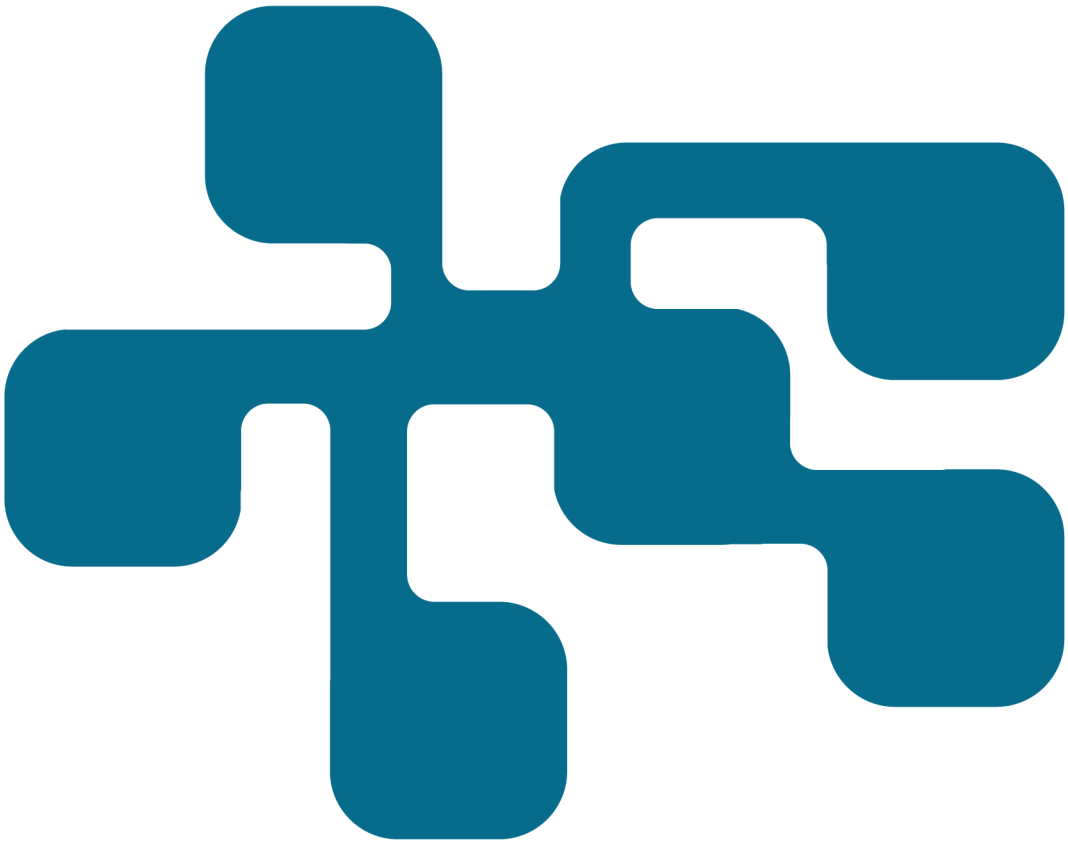
NCS3 - Fjärranslutning

Fjärranslutningstekniker för industriella informations- och styrsystem

Christian Valassi, Lars Westerdahl

FOI
MSB



FOI-R--4751--SE
MSB 2018-03308
ISSN 1650-1942

April 2019

Christian Valassi, Lars Westerdahl

Fjärranslutning

Fjärranslutningstekniker för industriella informations- och styrsystem

Titel	Fjärranslutning
Title	Remote access
Rapportnr/Report no	FOI-R--4751--SE
Månad/Month	April
Utgivningsår/Year	2019
Antal sidor/Pages	49
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E72331
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Möjlighet att fjärransluta till interna resurser är en nödvändig del av den dagliga verksamheten för många organisationer. Upprättandet och hanteringen av sådan funktionalitet kan dock vara en komplex process när det finns flera olika kategorier av användare, både interna och externa, som från distans behöver tillgång till interna resurser av varierande skyddsvärde. För organisationer som saknar intern kompetens att kravställa och hantera fjärranslutning blir problemet än mer svårt att lösa.

Denna rapport ämnar förse intressenter med säkerhetsrelaterad information kring fjärranslutningar vilken kan användas som kompetensgrund när beslut kring fjärranslutning ska fattas. Rapporten illustrerar arbetsprocessen för att upprätta fjärranslutningsfunktionalitet samt visar vilka frågor och beaktanden organisationen bör kunna besvara genom hela processen. Vidare beskrivs de vanligaste formerna av teknik för fjärranslutning som också exemplifieras i form av tre olika användningsscenarier. I scenarierna diskuteras olika hot och risker samt beskrivs hur olika tekniker och kompletterande mekanismer kan appliceras för att minska sannolikheten för hoten och mildra effekterna av de konsekvenser som kan uppstå därav.

Rapportens resultat visar att de allra flesta hot och risker som relaterar till fjärranslutningar kan motverkas med hjälp av de tekniker som rapporten beskriver. Samtidigt är det viktigt att påpeka att dessa tekniker generellt måste kompletteras med ytterligare säkerhetsfunktionalitet för att risker effektivt ska kunna minimeras. Resultatet visar också att en del risker inte kan motverkas eller mildras med hjälp av teknikerna. I dessa fall är det istället viktigt att minimera effekterna av de relaterade konsekvenserna.

Rapporten avslutas med ett antal rekommendationer för aspekter som bör uppfyllas innan processen med att upprätta fjärranslutning påbörjas, vilket bland annat inkluderar identifiering av behov, genomförande av säkerhetsanalys och applicering av relevanta säkerhetspolicyer.

Nyckelord: Fjärranslutning, säkerhetspolicy, säkerhetsanalys, industriella informations- och styrsystem.

Summary

The ability to access internal resources remotely is part of many organisations' day-to-day operations. Establishing and managing such functionality can however be a complex process when there are different categories of users, both internal and external, that need remote access to internal resources and information of varying protection value. The problem is even harder to solve for organisations that, in-house, lack the competence and capacity to define requirements and manage remote access solutions.

This report aims to provide stakeholders with security-related information pertaining to remote access issues, which can be used as a foundation for making decisions related to establishing remote access infrastructure. The report describes the process of constructing remote access functionality in an organisation and describes the questions that need to be answered, and the considerations to be made throughout this process. Furthermore, the report describes the most common remote access methods that provide remote access functionality. These methods are exemplified in three scenarios that discuss threats, risks and describe how each method, complemented with additional security mechanisms, can be used to lower the probability of a threat or to mitigate the effects of the consequences of an attack.

The results of this report show that most threats and risks pertaining to remote access in an organisation can be mitigated or counteracted with the techniques described in the report. However, it is important to note that each technique generally needs to be supplemented with additional security mechanisms. The results also show that some threats and risks cannot be mitigated by any of these techniques. In these cases, it is instead important for the organisation to focus on minimising the effects of related consequences.

The report ends with a number of recommendations for aspects that need to be fulfilled before the process of constructing a remote access infrastructure can begin. These recommendations include identifying the needs of the organisation, performing security analyses and implementing relevant security policies.

Keywords: Remote access, security policy, security analysis, industrial control systems.

Innehållsförteckning

1. Inledning

Många organisationer använder fjärranslutningstekniker i den dagliga verksamheten, vilket innebär att fjärranslutningsmöjligheter är en viktig del i den övergripande arbetsprocessen. Dessa tekniker används bland annat av anställda, konsulter, leverantörer eller affärspartners i syfte att utföra arbete från en extern plats. Att säkerställa dessa fjärranslutningar, både driftsäkerhetsmässigt och informationssäkerhetsmässigt, är därför kritiskt för organisationers verksamhet.

Säkerställandet av denna typ av kommunikation vilar, som mycket annat, på den så kallade CIA-triaden (*Confidentiality*, *Integrity* och *Availability*). *Confidentiality* eller *konfidentialitet* innebär för fjärranslutningskommunikation och relaterad data, att denna inte kan läsas av obehöriga aktörer. *Integrity* som på svenska översätts till *riktighet* innebär att olovliga ändringar i informationen som kommuniceras upptäcks. *Availability*, vilket översätts till *tillgänglighet*, innebär att behöriga användare har tillgång till de resurser de behöver via fjärranslutning när resurserna behövs.

Varje enhet och komponent som på något sätt inkluderas i fjärranslutningskommunikation (exempelvis fjärranslutningsservrar och användarenheter) bör säkras mot potentiella hot. Säkerhetsarbetet bör baseras på organisationens definierade hotmodeller samt de potentiella sårbarheter som finns med vald kommunikationstyp och infrastruktur. Processen med att påbörja och genomföra ett sådant säkerhetsarbete kan dock vara otydlig och komplicerad eftersom det finns många olika aspekter att ta hänsyn till. Användandet av vedertagna standarder och praxis (eng. *best practice*) är en bra utgångspunkt, men att applicera dessa i praktiken kan vara komplicerat.

1.1 Syfte och mål

Totalförsvarets forskningsinstitut (FOI) har inom ramen för *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3) fått i uppdrag av *Myndigheten för samhällsskydd och beredskap* (MSB) att undersöka fjärranslutningsteknik i syfte att ge en översikt av metoder och tekniker för säker fjärranslutning i industriella informations- och styrsystem. Målet med studien är att presentera exempel på tekniska lösningar för fjärranslutning utgående ifrån vilken åtkomst som systemägaren tillåter via fjärranslutning.

Fjärranslutning definieras i denna rapport som förmågan att ansluta till virtuella eller verkliga nätverk, servrar och datorer från en avlägsen plats för att få tillgång till information och funktionalitet.

1.2 Metod och genomförande

Inledningsvis genomfördes en litteraturstudie i syfte att identifiera standarder, praxis och olika tekniker för fjärranslutning. Därefter formulerades tre scenarier utifrån situationer som bedömdes vara realistiska för olika typer av organisationer som brukar fjärranslutning i verksamheten.

De framtagna scenarierna analyserades med stöd av Försvarsmaktens metod för säkerhetsanalys (Försvarsmakten 2013). Styrkan med denna metod är att den fokuserar på vad som ska skyddas och de relevanta oönskade händelser som i bästa möjliga mån ska undvikas. Genom att fokusera på tillgången och de oönskade händelserna behöver analytikern endast identifiera hot med direkt bäring på de oönskade händelserna. Detta ger en effektivare och mer fokuserad analys.

Metoden för säkerhetsanalys omfattar fem steg:

Steg 1. Kritiska tillgångar för verksamheten identifieras och vid behov prioriteras även dessa tillgångar sinsemellan. För varje tillgång definieras en till flera oönskade händelser samt en eller flera konsekvenser om händelsen skulle inträffa.
Steg 2. Därefter identifieras hot vilka skulle kunna orsaka en eller flera av de oönskade händelserna. Ett hot kan realisera flera oönskade händelser, lika väl som att en oönskad händelse kan realiseras av flera olika hot. För varje hot bedöms också en aktörs möjlighet att utföra ett angrepp.
Steg 3. Utifrån det system som står i fokus för analysen där tillgångarna ingår, identifieras sårbarheter som en aktör kan nyttja för att uppnå en oönskad händelse.
Steg 4. Därefter bedöms sannolikheten för att de oönskade händelserna ska inträffa och vilka konsekvenser detta skulle få. Om skyddsmekanismer redan finns på plats i systemet, tas dessa med i bedömningen.
Steg 5. Resultatet av riskbedömningen analyseras och, vid behov, föreslås ytterligare skyddsåtgärder för att reducera risknivån. De skyddsåtgärder som föreslås kan syfta till att minska sårbarheten alternativt minska hotet. Det sista är dock svårare att åstadkomma. Riskbedömningen görs om för att ta hänsyn till de nya åtgärder som föreslagits. Steg 5 återupprepas tills dess att en acceptabel risknivå erhålls.

I denna rapport diskuteras hypotetiska system dit aktörer fjärransluter. Detta upplägg medför att det inte går att identifiera existerande sårbarheter samtidigt som att tillskriva det hypotetiska systemet sårbarheter inte är meningsfullt inom ramen för rapporten. Därför kommer inte någon riskbedömning att göras, utan fokus ligger på att identifiera oönskade händelser och hot samt vilka skyddsmekanismer som mildrar eller motverkar dessa.

1.3 Läshänvisning

Kapitel 2 beskriver nödvändiga förutsättningar för möjligheten att använda fjärranslutningar på ett korrekt och säkert sätt. I kapitlet beskrivs bland annat policy och användarkategorier. Kapitel 3 beskriver olika tekniker som kan användas för fjärranslutning. I kapitel 4 beskrivs och analyseras tre scenarier för användning av fjärranslutning i olika situationer. Avslutningsvis diskuteras resultat och rekommendationer i kapitel 5.

2. Förutsättningar för fjärranslutning

I detta kapitel presenteras säkerhetsförutsättningar ur ett övergripande och primärt organisatoriskt perspektiv, framförallt gällande framtagning av en generell säkerhetsfilosofi och relevanta säkerhetspolicyer såväl som en beskrivning av vanligt förekommande användarkategorier inom industriella informations- och styrsystem.

2.1 Principiell säkerhetsfilosofi

Ett industriellt informations- och styrsystem består av komponenter vilka både fysisk och logiskt är sammankopplade i ett nätverk. I detta nätverk finns sannolikt även säkerhetsfunktioner som syftar till att bevara systemets konfidentialitet, riktighet och tillgänglighet mot både interna och externa hot. Tillsammans utgör ett sådant system en säkerhetsdomän, det vill säga ett avgränsat system med en ägare och en policy för hur systemet får användas (Försvarets materielverk (FMV) 2013, s.34; National Institute of Standards and Technology (NIST) 2013, s.B-22).

I ett avgränsat system är säkerhetsdomänen enkel att tydligt definiera, men för system med exempelvis flyttbara komponenter, externa kommunikationsbehov eller olika skyddsnivåer blir situationen mer komplex. Ett exempel på denna komplexitet kan vara en användare som ansluter till ett system från en plats utanför systemets fysiska lokaler. Logiskt befinner sig den behöriga användaren i systemet men fysiskt utanför, vilket medför att det fysiska skyddet som normalt ingår i helheten inte längre gäller. Ett annat exempel kan vara att leverantören av ett system fjärransluter till systemet för att utföra underhålls-arbete. I detta fall har en utomstående part tillgång till systemet, dess information och dess funktionalitet. Båda exemplen illustrerar en situation där systemägarens säkerhetsdomän utökas till att gälla områden som är svårare att kontrollera och som ställer andra typer av krav. Det kan dock vara viktigt i sammanhanget att notera att det inte enbart är kommunikation utanför en organisation som medför en utökad säkerhetsdomän. Även internt kan det finnas delar av systemen som kräver en mer kontrollerad informationsdelning.

Användare i ett system, vare sig de är anställda eller externa partners, bör inte ha mer tillgång till systemets funktionalitet och information än nödvändigt. En begränsad åtkomst till systemet, utifrån respektive användares arbetsuppgifter, begränsar sannolikheten för att en antagonist kan få tillgång till värdefulla resurser. Dessutom begränsas sannolikheten för att handhavandefel och andra icke medvetna hot får stora konsekvenser. I mer konkreta termer innebär detta att en användare endast får tillgång till den funktionalitet eller gränssnitt som krävs för att kunna utföra sina arbetsuppgifter, jämfört med att få åtkomst till en

hel server eller ett helt nätverk. En sådan uppdelning av rättigheter gällande nätverksresurser, funktioner och information är inte alltid möjlig att införa. För verksamheter där användarnas informationsbehov är svåra att förutse kan strikta begränsningar hämma möjligheterna för användarna att utföra sitt jobb, vilket i sin tur påverkar verksamheten negativt. I sådana fall kan det vara viktigare att spåra användarnas aktiviteter i syfte att kunna rekonstruera händelseförlopp snarare än att begränsa användningen.

Det kan vara bekvämt att definiera hot i form av något som uppträder utanför det egna systemet. Svagheten med ett sådant resonemang är dock uppenbar i dagsläget, då det finns flera exempel på angrepp initierade från insidan av system. Isolerade system, eller system med ett luftgap mellan systemet och omvärlden, har tidigare ansetts som säkra, men angrepp såsom Stuxnet[1] bör ha minskat tilltron till dessa. Det finns fortfarande ett behov av att kraftigt kunna begränsa åtkomst till vissa system, men det finns samtidigt ofta ett behov av att kunna kommunicera till och från dessa system. Detta gör att det blir svårt att dra en tydlig gräns mellan vad som anses vara en säker del av ett system och en mer osäker del. Således behöver säkerhetsfunktioner upprättas i flera led så att de kan hantera olika typer av situationer som kan utgöra ett hot mot systemet.

2.2 Policyer

En policy är i sin mest grundläggande form en etablerad plan eller idé för hur en organisation eller individ ska agera i en särskild situation. Policyer fyller en viktig roll i alla organisationers säkerhetsarbete, inte minst gällande IT- och informationssäkerhet. Dessa policyer syftar till att säkerställa att alla användare i organisationens domäner (exempelvis nätverk och system) följer uppsatta regler och riktlinjer gällande IT- och informationssäkerhet i organisationens domäner. Syftet med policyer är i sin tur att skydda organisationen från skada, exempelvis gällande ekonomi, juridiska påföljder eller anseende.

Ett av de första stegen i att anskaffa fjärranslutningsfunktionalitet för en organisation bör vara skapandet och tillämpningen av policyer som specifikt hanterar fjärranslutning och säkerheten relaterat till detta. En av de första frågorna som bör besvaras är rimligtvis: *vilka organisatoriska mål är fjärr-*

[1] Stuxnet är namnet på den datormask som användes för att sabotera urananrikningscentrifuger i Natanz, Iran år 2010. Det som är signifikativt för Stuxnet är dess komplexitet – masken utnyttjade vid angreppet fyra olika *zero-day* sårbarheter, vilket aldrig tidigare skådats; masken är även väldigt selektiv i vilka enheter den infekterar. Mer konkret riktar sig masken att infektera en specifik typ av mjukvara från Siemens och även till flyttbara enheter för att spridas till privata nätverk och över luftgap (Langner 2013).

anslutningsfunktionalitet tänkt att uppfylla? Detta är en övergripande fråga som kan behöva brytas ned till mer specifika frågor, exempelvis: *finns det grupper av anställda som behöver fjärranslutningsmöjligheter för att utföra sina uppgifter?* Eller, *kan effektiviteten hos de anställda och organisationen som helhet förbättras genom fjärranslutningsmöjligheter?* Exakt vilka frågor som bör formuleras och besvaras skiljer sig troligtvis mellan olika typer av organisationer. NIST (Souppaya & Scarfone 2016) ger ett antal rekommendationer som kan anses generella för fjärranslutningar oavsett vilken typ av organisation det rör:

- Utforma och tillämpa en säkerhetspolicy som definierar krav som ställs på distansarbete och fjärranslutningar.
- Utforma och tillämpa en säkerhetspolicy baserat på antagandet att externa miljöer innehåller fientliga hot.
- Utforma och tillämpa en säkerhetspolicy för att effektivt säkra organisationens fjärranslutningsservrar.
- Utforma och tillämpa en säkerhetspolicy för att skydda klientenheter mot vanliga hot och sårbarheter och uppdatera denna regelbundet samt specificera vilka klientenheter som har rätt att ansluta till interna system via fjärranslutning.

Mer riktade frågeställningar ges av Imran (2015). Rekommendationerna avser policyer för tunnlade (se avsnitt 3.1) fjärranslutningar, men de är även användbara i en något vidare bemärkelse. Imran (2015) trycker först på ett antal konkreta frågor utöver förutsättningarna för fjärranslutningen:

- Vilka användarkategorier avses?
- Vilken åtkomst till de interna systemen kommer att medges?
- Med vilka enheter kommer användarna tillåtas att ansluta till det interna systemet?
- Hur kommer användarna att autentiseras?

Vidare trycker även Imran (2015) på att en plan ska finnas i det fall som fjärranslutningen missbrukas och används för angrepp.

En organisation bör definiera vilka fjärranslutningstekniker som är tillåtna att använda för att komma åt och använda interna resurser. Vilka tekniker som är relevanta att tillåta påverkas till stor del av skyddsvärdet i de system och den information som fjärranslutningen är tänkt att hantera. Det bör även definieras vilka användare som har tillåtelse att använda fjärranslutningar samt vilken information dessa användare har tillgång till. Denna policy kan baseras på andra policyer relaterade till användarkategorier och vilken information olika grupper har tillgång till. Exempelvis bör en användare som inte har tillgång till visst

material lokalt på de interna nätverken heller inte ha tillgång till detta material via fjärranslutning.

En organisation bör anta att externa miljöer innehåller fientliga hot och genomföra åtgärder för att mildra dessa risker. Organisationen bör planera för att potentiella antagonister kommer att försöka få tillgång till klientenheter fysiskt eller logiskt med målet att komma åt organisationens resurser. Detta kan exempelvis ske med hjälp av lagrad data på klientenheten eller via fjärranslutningsmöjligheten till företagsnätverket. Organisationen bör därför implementera säkerhetsmekanismer för att hantera stöld eller förlust av klientenheter. Detta kan exempelvis uppnås genom att kryptera klientenhetens hårddisk eller genom att inte tillåta att data från fjärranslutningar lagras lokalt på klientenheterna. Starka autentiseringsmekanismer, i regel flerfaktor, bör användas för att minimera hotet av återanvändning av fjärranslutningsuppkoppling, kombinerat med *vitlistning* av fjärranslutande enheter för att minimera konsekvenserna av stulna inloggningsuppgifter.

Det är av specifikt intresse för organisationen att effektivt säkra de fjärranslutningsservrar som används eftersom dessa servrar representerar ingången som ger utomstående enheter tillgång till organisationens interna resurser. Dessa servrar är därför ofta ett viktigt mål för en antagonist, inte bara för obehörig åtkomst av interna resurser utan även som kontrollpunkt för att avlyssna och manipulera trafik eller för att angripa andra enheter i de interna nätverken. Det är därför av särskild vikt för organisationen att alltid se till att dessa servrar har de senaste säkerhetsuppdateringarna och att de endast kan hanteras via betrodda enheter av auktoriserade administratörer.

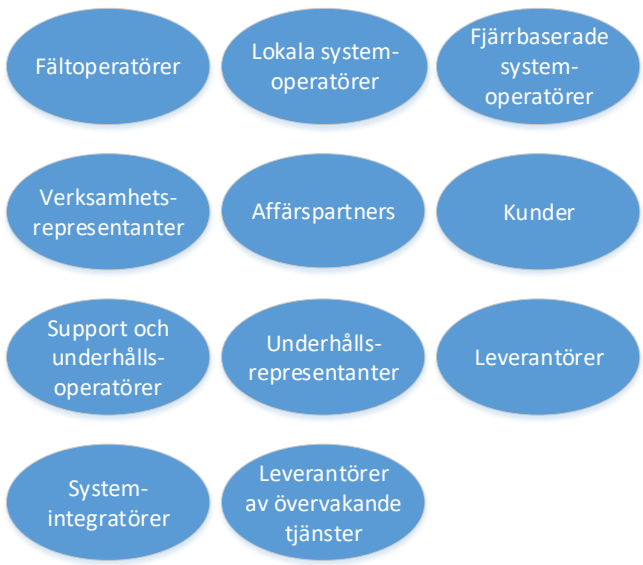
Nyttjande av extern kompentens istället för en intern IT-avdelning för att hantera kravställning, implementation och drift är vanligt förekommande. Detta eftersom organisationer i regel önskar att minimera storleken av den egna IT-avdelningen för att istället upphandla många av dess funktioner. Resultatet blir ofta en intern kompetensförlust, inte minst säkerhetsmässigt. Organisationer bör därför sträva efter att behålla nyckelpersonal internt, speciellt för kravställning och säkerhetsstyrning. Sådan personal innehar både viktig teknisk kunskap, verksamhetskunskap och är troligtvis även mer investerade i organisationens mål avseende en välfungerande IT-miljö än vad en extern part är. Samtidigt bör det även undvikas att nyttja säkerhetstjänster som levereras av samma externa part som hanterar IT-drift utan att dessa först kvalitetssäkras och kravställs av, i förhållande till leverantören, oberoende säkerhetsexperter (FRA 2017).

2.3 Användarkategorier

Fjärranslutning är en vanlig lösning för att kommunicera med en anläggning eller ett system. En av orsakerna bakom detta i kontexten av industriella informations- och styrsystem är förstås den ökade datoriseringen och möjligheter till datorkommunikation, men även en högre grad av automation vilket möjliggör för fler intressenter att övervaka och påverka system.

Det finns flera anledningar att fjärransluta till ett system eller en anläggning, exempelvis kan en driftingenjör studera larm via en dator hemifrån, en leverantör kan utföra underhåll av mjukvara utan att behöva vara på plats. Fjärranslutning sker inte enbart fysiskt utanför en anläggning och in. Även inom en anläggning är fjärranslutningar vanliga, exempelvis när tekniker i anläggningens kontrollrum vill påverka en maskin på en annan plats i anläggningen.

Utifrån ett systems perspektiv kan alla användare delas in i kategorier där varje kategori innehåller en uppsättning behörigheter utifrån de behov som en användare i gruppen har gentemot systemet. Det finns sannolikt även individuella skillnader i behörighet för användare inom en användargrupp. Figur 1 presenterar en övergripande bild av möjliga användarkategorier (DHS/CPNI 2010).



Figur 1 Exempel på användarkategorier.

Fältoperatörer, lokala systemoperatörer och fjärrbaserade systemoperatörer är en samling användarkategorier med en i princip oinskränkt tillgång till anläggningens system. Det är sannolikt så att för stora anläggningar delas ansvar och därmed behörigheter upp mellan användare internt inom dessa kategorier, men på det stora hela är det kategorier med omfattande rättigheter. Användarna inom dessa kategorier är sannolikt anställda av anläggningens ägare, alternativt är det ett företag som arbetar under ett tidsbegränsat kontrakt.

Leverantörer av hela system eller delsystem har idag en stor påverkan på det levererade systemet, även efter leverans. Utöver rena garantiåtaganden kan leverantörer även erbjuda underhåll och support, vilka ofta utförs via en fjärranslutning från leverantören till systemet i fråga. I och med att ett garantiåtagande eller en supporttjänst kan medföra behov av övervakning av det levererade systemet (inte av själva produktionen inom anläggningen) medför detta behov av omfattande rättigheter i systemen. Ur en anläggningsansvarigs perspektiv bör det övervägas hur fjärranslutningen etableras och vad leverantören får göra, då denne ansluter ifrån en egenkontrollerad miljö utanför anläggningens säkerhetsdomän.

Systemintegratörer är den organisation som levererar det färdiga systemet till kunden. Systemintegratörer kan i vissa fall vara tillverkare av systemet, men är i andra fall en leverantör som sätter samman ett system av komponenter från andra leverantörer. I det senare fallet är det inte säkert att anläggningsägaren har direktkontakt med tillverkarna av de enskilda komponenterna då all kommunikation sker via integratören. En integratör kan få större rättigheter i ett system än en enskild leverantör då integratören ansvarar för hela systemet eller ett större delsystem.

Vissa produkter, särskilt inom IT-säkerhetsområdet, kan idag levereras paketerade som hård- och mjukvara eller som tjänster. I det första fallet tar kunden ansvar för övervakning och underhåll av produkten, men i det andra fallet ansvarar *leverantörer av övervakande tjänster* (eng. *managed services*). Leverantören, som tidigare beskrivits, hantera uppdateringar och underhåll men den primära uppgiften är att övervaka en eller flera komponenter, exempelvis en brandvägg. Leverantören behöver således rättigheter att påverka det system som övervakas, men inte i sådan utsträckning att anläggningens produktion påverkas utan att anläggningsägaren informeras om detta.

Tillgång till exempelvis material och bränsle är ett viktigt behov för produktionen, men det kan även vara lika viktigt med transporter av det som produceras. Det är få företag som vill ha större lager då detta medför kostnader och ekonomiska osäkerheter. För att hantera detta behöver inköps- och säljavdelningen tillgång till produktionsinformation så att de kan kommunicera behov till *underhållsrepresentanter* (eng. *supply chain*). Viss information,

angående exempelvis framtida bränsle- och transportbehov, kan vidarebefordras till leverantörer. Oavsett organisationstillhörighet är behovet primärt att ha tillgång till aktuell information, inte att kunna påverka produktionssystemen.

Företag samarbetar ibland med andra företag, tillfälligt eller över tid, mot ett gemensamt mål eller en produkt. I energisammanhang kommer denna typ av samarbeten sannolikt att öka när smarta system (exempelvis smart grid) införs. I smarta system kan det finnas flera jämställda aktörer som behöver dela information med varandra. Likt underhållsrepresentanter handlar det mest om informationsutbyte mellan *affärspartners*.

Kunder inom energisektorn, men även andra sektorer där en kontinuerlig produkt levereras, har idag flera möjligheter än innan att göra val baserat på tillgängliga produkter leverantörer. För att kunna göra dessa val behöver kunder tillgång till mer aktuell information än tidigare. Detta behov medför i sig självt inte ett behov av fjärranslutning. I exempelvis smart grid kan dock kunden även bli producent och därmed i någon mening en affärspartner till huvudägaren av nätet. Kundens egen produktion behöver kommuniceras till huvudägaren och dennes system.

En viktig del för den verksamhet som bedrivs är de interna ekonomiska processerna för debitering av kunders konsumtion av den tjänst eller produkt som erbjuds. *Verksamhetsrepresentanter* som kundadministratörer och säljare kan ha behov av aktuell produktionsdata, vilket medför behov av intern kommunikation mellan affärsledningssystem i kontorsnätverk och uppföljnings- eller analyssystem på kontrollnätet.

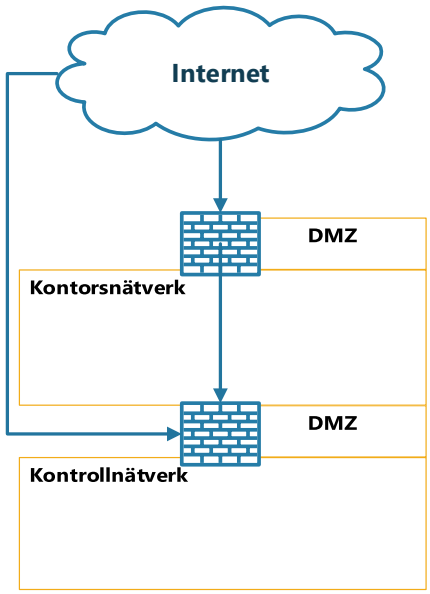
2.4 Anslutningspunkter

Nätverken i en anläggning kan antas vara uppdelade i minst två delar: ett kontorsnätverk och ett kontrollnätverk. Kontorsnätverket avser ett vanligt IT-nätverk för den affärsmässiga verksamheten av anläggningen. På ett sådant nät återfinns exempelvis servrar och applikationer för att hantera exempelvis epost, debitering, tidredovisning och planering. Ett kontorsnätverk är oftast anslutet till internet via en brandvägg. Kontrollnätverket är det nätverk där systemen som styr produktionen finns. På kontrollnätverket finns exempelvis styrsystem, PLC:er och operatörsgränssnitt (eng. *Human-Machine Interface*, HMI).

Det kan konstateras att det finns flera olika användarkategorier som har behov av fjärråtkomst till applikationer och system i en anläggning. Som framkom i avsnitt 2.3 så är behoven av åtkomst högst varierande och därmed även vilka system som användarna behöver ha åtkomst till. Fjärranslutning till kontorsnät är vanligt förekommande. Användare kan behöva tillgång till epost och tjänster

på intranät samt arbetsdokument. Från kontorsnätverken hanteras även affärsverksamhetens externa kommunikation exempelvis via en webbserver. System och tjänster som är avsedda att vara nåbara externt, såsom epost- och webbservrar, placeras oftast på ett eget nät mellan kontorsnätet och internet. Detta nätverk benämns som en *demilitariserad zon* (DMZ). En fjärranslutning till kontorsnätverk dirigeras oftast om till DMZ innan kommunikationen går vidare till aktuell applikation.

Även kontrollnätverk kan och bör ha en DMZ. Denna befinner sig då mellan kontorsnätverket och kontrollnätverket och syftar till att hantera kommunikation mellan dessa nätverk. En fjärranslutning för användare som har behov av att kommunicera med system på kontrollnätverket kan etableras i kontrollnätverkets DMZ, alternativt slussas trafik från kontorsnätverkets DMZ till kontrollnätverkets DMZ. Den trafik som slussas genom kontorsnätverket skickas genom en intern tunnel för att inte användaren ska lära sig något om det interna nätverket. En schematisk bild över anslutningspunkter visas i Figur 2.



Figur 2 Översikt över anslutningspunkter.

2.5 Alternativ till fjärranslutning

Fjärranslutning är ett sätt att tillgodose åtkomst till system för exempelvis övervakning, styrning och underhåll. Teknikerna ställer krav på hur fjärranslutningen etableras, men även vad som ges åtkomst till. Om fjärranslutning

bedöms som en olämplig teknik för verksamheten återstår alternativ där exempelvis tekniker, leverantörer och underhållspersonal måste vara fysiskt närvarande för att utföra sitt arbete.

Att kräva fysisk närvaro för support och underhåll reducerar internetbaserade risker kraftigt, men de försvinner inte helt. En servicetekniker behöver fortfarande kunna kommunicera med anläggningens system, så en dator är nödvändig. Att bära in en dator på en anläggning och koppla in denna i ett system ger inte en dubbelriktad kommunikation till och från anläggningen utifrån, men anläggningsägaren vet inte var den datorn har varit, vad den varit uppkopplad emot eller vilka som har använt den. Således är införandet av en dator i princip ett lika stort hot som en internetanslutning när det gäller skadlig kod. Kopplar dessutom teknikern upp sig mot internet med den medförda datorn skapas en okontrollerad bakdörr in i systemet.

Ny information måste dock tillföras på något sätt, särskilt om det gäller uppdateringar. Tvingas leverantörer, support och integratörer till att endast använda utrustning som tillförts från systemägaren samt en mer rigorös användarpolicy minskar riskerna ytterligare något. Informationen måste dock fortfarande föras över till avsedd dator, exempelvis via ett USB-minne. Dessa flyttbara medium utgör en risk på samma sätt som en dator som förs in i anläggningen. Anläggningsägaren kan således inte veta var dessa medium har varit, vad de innehåller eller vem som använt dem tidigare.

3. Teknik för fjärranslutning

I detta kapitel beskrivs fyra kategorier av fjärranslutning som vanligen används av kommersiella aktörer idag. Dessutom ges exempel på tekniska applikationer inom dessa kategorier. NIST (Souppaya & Scarfone 2016) beskriver fyra fjärranslutningskategorier: tunnlar, applikationsportaler, fjärråtkomst till skrivbord samt direkt applikationstillgång. Dessa kategorier har enligt NIST (Souppaya & Scarfone 2016) ett antal gemensamma egenskaper som beskrivs nedan:

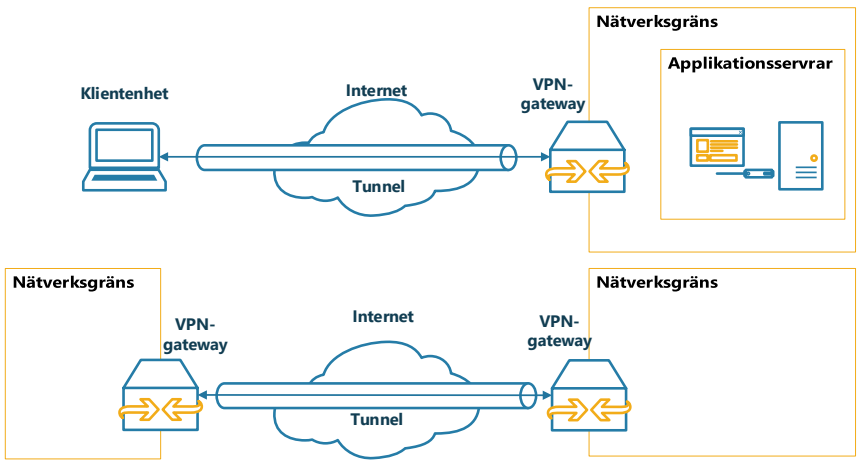
- De har alla möjlighet att kryptera kommunikationskanalen för att skydda dataflödet i denna. För *virtuella privata nätverk* (VPN) och andra tunnelkommunikationer finns detta inbyggt, medan kryptering ofta finns inkluderat som ett alternativ för andra former av fjärranslutningskommunikation (exempelvis *fjärråtkomst till skrivbord*).
- Alla kategorier är beroende av den fysiska säkerheten hos klientenheterna.
- Flera olika typer av autentiseringsmekanismer kan användas för alla kategorier. Detta ger en flexibilitet eftersom organisationens existerande autentiseringsmekanismer troligtvis kan användas även för autentisering mot fjärranslutningsklienten.
- De flesta implementationer av dessa kategorier kan möjliggöra lagring av data på klientenheter både avsiktligt och oavsiktligt. Detta ger användare möjlighet att använda och utföra arbete på data lokalt på sina enheter. Samtidigt kan detta innebära en säkerhetsrisk om data lagras på enheter (exempelvis i operativsystemets *page file* eller i en cache för en webbläsare). Eftersom dessa data kan bli tillgängliga för en antagonist om denne exempelvis stjäl datorn eller via ett digitalt angrepp får tillgång till datorn. Det är därför väldigt viktigt att alla data som kan delas via fjärranslutning täcks in av organisationens policy för distribution av data samt att hemliga data inte öppet hanteras via fjärranslutning.

Det finns även gemensamma problem eller sårbarheter för de fyra fjärranslutningskategorierna. Exempelvis är bristen på fysiska säkerhetskontroller ett problem. Fjärranslutningar används oftast utanför organisationens interna nätverk och är då även fysiskt utanför den kontroll som kan tillämpas innanför organisationens väggar. Detta innebär i sin tur att enheter som vistas i publika miljöer löper en större risk att tappas bort eller stjälas. Ett relaterat problem är att dessa enheter ansluter mot organisationens nätverk från vad som kan vara osäkra nätverk, vilket kan leda till ökad exponering. Enheter som kopplas upp mot nätverk utanför organisationens kontroll löper kan även löpa större risk att infekteras av skadlig kod beroende på vilken säkerhet som erhålls av dessa nätverk. Detta utsätter i sin tur organisationens nätverk för potentiell fara när

dessa enheter ansluter till de interna nätverken. De interna resurser som kan nås via fjärranslutning utsätts även dessa för samma risk (Souppaya & Scarfone 2016; DHS 2010).

3.1 Tunnlar

Tunnlar används vanligtvis i form av VPN. Det som utgör själva tunneln för kommunikationen är den krypterade anslutningen mellan en klientenhet och en VPN-gateway. VPN-tunnlar används även för att koppla samman nätverk med varandra, Figur 3 nedan visar en översiktlig lösning för båda anslutningstyper. Krypteringen av tunneln skyddar kommunikationen mot både avlyssning och manipulering av innehåll. För att kunna använda VPN måste användaren antingen ha en VPN-mjukvara installerad på sin enhet eller vara ansluten till ett nätverk som har ett VPN-gatewaysystem. När en VPN-tunnel mellan en klientenhet och organisationens VPN-gateway har etablerats får användaren tillgång till många av de resurser som finns på organisationens interna nätverk. Vanligtvis finns dessa resurser lagrade i separata applikationsservrar (Souppaya & Scarfone 2016; DHS 2010).



Figur 3 Översiktlig VPN-lösning.

VPN skyddar inte bara kommunikationen i tunneln genom kryptering utan kan även autentisera användare och hantera åtkomstkontroll, exempelvis genom att specificera vilka enheter som kan nås via fjärranslutning (Souppaya & Scarfone 2016; Imran 2015). En viktig aspekt att ha i åtanke gällande tunnlar är att de endast skyddar själva kommunikationen mellan ändpunkter och att ändpunkterna själva fortfarande kan vara sårbara.

De vanligaste typerna av VPN som används idag är *SSL/TLS*[2]- och *IPsec*[3]-baserade. Det går även att använda *SSH*[4] för dessa ändamål, dock med viss ökad arbetsinsats och underhåll (Souppaya & Scarfone 2016; Imran 2015).

3.2 Applikationsportaler

En portal är i detta avseende en server som via ett centraliserat gränssnitt ger tillgång till en eller flera applikationer via de interna applikationsservrarna. En portal är oftast webbaserad, vilket innebär att portalen för användaren ser ut som en vanlig webbsida I portalservern finns applikationsklientmjukvara som kommunicerar med de interna applikationsservrarna varpå portalservern kan presentera hämtad data för användaren och kommunicera med denne när så behövs.

Portaler och tunnlar liknar varandra till stor del, speciellt gällande säkerhets-aspekter, då båda skyddar kommunikation till och från användarenheten samt att båda kan autentisera och hantera åtkomstkontroll. Det finns dock en viktig skillnad mellan dessa två: för tunnlar finns applikationsklientmjukvaran och data lokalt i användarenheten medan det för portaler generellt finns i portalservern. Portaler kan på så sätt göra hantering och kontroll av fjärranslutning lättare för en organisation eftersom de ger en mer centraliserad arkitektur.

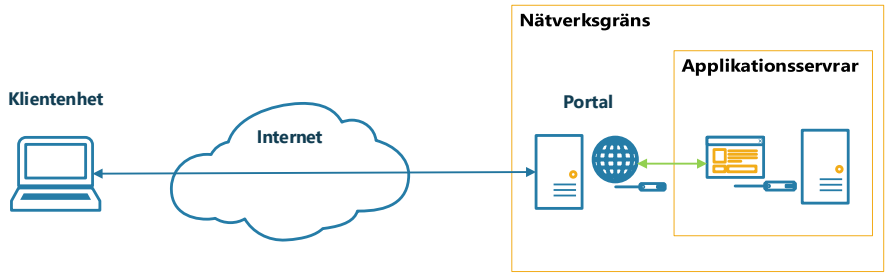
Det finns primärt tre vanligen använda typer av portaler: (1) *Webbportaler*, (2) *Virtual Desktop Infrastructure* (VDI) och (3) *Terminal Server*. Via webb-portaler, som illustreras i Figur 4, ges användare tillgång till flera olika webbaserade applikationer från en och samma webbsida genom en SSL/TLS-baserad VPN-tunnel. Med VDI kan användare fjärransluta till personliga virtuella skrivbord. Terminal Server liknar VDI i det att båda skapar virtuella skrivbord. Terminal server skapar dock standardiserade virtuella skrivbord snarare än personliga. När en användare är klar med sin virtuella session raderas denna av systemet så att nästa användare får tillgång till en oanvänd virtuell session. Denna metod kräver även att användaren installerar speciell mjukvara eller använder ett webbaserat gränssnitt, ofta med specifik tillhörande mjukvara från organisationen. Dessa virtuella metoder bidrar till en högre informations-säkerhet i och med att alla data hanteras i den virtuella maskinen och raderas när

[2] *Secure Sockets Layer* / *Transport Layer Security* – Tekniken är fortfarande känd som SSL men i praktiken är det oftast TLS som används för kryptering eftersom det erhåller en högre grad av säkerhet.

[3] Internet Protocol Security.

[4] Secure Shell

sessionen avslutas. Andra typer av portaler kan också konfigureras med en VDI-lösning för att förbjuda dataextraktion från den virtuella maskinen.



Figur 4 Översiktlig webbportallösning.

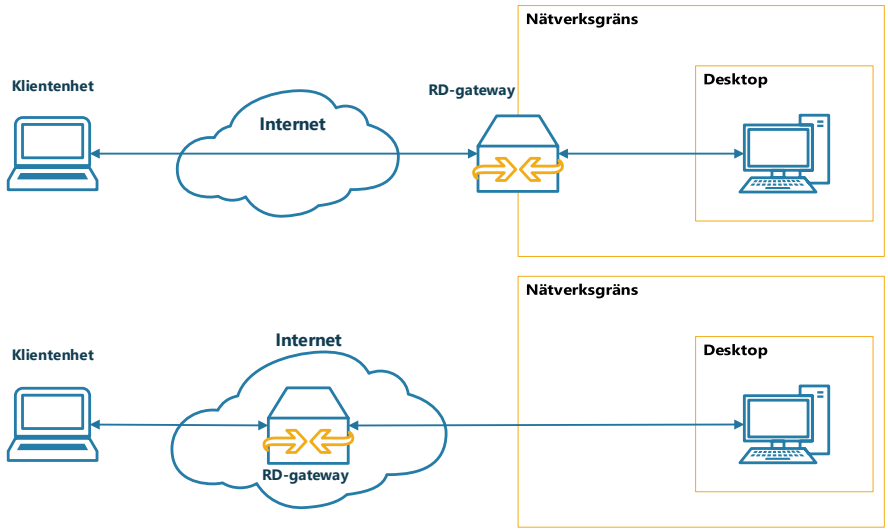
3.3 Fjärråtkomst till skrivbord

Fjärråtkomst till skrivbord eller *Remote Desktop* är ett sätt att fjärransluta till specifika enheter i ett nätverk. Den mest kända implementationen av detta är Microsofts *Remote Desktop Protocol* (RDP). RDP och fjärråtkomst till skrivbord skiljer sig från liknande implementationer, exempelvis VDI och Terminal Server, i det att RDP och andra applikationer för fjärråtkomst till skrivbord ansluter till verkliga datorer, servrar och instanser istället för virtuella versioner. Det finns två primära metoder för fjärråtkomst till skrivbord, direkt och indirekt. En direkt anslutning uppnås genom att en fjärrenhet direkt ansluter till en PC i en organisations interna nätverk medan en indirekt anslutning innebär att kommunikationen går genom en mellanliggande server, Figur 5 visar en övergripande lösning för båda metoderna . Direkt anslutning är i många fall inte möjlig att utföra från ett externt nätverk på grund av att organisationens brandväggar, genom *nätverksadressöversättning* (NAT), inte tillåter en sådan anslutning. För indirekt anslutning ansluter en fjärrenhet via en server[5] som antingen ligger inom organisationens nätverksgräns eller hos en betrodd tredje part.

En mellanliggande server via tredje part är ett objekt av speciellt skyddsvärde för organisationen som dessutom ligger utanför organisationens direkta kontroll. Om en organisation vill använda en sådan lösning är det först viktigt att utförligt utvärdera den erhållna säkerheten av tredjepartsorganisationen som helhet och servertjänsten i detalj. Organisationen bör även utföra en hotanalys kopplat till tredjepartsorganisationen och den tjänst som erbjuds. Resultatet av denna analys

[5] Ibland benämnd som *Remote Desktop Gateway* eller *RD-gateway*.

bör sedan användas som grund för införande av exempelvis kompenserande säkerhetskontroller eller nätverkssegmentering i syfte att mildra potentiella hot som skulle kunna påverka den egna organisationen (Souppaya & Scarfone 2016; FRA 2017).



Figur 5 Översiktlig RD-lösning. Indirekt anslutning via intern gateway och extern gateway.

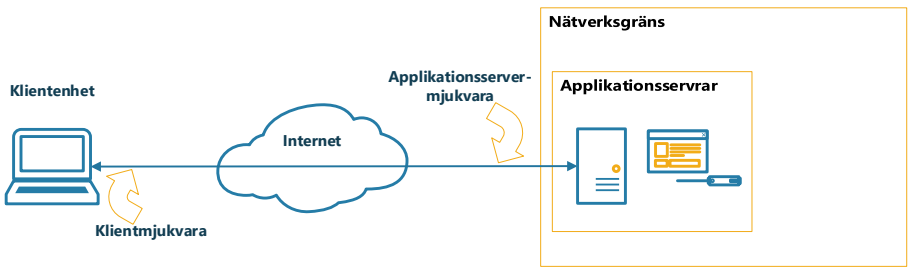
Fjärråtkomstmjukvaran upprätthåller konfidentialitet och riktighet hos kommunikationen, samt autentiserar användare. Denna involverar nyttjandet av *end-to-end*-kryptering, vilket för externa och osäkra nätverk är eftersträvansvärt, men för interna nätverk inte är önskat eftersom innehållet i kommunikationen då döljs från säkerhetsfunktionerna vid nätverksgränsen. Vidare innebär den decentraliserade egenskapen för fjärråtkomst till skrivbord ett säkerhetsmässigt problem eftersom organisationen, istället för att säkra en eller ett fåtal servrar, måste säkra varje enskild enhet som kan nås via fjärranslutning. Den erhållna säkerhetsnivån för varje enhet måste vara av nästan samma grad som för fjärr-anslutningsservrar, vilket kan resultera i höga kostnader för organisationen både tids- och resursmässigt.

Generellt bör externa fjärranslutningar till skrivbord undvikas utom där det är absolut nödvändigt då de andra metoder som beskrivs i denna rapport erbjuder en högre grad av säkerhet. Det är dock vanligt att fjärranslutningar till skrivbord används mellan två enheter i organisationens interna nätverk. I dessa fall är

säkerhetskraven inte lika rigorösa[6] eftersom ingen trafik färdas externt från nätverket, istället är autentisering och auktorisering av användare de två viktigaste aspekterna.

3.4 Direkt applikationstillgång

Fjärranslutning kräver inte alltid extra och specifik mjukvara på klientenheten. Vissa applikationer kan nås direkt via en webbläsare där applikationen själv står för säkerheten i kommunikationen. Det vanligaste exemplet på en sådan applikation är webbmail, där användaren via en webbläsare ansluter till en server som kör en webbmailapplikation. Servern kommunicerar med HTTP över TLS (HTTPS) för att skydda kommunikationen och autentiserar användaren innan tillgång till användarens epost medges. Figur 6 visar en övergripande lösning för direkt applikationstillgång. Denna typ av fjärranslutning bör endast användas om applikationsservrarna är belägna precis innanför organisationens nätverksgräns i en DMZ. Vidare, bör direkt applikationstillgång endast för applikationer med relativt lågt informationssäkerhetsvärde.



Figur 6 Översiktlig lösning för direkt applikationstillgång.

[6] Såvida inte dessa enheter kan nås via extern fjärranslutning.

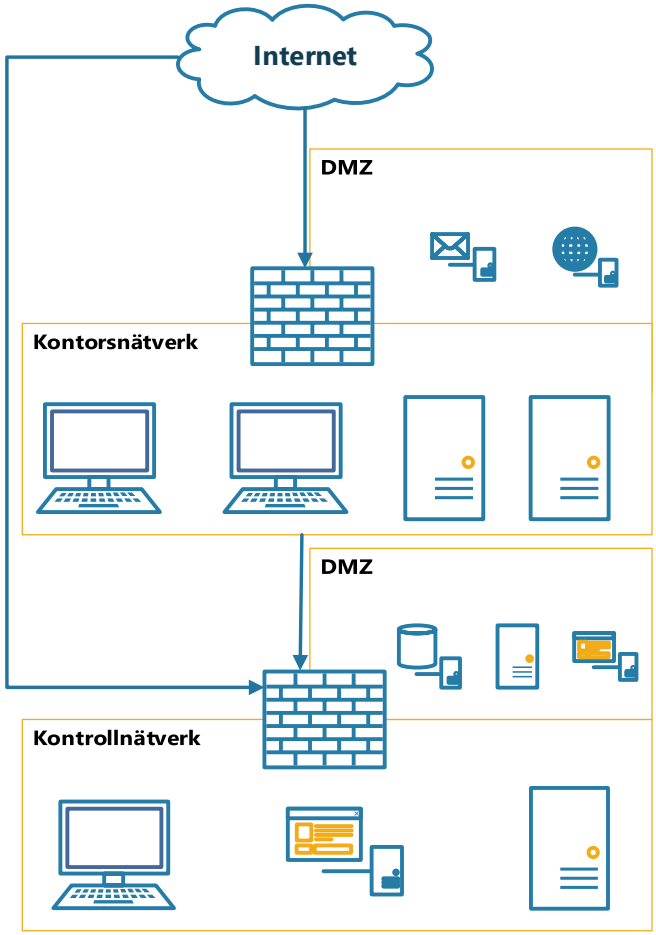
4. Säkerhetsanalys av fjärranslutningsscenarier

I detta kapitel beskrivs och diskuteras olika användningsscenarier för fjärranslutningstekniker. Kapitlet delas in i sex avsnitt, där de tre inledande avsnitten 4.1–4.3 beskriver generella aspekter och egenskaper som gäller för alla scenarier. Kapitlets resterande tre avsnitt 4.4–4.6 beskriver studiens olika scenarier. Dessa avsnitt inleds med en beskrivning av det aktuella scenariots kontext, följt av oönskade händelser, hot och lösningsförslag. Lösningsförslagen beskriver både administrativa och tekniska åtgärder för att ge en heltäckande informationssäkerhetsbild (Swedish Standards Institute (SIS) 2015). Varje scenario avslutas med en sammanfattande diskussion kring lösningsförslagen och eventuella genomgående problem i scenariot.

4.1 Generell nätverksstruktur

Alla scenarier innefattar tänkta organisationer som använder industriella informations- och styrsystem. Den grundläggande nätverksarkitekturen ser likadan ut för alla scenarier. Detta görs då fokus för denna studie ligger på problem och möjligheter relaterat till fjärranslutningar snarare än nätverksarkitektur. Olika nätverksarkitekturer för olika scenarier riskerar således att skifta fokus från fjärranslutningskommunikationen eller snedvrida de slutsatser och rekommendationer som beskrivs för lösningsförslagen.

Arkitekturen som illustreras i Figur 7 innehåller två interna nätverk – *kontorsnätverket* och *kontrollnätverket*. Mellan dessa två nätverk finns en DMZ med en brandvägg innehållande en eller flera applikationsservrar. Detta innebär att nätverken är logiskt separerade. En DMZ finns även belägen i anslutning till kontorsnätverkets utsida, denna innehåller en brandvägg samt mailserver och webbservrar.



Figur 7 Övergripande nätverksstruktur.

4.2 Generella oönskade händelser

Följande avsnitt beskriver de oönskade händelser som är återkommande i alla studiens scenarier.

4.2.1 Oplanerat driftstopp (OH:1)

Ett oplanerat driftstopp i produktion eller distribution kan i första hand innebära att leveranser av den produkt som organisationen framställer försenas eller uteblir för de delar av samhället som organisationen levererar till. I förlängningen innebär detta även en betydande förlust av inkomst för

organisationen som dessutom kan bli ersättningsskyldiga för försenade eller uteblivna leveranser.

4.2.2 Oplanerade förändringar i systemet (OH:2)

Oplanerade förändringar i systemets komponenter kan exempelvis innebära att systemet inte längre fungerar på ett korrekt sätt eller att systemet exponeras för tredje part. I förlängningen kan dessa förändringar leda till den oönskade händelsen av ett oplanerat driftstopp (OH:1).

4.2.3 Informationsläckage (OH:3)

Konsekvenserna av ett informationsläckage varierar beroende på vilken information som röjs. I de fall där det inte går att fastslå vilken information som röjts är potentialen för konsekvenser som värst eftersom organisationen i fråga inte vet vilka motmedel som bör appliceras för att mildra konsekvenserna av läckaget.

Konsekvenser av ett informationsläckage kan exempelvis innebära ett röjande av företagshemligheter, nätverkskartor eller användarkonton och lösenord.

4.3 Generella säkerhetspolicyer

Följande avsnitt beskriver de policyer som är återkommande i alla studiens scenarier.

4.3.1 Autentisering

Autentisering kräver en generell säkerhetspolicy som bör definieras för alla typer av kommunikation inom en organisation. Specifikt definierar denna policy att all fjärranslutningsrelaterad kommunikation ska innehålla flerfaktor-autentiseringsfunktionalitet. Ingen fjärranslutning får genomföras med autentisering som endast baseras på en faktor, exempelvis ett lösenord.

4.3.2 Kryptering av kommunikation

All kommunikation som färdas utanför en organisations interna nätverk ska krypteras. Den eller de specifika algoritmer som bör användas för detta nämns inte här utöver att de bör baseras på vedertagna och rekommenderade standard-algoritmer. Egenutvecklade eller proprietära algoritmer ska i regel undvikas.

4.3.3 Åtkomstkontroll

Fjärransluten kommunikation får, oavsett användargrupp, inte ha rättigheter som om den kommunicerande parten fysiskt befann sig i organisationens interna nätverk. I övrigt baseras åtkomstkontroll på organisationens etablerade användarkategorier. Principen om minsta möjliga rättigheter bör appliceras och strikt följas (Saltzer & Schroeder 1975).

4.4 Scenario 1: Fjärranslutning från ett supportcenter utomlands

Detta scenario innefattar ett elkraftbolag som driver en vattendamm utanför Luleå. Elkraftbolaget innehar ett antal system från olika leverantörer, däribland ett system från en utländsk leverantör vars supportcenter också är beläget i utlandet. Företaget har i detta fall fått problem med just detta system och kontaktar därför supportcentret. Supportcentret behöver tillgång till systemet via fjärranslutning och har genom denna möjlighet att direkt påverka det supporterade systemet. Supportcentret kan dock inte själva initiera fjärranslutningen. Kontakt om support måste istället initieras via mejl eller telefon av elkraftbolaget som därefter aktivt måste släppa in fjärranslutningen från supportcentret.

Den primära resursen i detta scenario är enheter och mjukvara i organisationens kontrollnätverk.

4.4.1 Oönskade händelser

De oönskade händelser som relaterar till den resurs som scenariot innefattar beskrivs i detta avsnitt.

Oplanerat driftstopp (1OH:1)

Se avsnitt 4.2.1.

Oplanerade förändringar i systemet (1OH:2)

Se avsnitt 4.2.2.

Informationsläckage (1OH:3)

Se avsnitt 4.2.3.

Störningar (1OH:4)

Störningar i systemet kan uppstå från en rad olika typer av händelser, exempelvis kan en felkonfigurering under ett supportärende resultera i att andra

system påverkas negativt av det aktuella systemet. En störning som inte uppmärksammas eller åtgärdas kan resultera i ett oplanerat driftstopp (1OH:1).

4.4.2 Hot

Följande avsnitt beskriver hot relaterat till den för scenariot beskrivna resursen som kan leda till de oönskade händelserna i föregående avsnitt.

Hot 1: Informationssäkerhet hos supportcentret

För att supportcentret effektivt och korrekt ska kunna utföra support på sin produkt krävs inte bara tillgång till produkten utan även att supportcentret innehar kunskap om hur det system som produkten är en del av är uppbyggt. Detta för att inte riskera att supportens handlingar påverkar övriga delar av systemet negativt. Denna kunskap måste lagras i någon form hos supportcentret, vilket innebär en problematik för elkraftbolaget eftersom att skyddsvärd intern systeminformation exponeras och sprids till en extern part (1OH:3).

Hot 2: Felaktig uppdatering

Uppdateringar som involverar förändringar på den supporterade produkten kan medföra att produkten inte längre fungerar eller kommunicerar korrekt i förhållande till andra enheter i systemet (1OH:2; 1OH:4). Detta kan i värsta fall resultera i ett oplanerat driftstopp (1OH:1).

Hot 3: Skadlig kod

Ett problem relaterat till föregående hot är att uppdateringar oavsiktligt kan innehålla skadlig kod. Skadlig kod kan i sin tur: orsaka oönskade förändringar i systemet (1:OH2), läcka skyddsvärd information (1:OH3), orsaka störningar i systemets funktion (1:OH4) och kan i värsta fall leda till ett oplanerat driftstopp (1:OH1).

Hot 3: Störningsangrepp (DoS) mot leverantör

Störningsangrepp mot leverantören har potential att begränsa eller helt motverka leverantörens möjlighet att tillhandahålla support. Om elkraftbolaget behöver support under pågående störningsangrepp eller i direkt anslutning till ett sådant, kan detta få konsekvenser för elkraftbolaget. Det kan exempelvis vara som så att problemen med den supporterade produkten är så allvarliga att produktionen inte kan köra på full kapacitet på ett korrekt sätt (1:OH4) eller i värsta fall inte alls (1OH:1). Detta leder i sin tur till betydande ekonomiska konsekvenser för elkraftbolaget i form av förlorade intäkter, men kan även resultera i betydande konsekvenser för de kunder och delar av samhället som berörs av det potentiella elavbrottet.

Hot 4: Störningsangrepp (DoS) mot elkraftbolaget

Störningsangrepp mot elkraftbolagets internetanslutna resurser kan i regel inte resultera i att produktionssystemet måste stängas ner (1OH:1) såvida den supporterade produkten inte för tillfället behöver support eller om något del-system eller komponent av produktionssystemet av någon anledning direkt kan adresseras från internet. I dessa fall har störningsangrepp potential att resultera i nedsatt funktionalitet (1OH:4) i produktionen eller att hela systemet måste stängas ned (1OH:1).

Hot 5: Icke-verifierad kommunikation

Det är alltid viktigt att säkerställa identiteten på vem som försöker ansluta till systemen och att den som ansluter faktiskt är den som denne utger sig för att vara. Elkraftbolaget måste ha möjlighet att verifiera kontakten med support-centret oavsett om denna kommunikation sker via mail, telefon eller annat kommunikationsmedel. På samma sätt är det även viktigt för supportcentret att verifiera att det verkligen är elkraftbolaget som ringer och inte någon annan. Konsekvenserna av en bristande autentisering av parter kan i värsta fall leda till att en antagonist behandlas som en betrodd användare (*Man-in-the-Middle*) i interna system från vilket denne sedan kan stjäla information från systemet (1OH:3), utföra störningsangrepp mot systemet (1OH:4), förändra information eller inställningar i systemet (1OH:2) eller stänga ner systemet (1OH:1).

4.4.3 Säkerhetsåtgärder och lösningsförslag

Följande avsnitt delas in i två kategorier av säkerhetsåtgärder där den första beskriver övergripande administrativ funktionalitet i form av säkerhetspolicyer. Den andra kategorin beskriver hur fjärranslutningsteknikerna från kapitel 3 kan appliceras i detta scenario.

Policy

Nedan beskrivs de säkerhetspolicyer som är relevanta för detta scenario och dess primära resurs.

Policy 1: Autentisering

Se avsnitt 4.3.1.

Policy 2: Kryptering av kommunikation

Se avsnitt 4.3.2.

Policy 3: Åtkomstkontroll

Se avsnitt 4.3.3.

Teknik

Nedan beskrivs hur fjärranslutningsteknikerna från kapitel 3 kan appliceras i detta scenario samt beskrivs kompletterande mekanismer eller beaktanden som krävs för en säker implementation av varje teknik.

Teknisk lösning 1: Tunnlar

Tunnlar i form av VPN kan användas i detta scenario för att skapa en säker kommunikationskanal mellan supportcenter och elkraftbolaget. Själva tunneln och den kommunikation som utbyts däri kan betraktas som säker eftersom allt i tunneln krypteras. Istället är det ändpunkterna som är de potentiellt sårbara punkterna för detta teknikalternativ.

För att undvika att en antagonist fångar upp inloggningsuppgifter till VPN på klientenheten och själv nyttjar anslutningen är det viktigt att flerfaktor-autentiseringsmekanismer används i VPN-lösningen. Flerfaktorautentisering bör även appliceras på de lokala enheter och användarkonton som används av supportcentret.

Vidare bör VPN-lösningen konfigureras så att information och data inte hanteras lokalt på den anslutande enheten, samt att nedladdningsmöjligheter begränsas eller stängs av.

För elkraftbolaget är det viktigt att den krypterade tunneln termineras vid organisationens nätverksgräns, exempelvis i DMZ. Det är sällan önskvärt att låta krypterad kommunikation flöda i de interna nätverken, oavsett hur mycket tilltro som sätts till den part som utför kommunikationen bör elkraftbolaget ha möjlighet att övervaka all kommunikation i de interna nätverken. Detta är inte bara viktigt i syfte att se till att inget skadligt åsamkas systemet utan också i syfte att få en spårbarhet över ändringar och händelser i nätverket och systemet.

Genom den beskrivna lösningen kan hot 1, 2 och 5 motverkas och i förlängningen de oönskade händelserna 1, 2 och 3. Störningar och störningsangrepp går inte att motverka via en VPN-lösning.

Teknisk lösning 2: Applikationsportaler

Applikationsportaler liknar till stor del det föregående lösningsförslaget. En skillnad är dock att portaler generellt håller data och mjukvara i portalservern istället för på användarenheten. Detta går dock även att konfigurera för en VPN, men den stora skillnaden mellan detta och föregående lösningsförslag är i stället att VPN-lösningen kräver en speciell applikationsmjukvara, vilket för applikationsportaler inte är nödvändigt då gränssnittet till portalen kan visas via en webbläsare.

En användare ansluter till organisationens webbportal via en webbläsare som krypterar kommunikationen med HTTPS. Väl ansluten till portalen måste användare autentisera sig för att få tillgång till den information och funktionalitet som portalen erbjuder. Denna autentisering bör ske med ett minimum av personligt användarnamn och lösenord, men ska utökas till att inkludera flerfaktorautentisering. Vidare kan Windows *Account Lockout Policy* (ALP) eller en dylik mekanism implementeras för att minska risken för att en antagonist använder uttömmande sökning (eng. *brute force*) för att pröva inloggningsuppgifter. Om portalen endast är ämnad för supportärenden från en eller flera leverantörer är det, trots ALP, inte önskvärt att portalen är öppen hela tiden. I och med att supportärenden endast ska initieras av elkraftbolaget vill man inte ge tillgång till portalen när support inte behövs, oavsett om det är till betrodda leverantörsanvändare eller ej. Därför bör portalen kräva ett manuellt godkännande av personal på elkraftbolaget. Detta kan exempelvis innebära att personalen notifieras när någon försöker ansluta till portalen och själva kan godkänna eller neka anslutningen oavsett om rätt inloggningsuppgifter har matats in.

Genom den beskrivna lösningen kan hot 1, 2 och 5 motverkas och i förlängningen de oönskade händelserna 1, 2 och 3. Störningar och störningsangrepp går inte att motverka via en applikationsportallösning.

Teknisk lösning 3: Fjärråtkomst till skrivbord

Fjärråtkomst till skrivbordslösningar bör generellt undvikas för extern kommunikation, vilket delvis beror på att de andra tekniker som presenteras i denna studie innehar en högre grad av inneboende säkerhet. Det är dock möjligt att applicera en fjärråtkomstlösning för dessa ändamål. I ett sådant fall är det viktigt att den mellanliggande server som nyttjas, eftersom direkta anslutningar inte är möjliga, inte beläggs hos en tredje part utan istället placeras i direkt anslutning till organisationens nätverksgräns i en DMZ. Vidare bör fjärråtkomst till skrivbord konfigureras så att flerfaktorautentisering krävs av användaren, att filöverföring blockeras samt att en ALP är aktiverad. Fjärråtkomst till skrivbord kan med fördel även kombineras med tunnlar för att addera ett lager av säkerhet gällande både autentisering och konfidentialitet, trots att kommunikationen ofta är krypterad i vanliga tekniker som RDP.

Genom den beskrivna lösningen kan hot 1, 2 och 5 motverkas och i förlängningen de oönskade händelserna 1, 2 och 3. Störningar och störningsangrepp går inte att lösa via fjärråtkomst till skrivbord.

Teknisk lösning 4: Direkt applikationstillgång

Direkt applikationstillgång är inte ett applicerbart alternativ för detta scenario då lösningen bedöms bli väldigt komplicerad och svår att kontrollera säkerhetsmässigt för organisationen i fråga. Som bekant lämpar sig dessa lösningar endast för applikationer med relativt lågt skyddsvärde, vilket sällan passar in på enheter i ett kontrollnätverk. Om lösningen baseras på proprietär mjukvara som tillhandahålls och utvecklas av leverantören bör mjukvaran genomgå en rigorös säkerhetsgranskning för att säkerställa att mjukvaran inte innehåller några uppenbara sårbarheter eller problem.

Skulle denna lösning användas är det viktigt att organisationen kräver kryptering, men samtidigt inte tillåter att kommunikationen krypteras end-to-end eftersom detta döljer innehållet i kommunikationen från övervakning och från nätverkets interna säkerhetsfunktioner. Istället bör krypteringen termineras vid organisationens nätverksgräns, exempelvis i en gateway-server placerad i någon av organisationens DMZ.

Lösningen bör även inkludera flerfaktorautentisering samt tillse att lösenord och andra autentiseringsvärden aldrig skickas eller lagras i klartext.

Genom den beskrivna lösningen kan hot 1, 2 och 5 motverkas och i förlängningen de oönskade händelserna 1, 2 och 3. Störningar och störningsangrepp går inte att lösa via direkt applikationstillgång.

4.4.4 Sammanfattning

Inget av lösningsalternativen förhindrar ett informationsläckage av den systeminformation som supportcentret innehar. Utöver kravställning i avtalsform är det svårt för organisationen att kontrollera hur systeminformationen hanteras hos supportcentret. Organisationen bör därför se den informationen som röjd och implementera säkerhetsåtgärder utifrån det antagandet.

Inget lösningsförslag förhindrar heller påverkan från störningar varken mot supportcentret eller mot den egna organisationen. Organisationen bör även implementera säkerhetsåtgärder för att minimera konsekvenserna av detta hot, exempelvis genom att ha en incidentberedskap efter en uppdatering. Det är dock för organisationen svårt att motverka störningspåverkan mot supportcentret eftersom organisationen inte har möjlighet att direkt påverka eller kontrollera vilka säkerhetsfunktioner som supportcentret innehar.

4.5 Scenario 2: Fjärranslutning från en konsult som tillfälligt arbetar hemifrån

Göran arbetar som konsult på ett dricksvattenverk och behöver jobba hemifrån över en helg för att hinna klart med en rapport angående produktionen hos dricksvattenverket. För att utföra det arbetet behöver Göran tillgång till data och analysverktyg från både kontors- och kontrollnätverket hos dricksvattenverket. För att utföra arbetet hemifrån använder Göran den dator som han har blivit tilldelad av konsultföretaget där han är anställd.

Den primära resursen för detta scenario är organisationens interna mjukvara och data.

4.5.1 Oönskade händelser

De oönskade händelser som relaterar till den resurs som scenariot innefattar beskrivs i detta avsnitt.

Oönskad händelse 1: Oplanerat driftstopp (2OH:1)

Se avsnitt 4.2.1.

Oönskad händelse 2: Oplanerade förändringar i systemet (2OH:2)

Se avsnitt 4.2.2.

Oönskad händelse 3: Informationsläckage (2OH:3)

Se avsnitt 4.2.3.

Oönskad händelse 4: Informationsförlust (2OH:4)

Informationsförlust skiljer sig från informationsläckage genom att informationen går förlorad för organisationen. En förlust kan innebära ett läckage och vice versa, men det viktiga vid förlust är att informationen inte längre finns tillgänglig för organisationen.

Oönskad händelse 5: Oönskad påverkan på systemet (2OH:5)

Oönskad påverkan inkluderar både avsiktlig och oavsiktlig påverkan av användaren som resulterar i en försämrad förmåga för systemet att utföra sina uppgifter eller ett oplanerat driftstopp (2OH:1).

Oönskad händelse 6: Icke-auktoriserad användare (2OH:6)

Icke-auktoriserad innebär i sammanhanget en individ annan än Göran som använder Görans inloggningsuppgifter för att nyttja en legitim fjärranslutning. I och med att Göran har vissa rättigheter i de interna systemen via fjärranslutning innebär detta att den icke-auktoriserade användaren kan agera med samma

rättigheter och kan via dessa försöka att påverka systemet (2OH:5), orsaka driftstopp (2OH:1), samt stjäla (2OH:3) eller förstöra information (2OH:4).

4.5.2 Hot

Följande avsnitt beskriver hot relaterat till den beskrivna resursen för scenariot som kan leda till de oönskade händelserna i föregående avsnitt.

Hot 1: Avsiktlig och oavsiktlig destruktion av information

Destruktion av information (2OH:4) innebär samma konsekvenser oavsett om händelsen som ledde fram till destruktionen var avsiktlig eller inte. Konsekvenserna varierar istället beroende på vilken typ av information som destrueras och om denna information även finns lagrad på en annan plats eller inte. Destruktionens resultat kan bland annat leda till att systemet inte längre kan fungera på ett korrekt sätt (2OH:5) vilket kan innebära ett oplanerat driftstopp (2OH:1).

Hot 2: Uppladdning av skadlig kod

Om inte användandet av den dator som fjärransluter till interna system regleras kan denna komma att innehålla skadlig kod. Den skadliga koden kan sedan laddas upp via fjärranslutning in i de interna systemen utan användarens vetskap.

Hot 3: Obehörigt användande av uppkoppling

Reglering (exempelvis genom policyer och inställningar i datorn) av användandet av den dator som fjärransluter är viktigt. Om exempelvis enheten konfigureras att fjärransluta automatiskt när enheten startas kan en obehörig användare med tillgång till datorn också få tillgång till de interna systemen. En antagonist som lyckas ta kontroll över datorn kan även nyttja fjärranslutningen utan hinder och utan att detta nödvändigtvis uppmärksammas.

Hot 4: Stöld av information och hårdvara

Ett privat och oförsiktigt nyttjande av datorn kan leda till att datorn utsätts för angrepp. Om datorn innehåller kritisk information för verksamheten kan denna information stjälas utan att angriparen behöver ta sig in i organisationens system eller stjäla datorn fysiskt. En användare som har möjlighet att fjärrstyra datorn kan stjäla information från det interna nätverket när datorn är fjärransluten. En förlust av hårdvara genom att denna stjäls eller glöms är relativt vanligt förekommande och när en sådan förlust sker kan även informationen som finns lagrad på enheten stjälas.

Hot 5: Avlyssning

Det är vanligt att använda trådlösa uppkopplingar till publika wifi-nätverk för mobila användare. På publika nätverk finns flera användare och datatrafiken är ofta oskyddad, vilket medför att fjärranslutningen mot de interna systemen måste skydda datakommunikationen mellan klientenheten och de interna systemen. På så sätt minimeras risken för informationsläckage, informationsförlust eller kartläggning av organisationens nätverk.

4.5.3 Säkerhetsåtgärder och lösningsförslag

Följande avsnitt delas in i två kategorier av säkerhetsåtgärder där den första beskriver övergripande administrativ funktionalitet i form av säkerhetspolicyer. Den andra kategorin beskriver hur fjärranslutningsteknikerna från kapitel 3 kan appliceras i detta scenario.

Policy

Nedan beskrivs de säkerhetspolicyer som är relevanta för detta scenario och dess primära resurs.

Policy 1: Autentisering

Se avsnitt 4.3.1.

Policy 2: Kryptering av kommunikation

Se avsnitt 4.3.2.

Policy 3: Åtkomstkontroll

Se avsnitt 4.3.3.

Policy 4: Tilldelad eller extern enhet

Denna policy begränsar användares rättigheter i de interna systemen för nyttjande genom fjärranslutning. Detta är särskilt viktigt för externa enheter som inte tillhör dricksvattenorganisationen.

Konsulters användande av utrustning som inte tillhör eller kontrolleras av dricksvattenorganisationen innebär generellt en säkerhetsrisk eftersom de krav och regler som gäller för denna utrustning kan skilja sig från organisationens interna regler. Om dessa enheter sedan tillåts fjärransluta med samma behörighet som intern utrustning innebär det en risk för dricksvattenorganisationen. I förlängningen kan det innebära att korrupt tredjepartsmjukvara i form av skadlig kod angriper, och sprider sig till, de interna nätverken via Görans fjärranslutning. Konsekvenserna av en sådan infektion kan innebära att hela

system hos dricksvattenverket stängs ner eller slutar fungera, vilket i sin tur innebär en ekonomisk förlust för organisationen.

Teknik

Nedan beskrivs hur fjärranslutningsteknikerna från kapitel 3 kan appliceras i detta scenario samt beskrivs kompletterande mekanismer eller beaktanden som krävs för en säker implementation av varje teknik.

Teknisk lösning 1: Tunnlar

En tunnel i form av en VPN-anslutning kan användas för att möjliggöra fjärr-anslutning mellan Görans dator och dricksvattenverket. Som föregående scenario beskriver kan kommunikationen i denna tunnel betraktas som säker, istället är det ändpunkternas säkerhet som måste uppmärksammas och hanteras.

Risken för obehörigt användande av Görans dator och fjärranslutningen kan hanteras genom att använda flerfaktorautentisering som är tvingande att mata in innan varje session påbörjas. Vidare bör sessioner termineras efter en viss period av inaktivitet från användaren (Göran). Flerfaktorautentisering minskar även risken för att någon annan kan använda Görans inloggningsuppgifter.

I syfte att minimera risken för informationsstöld bör VPN-lösningen konfigureras till att inte tillåta att data hämtas och lagras lokalt på klientenheten. Istället bör alla data och information hanteras i organisationens VPN-gateway. Vidare bör organisationens åtkomstpolicy begränsa Görans rättigheter så att systemets information inte kan ändras eller raderas.

Genom den beskrivna lösningen kan hot 1, 2, 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4, 5 och 6. Stöld eller förlust av hårdvara som inte tillhör organisationen i fråga kan inte motverkas genom detta teknikalternativ.

Teknisk lösning 2: Applikationsportaler

En applikationsportal som Göran, andra konsulter och medarbetare kan använda för fjärranslutning är ett rimligt alternativ för detta scenario. Lösningen bör inkludera flerfaktorautentisering och personliga användarkonton.

Eftersom det finns en begränsad tilltro till Görans dator, då denna inte är intern utrustning, bör uppladdningsförmåga via fjärranslutningen begränsas i syfte att minimera risken för att skadlig kod laddas in i de interna systemen.

Applikationsportalen bör inte heller tillåta nedladdning av verksamhetskritisk information. Det kan även vara ett alternativ att helt neka åtkomst till viss information via fjärranslutning.

Denna lösning skulle kunna nyttja VDI för att ge Göran tillgång till de analysverktyg han behöver utan att ge honom möjlighet att direkt påverka enheter eller information i kontrollnätverket.

Genom den beskrivna lösningen kan hot 1, 2 och 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4, 5 och 6. Stöld eller förlust av hårdvara som inte tillhör organisationen i fråga kan inte motverkas genom detta teknikalternativ.

Teknisk lösning 3: Fjärråtkomst till skrivbord

Som bekant bör externa fjärranslutningar till skrivbord undvikas, men de är ändå möjliga att använda om så önskas. I ett sådant fall, eftersom direkta anslutningar inte är möjliga, bör den mellanliggande servern som används placeras i en av organisationens DMZ.

Fjärråtkomst till skrivbord bör implementeras med flerfaktorautentisering, blockera filöverföring samt använda en ALP eller dylik mekanism. Fjärråtkomst till skrivbord kan för externa anslutningar, som i detta scenario, med fördel kombineras med tunnlar för att addera ett lager av säkerhet gällande både autentisering och konfidentialitet, trots att kommunikationen ofta är krypterad i vanligt använda tekniker som RDP.

Det är även viktigt att policyn för åtkomstkontroll och användarkategorier kompletteras eller utökas för att även specificera att majoriteten av användarkategorier (undantaget vissa administratörer) endast har rättighet att ansluta till ett fåtal specifika datorer och inte till generella klasser av enheter.

Genom den beskrivna lösningen kan hot 1, 2 och 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4, 5 och 6. Stöld eller förlust av hårdvara som inte tillhör organisationen i fråga kan inte motverkas genom detta teknikalternativ.

Teknisk lösning 4: Direkt applikationstillgång

Om den information som Göran vill använda har ett relativt lågt skyddsvärde för organisationen är direkt applikationstillgång ett smidigt alternativ att tillgå. Tekniken bör dock inte användas för information av högt skyddsvärde.

Infrastrukturen för alternativet bör inkludera att användaren ansluter till en gateway som placeras i en av organisationens DMZ. Informationen och de verktyg som lösningen ämnar ge tillgång till, kan hämtas från andra delar av nätverket och lagras i en databas eller på en server som är ansluten till den gateway som användaren ansluter till. På så sätt kan tillgång till nödvändig information och verktyg ges till användare utan att utsätta det faktiska systemet eller nätverket.

Lösningen bör inkludera flerfaktorautentisering och personliga användarkonton för alla användare. Konfigurationen bör kryptera kommunikationen mellan klientenhet och server, exempelvis genom en tunnel. Lösningen bör inte tillåta filöverföring till eller från applikationen.

Genom den beskrivna lösningen kan hot 1, 2 och 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4, 5 och 6. Stöld eller förlust av hårdvara som inte tillhör organisationen i fråga kan inte motverkas genom detta teknikalternativ.

4.5.4 Sammanfattning

Inget av teknikalternativen kan hindra fysisk stöld av klientenheter. För organisationen blir det istället viktigt att intern värdefull information skyddas på ett effektivt sätt. Ett alternativ är att inte låta någon information extraheras från de interna nätverken via fjärranslutning för att lagras på klientenheter. Ett annat alternativ är att kryptera hårddiskarna på klientenheterna för att förhindra att en antagonist får tillgång till lagrad information, även om denne får fysisk tillgång till enheten. I detta scenario är Göran en extern konsult som inte använder organisationens egna enheter, vilket innebär att alternativet ovan inte är relevant sett från organisationens perspektiv eftersom de inte har kontroll över Görans dator och således inte kan tvinga eller försäkra att tillräcklig kryptering används.

4.6 Scenario 3: Fjärranslutning från underhållspersonal

Berit jobbar som underhållstekniker på ett fjärrvärmeföretag. Företaget har ett antal geografiskt utspridda undercentraler som underhålls av Berit och hennes kollegor. Vissa delar av arbetet kräver att underhållspersonalen närvarar fysiskt vid undercentralerna. Andra delar kräver fjärranslutningsåtkomst till kontrollnätverket och undercentralerna. Således behöver Berit och hennes kollegor en dator med sig i de fordon som används för att ta sig till de olika undercentralerna. Vidare krävs även uppkopplingsmöjligheter från platser där det normalt inte finns någon uppkoppling att tillgå.

Den primära resursen för detta scenario är Berits dator och organisationens fältstationer och fältsystem.

4.6.1 Oönskade händelser

De oönskade händelser som relaterar till den resurs som scenariot innefattar beskrivs i detta avsnitt.

Oönskad händelse 1: Oplanerat driftstopp (3OH:1)

Se avsnitt 4.2.1.

Oönskad händelse 2: Oplanerade förändringar i systemet (3OH:2)

Se avsnitt 4.2.2.

Oönskad händelse 3: Informationsläckage (3OH:3)

Se avsnitt 4.2.3.

Oönskad händelse 4: Informationsförlust (3OH:4)

Informationsförlust skiljer sig från informationsläckage genom att informationen går förlorad för organisationen. En förlust kan innebära ett läckage och vice versa, men det viktiga vid förlust är att informationen inte längre finns tillgänglig för organisationen.

Oönskad händelse 5: Oönskad påverkan på systemet (3OH:5)

Oönskad påverkan inkluderar både avsiktlig och oavsiktlig påverkan av användaren som resulterar i en försämrad förmåga för fältsystemet att utföra sina uppgifter. Exempelvis kan Berit av misstag ändra en inställning för en fältstation som resulterar i att fältstationen inte längre skickar korrekta värden till det centrala kontrollnätverket. Ett exempel på avsiktlig påverkan kan även detta inkludera Berit, som en insider, där hon utför samma ändring och i detta fall är medveten om konsekvenserna på förhand. Ett annat exempel är en icke-auktoriserad användare som använder Berits legitima uppkoppling för att påverka ett fältsystem.

Oönskad händelse 6: Stöld av inloggningsuppgifter (3OH:6)

Icke-auktoriserad innebär i sammanhanget en individ annan än Berit som använder hennes inloggningsuppgifter för att nyttja en legitim fjärranslutning. I och med att Berit har vissa rättigheter i de interna systemen via fjärranslutning innebär detta att den icke-auktoriserade användaren har samma rättigheter och kan via dessa försöka att påverka systemet (3OH:5), stjäla (3OH:3) eller förstöra information (3OH:4) alternativt orsaka ett lokalt oplanerat driftstopp (3OH:1).

4.6.2 Hot

Nedanstående hot är de samma som beskrevs i föregående scenario men listas här i syfte att scenariot ska vara komplett.

Hot 1: Avsiktlig och oavsiktlig destruktion av information

Destruktion av information innebär samma konsekvenser oavsett om händelsen som ledde fram till destruktionen var avsiktlig eller inte. Konsekvenserna

varierar istället beroende på vilken typ av information som destrueras och om denna information finns lagrad på en annan plats eller inte. Destruktionens resultat kan bland annat leda till att systemet inte längre kan fungera på ett korrekt sätt (3OH:5) vilket kan innebära ett oplanerat driftstopp (3OH:1).

Hot 2: Uppladdning av skadlig kod

Om inte användandet av den dator som fjärransluter till interna system regleras, kan denna komma att innehålla skadlig kod. Denna kod kan sedan laddas upp via fjärranslutning i de interna systemen utan användarens vetskap.

Hot 3: Obehörigt användande av uppkoppling

Reglering av användandet av den dator som fjärransluter är viktigt även här. Om exempelvis enheten konfigureras att fjärransluta automatiskt när enheten startas kan en obehörig användare med tillgång till datorn också få tillgång till de interna systemen. En antagonist som lyckas ta kontroll över datorn kan även denne nyttja fjärranslutningen utan hinder och utan att detta nödvändigtvis uppmärksammas.

Hot 4: Stöld av information och hårdvara

Ett privat och oförsiktigt nyttjande av datorn kan leda till att datorn utsätts för ett angrepp. Om datorn innehåller kritisk information för verksamheten kan denna information stjälas utan angriparen behöver ta sig in i organisationens system eller stjäla datorn fysiskt. En användare som har möjlighet att fjärrstyra datorn kan stjäla information från det interna nätverket när datorn är fjärransluten. En förlust av hårdvara genom att denna stjäls eller glöms är relativt vanligt och när en sådan förlust sker finns en risk att information som finns lagrad på enheten stjäls.

Hot 5: Avlyssning

Det är vanligt att använda trådlösa uppkopplingar till publika wifi-nätverk för mobila användare. På dessa nätverk finns flera användare och datatrafiken är ofta oskyddad vilket medför att fjärranslutningen mot de interna systemen måste skydda datakommunikationen mellan klientenheten och de interna systemen. Detta för att minimera risken för informationsläckage, informationsförlust eller kartläggning av organisationens nätverk.

4.6.3 Säkerhetsåtgärder och lösningsförslag

Följande avsnitt delas in i två kategorier av säkerhetsåtgärder där den första beskriver övergripande administrativ funktionalitet i form av säkerhetspolicyer. Den andra kategorin beskriver hur fjärranslutningsteknikerna från kapitel 3 kan appliceras i detta scenario.

Policy

Nedan beskrivs de säkerhetspolicyer som är relevanta för detta scenario och dess primära resurs.

Policy 1: Autentisering

Se avsnitt 4.3.1.

Policy 2: Kryptering av kommunikation

Se avsnitt 4.3.2.

Policy 3: Åtkomstkontroll

Se avsnitt 4.3.3.

Policy 4: Tilldelad eller extern enhet

Till skillnad från Göran i föregående scenario så använder Berit en dator som hon har blivit tilldelad av organisationen. Skillnaden blir således att organisationen kan ha en större tilltro till hårdvaran eftersom det finns möjlighet att i större utsträckning kontrollera den.

Organisationens regler för användning av dessa enheter säger att ingen mjukvara får installeras av användaren, användaren har inte administratörsrättigheter, enheten får endast användas till arbetsrelaterade uppgifter samt att hårddisk-kryptering nyttjas.

Teknik

Nedan beskrivs hur fjärranslutningsteknikerna från kapitel 3 kan appliceras i detta scenario samt beskrivs kompletterande mekanismer eller beaktanden som krävs för en säker implementation av varje teknik.

Teknisk lösning 1: Tunnlar

Tunnlar skyddar som bekant inte endast kommunikationen mellan klientenheten och det mottagande systemet utan hanterar även autentisering och åtkomst-kontroll. Den autentisering som används bör utökas till att innefatta flerfaktor-autentisering, ömsesidig autentisering, samt att alla användare har personliga konton.

Det kan vara relevant att begränsa möjlighet att hämta och lagra information lokalt på de klientenheter som fjärransluter. Exempelvis gäller detta där sådan information inte är nödvändig att ha tillgång till lokalt för att Berit och hennes kollegor ska kunna utföra sina arbetsuppgifter. I annat fall är det viktigt att skydda Berits dator mot skadlig kod, intrångsförsök och avlyssning för att inte riskera att information och användaruppgifter stjäls från datorn eller att VPN-anslutningen tas över av en antagonistisk tredje part.

Genom den beskrivna lösningen kan hot 1,2, 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4 och 6. Stöld eller förlust av hårdvara som tillhör organisationen i fråga kan inte motverkas genom detta teknikalternativ men informationen lagrad på datorns hårddiskar kan skyddas även om datorn stjäls.

Teknisk lösning 2: Applikationsportaler

Applikationsportaler bedöms inte vara ett sannolikt alternativ för detta scenario eftersom en sådan lösning troligtvis skulle bli alldeles för komplext att implementera jämfört med andra teknikalternativ. Det är dock möjligt att implementera en portallösning om användaren i första hand ansluter till en central portalserver i organisationens DMZ. Denna portalserver ansluter i sin tur via en tunnel till den fältstation som användaren vill kommunicera med och agerar mellanhand mellan användaren och fältstationen. Alternativet till detta är att varje fältsystem ges en egen portallösning och gränssnitt, vilket inte är önskvärt eftersom detta ökar organisationens exponering mot internet.

Det kan även för detta alternativ vara relevant att begränsa möjligheten att hämta och lagra information på Berits enhet, beroende på om sådan lagring är nödvändig för Berits arbetsuppgifter eller inte.

Flerfaktorautentisering bör appliceras på portallösningen, i synnerhet om varje fältstation ges ett eget gränssnitt.

Genom den beskrivna lösningen kan hot 1, 2, 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4 och 6. Stöld eller förlust av hårdvara som tillhör organisationen i fråga kan inte motverkas genom detta teknikalternativ men informationen lagrad på datorns hårddiskar kan skyddas även om datorn stjäls.

Teknisk lösning 3: Fjärråtkomst till skrivbord

Precis som för tidigare lösningsförslag för fjärråtkomst till skrivbord måste en mellanliggande server eller gateway placeras i DMZ även i detta scenario. Lösningen bör även nyttja personliga användarkonton och flerfaktor-autentisering, där användarens tillgång att ansluta till enheter begränsas beroende på vilken användargrupp denne tillhör.

Genom den beskrivna lösningen kan hot 1, 2, 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4 och 6. Stöld eller förlust av hårdvara som tillhör organisationen ifråga kan inte motverkas genom detta teknikalternativ, men information lagrad på datorns hårddiskar kan skyddas även om datorn stjäls.

Teknisk lösning 4: Direkt applikationstillgång

För att direkt applikationstillgång ska vara relevant för detta scenario krävs att applikationen centralt kan samla in information från de olika fältstationerna. Användaren ansluter sedan till en central gateway eller server som visar aktuell information för varje fältstation och system. För att ha möjlighet att utföra förändringar i dessa fältstationer krävs att applikationen kan ansluta och kryptera kommunikationen mellan fältstationerna och de centrala servrarna som användaren ansluter emot. Denna kryptering kan exempelvis hanteras genom att kombinera lösningen med VPN-tunnlar.

Lösningen bör utöver krypterad kommunikation även implementera flerfaktor-autentisering och personliga användarkonton för samtliga användare.

Genom den beskrivna lösningen kan hot 1, 2, 5 samt delvis 3 och 4 motverkas och i förlängningen de oönskade händelserna 1, 2, 3, 4 och 6. Stöld eller förlust av hårdvara som tillhör organisationen ifråga kan inte motverkas genom detta teknikalternativ, men information lagrad på datorns hårddiskar kan skyddas även om datorn stjäls.

4.6.4 Sammanfattning

Som i föregående scenario löser inget av teknikalternativen problemet med fysisk stöld av Berits dator. Skyddet av den information som finns på datorn är därför viktig. Till skillnad från föregående scenario är Berit anställd hos organisationen och använder en tilldelad intern dator. Detta innebär att organisationen har större möjlighet att kontrollera hur enheten används och vilka säkerhetsmekanismer som finns på enheten. Hårddiskkryptering är därför möjlig att implementera på Berits och hennes kollegors datorer och på så sätt kan informationen i dessa datorer skyddas även om datorerna skulle stjälas. Det kan dock fortfarande vara relevant att inte tillåta att information från fjärr-anslutningar lagras lokalt på dessa enheter om detta inte är nödvändigt för Berits arbetsuppgifter.

Eftersom Berit och hennes kollegor behöver utföra förändringar och upp-dateringar på systemkomponenter eller fältsystem kan det, oavsett lösning, inte garanteras att någon av dessa förändringar inte resulterar i en oönskad påverkan på systemet (3OH:5).

5. Diskussion

I en modern företagsverksamhet är fjärranslutningskapacitet mer eller mindre ofrånkomligt eftersom det är en viktig del i den dagliga verksamheten på grund av den ökade tillgänglighet och de ekonomiska fördelar som fjärranslutning medger. Organisationer måste således förbereda och implementera en infrastruktur för att hantera fjärranslutningar på ett säkert sätt. Detta är ofta ett väldigt komplext problem att lösa när det finns flera olika kategorier av användare, både interna och externa, som behöver tillgång till fjärranslutnings-kapacitet. Att implementera och hantera funktionalitet för fjärranslutningar blir särskilt svårt i de fall intern kompetens för att utföra detta arbete saknas i organisationen. Om intern kompetens gällande kravställning saknas är det viktigt att organisationen anlitar kravställare från en oberoende tredje part. Vidare finns stöd att tillgå, exempelvis i form av standarder och allmänna principer som bland annat återfinns i NIST (Souppaya & Scarfone 2016) och Imran (2015). Exempel på en sådan princip är att en användare aldrig bör ha tillgång till mer information eller rättigheter i system via fjärranslutning än vad denne har lokalt på arbetsplatsen. Ett annat exempel är att flerfaktorautentisering generellt bör nyttjas i syfte att minska risken för att en antagonist får tillgång till en användares inloggningsuppgifter.

De risker som existerar för fjärranslutningar varierar beroende på skyddsvärdet av den information och de funktioner som kan hanteras via fjärranslutningen. De allra flesta hot och risker som kan tänkas uppstå för en organisation kan motverkas med hjälp av de fyra teknikalternativ som presenterats i denna studie. Det är dock viktigt att inse att dessa tekniker generellt måste kompletteras med annan säkerhetsfunktionalitet för att risker ska kunna minimeras. Ett tydligt exempel på detta är flerfaktorautentisering, som i varje teknikalternativ för alla scenarier används som komplement till den säkerhet som teknikerna erbjuder.[7] En del risker kan inte fullständigt tas bort och i vissa fall går det heller inte att effektivt minimera riskerna för att ett hot realiseras. I dessa fall blir det istället viktigt för organisationen att minska sannolikheten för att en oönskad händelse inträffar. Ett sådant exempel återfinns i studiens tredje scenario där Berit och hennes kollegor behöver rättigheter att utföra förändringar och uppdateringar på fältsystem. Även om vi antar att Berit är väldigt kompetent och noggrann kan det inte garanteras att hon aldrig kommer göra ett misstag i en förändring som resulterar i en negativ effekt på fältsystemet.

[7] I många fall är flerfaktorautentisering (och andra funktioner) inbyggt som en valmöjlighet och kan därför inte sägas ingå i tekniken då det inte behövs för att tekniken ska fungera.

De scenarier som denna studie beskriver syftar till att belysa olika situationer där fjärranslutning används och vad som är viktigt att beakta i varje situation. Huvudsyftet med fjärranslutning är att öka tillgängligheten till information eller funktionalitet som finns i en organisations interna system. Som bekant är det oftast konfidentialitet som ges störst fokus för extern kommunikation, men för industriella informations- och styrsystem är det i regel tillgänglighet som är i fokus. Fjärranslutningen i de scenarier som denna studie beskriver har olika behov av konfidentialitet för information och skydd av tillgänglighet. Vilken av dessa två aspekter som ligger i fokus för scenariot påverkar vilken tekniklösning som lämpar sig bäst. Sammantaget kan dock sägas att tunnel- och portal-lösningar är de mest mångsidiga av teknikerna, men att även dessa i regel måste kompletteras med annan funktionalitet för att utgöra en tillräckligt säker lösning.

Scenariernas relevans kan ifrågasättas eftersom de inte är direkt hämtade eller baserade på verkliga situationer och endast övergripande beskriver situationen ifråga. Detaljrikedomen kan därmed påverka scenariernas realism negativt. Däremot är målet med dessa avsnitt att belysa viktiga frågor och beaktanden och hur dessa kan skilja sig beroende på olika, vanligt förekommande, situationer.

Rekommendationer

Avslutningsvis ges nedan ett antal rekommendationer på aktiviteter som alltid ska föregå ett beslut om implementation av fjärranslutningskapacitet:

- Identifiering av behov av fjärranslutningskapacitet.
- Identifiering av information och funktioner som behöver finnas tillgängliga via fjärranslutning.
- Säkerhetsanalys av behovet för fjärranslutning, information och funktioner.
- Eventuella justeringar och tillägg av relevanta säkerhetspolicyer.

När dessa aktiviteter är genomförda kan kravställning och därefter upphandling av tekniklösning för fjärranslutning påbörjas.

Referenser

Department of Homeland Security (DHS) (2010). *Configuring and Managing Remote Access for Industrial Control Systems*. Centre for the Protection of National Infrastructure (CPNI).

Försvarets Materielverk (FMV) (2013). *Industrisäkerhetsskyddsmanual* (13FMV4466-1:1). Stockholm: FMV.

Försvarets Radioanstalt (FRA) (2017). *Åtgärdsförslag: Angrepp via tjänsteleverantörer*. Stockholm: FRA.

Försvarsmakten (2013). *Handbok för Försvarsmaktens säkerhetstjänst Grunder* (H SÄK Grunder) (M7745-734011). Stockholm: Försvarsmakten.

Imran, Z. (2015). Best Practices for Securing Remote Access. *Infosec Institute*, 13 oktober. http://resources.infosecinstitute.com/best-practices-for-securing-remote-access/ [2018-03-01]

Langner, R. (2013). *To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

National Institute of Standards and Technology (NIST) (2013). *SP800-53 Security and Privacy Controls for Federal Information Systems and Organizations* (SP800-53r4). Gaithersburg: NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Saltzer, J.H. & Schroeder, M.D. (1975). The Protection of Information in Computer Systems. I *Proceedings of the IEEE*, 63(9), ss.1278–1308. DOI: 10.1109/PROC.1975.9939

Souppaya, M. & Scarfone, K. (2016). *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (SP800-46, rev.2). Gaithersburg: NIST. DOI: http://dx.doi.org/10.6028/NIST.SP.800-46r2

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

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

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

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

www.msb.se