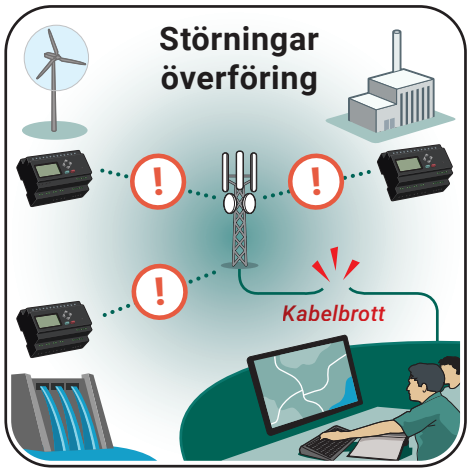
18 Risker vid nyttjande av trådlös teknik i industriella informations- och styrsystem.



NERC CIP-005-5/6 R2
NIST 800-53 AC-18, 800-97
27002 kap 13.1.1, 13.1.3
27033-6

Utvecklingen av nya tekniker för trådlös kommunikation har lett till att priset för denna typ av utrustning har sjunkit. Inköp och installation har blivit mer kostnadseffektiv än för trådbunden kommunikation. Samtidigt införs nya risker med trådlös kommunikation jämfört med trådbunden.

Trådlös kommunikation kräver en annan typ av säkerhetskompetens än vid nyttjande av trådbunden. Det är enklare att skydda den trådbundna kommunikationen mot obehörig åtkomst genom att skydda utrustningen och kablaget. All kommunikation via radiovågor är däremot tillgänglig för vem som helst inom räckvidden med rätt utrustning och kompetens. En angripare behöver alltså inte ha fysisk tillgång till radioutrustningen eller kablage. Flera radiotekniker går att avlyssna, imitera eller störa ut. Störningar kan också ske genom naturliga eller omedvetna händelser.

Det är väsentligt att de samhällsviktiga funktioner som finns i vårt samhälle är robusta och tåliga mot olika typer av störningar. Ansvariga aktörer bör därför inte förlita sig enbart på trådlös kommunikation.

Användningen av utrustning som sänder radiovågor är reglerad och varje teknik använder olika frekvensområden. Det är viktigt att endast använda sådan radioutrustning som är godkänd och certifierad i det land där utrustningen används. Det skiljer sig exempelvis mellan EU och Nordamerika och utrustning som anskaffats till ett lägre pris i ett annat land kan vara förbjuden att använda i Sverige. Ansvarig myndighet för frekvenstilldelning i Sverige är Post- och telestyrelsen (PTS). Det krävs särskilt tillstånd av PTS om man avser att sända på radiofrekvenser som inte tillhör de licensfria frekvenserna.

Rekommendationer

- Tänk på att den trådlösa kommunikationen kan
  - störas vilket får till följd att kommunikation till eller från enheten inte kan genomföras;
  - ändras eller imiteras och på så sätt få följdverkningar såsom felaktiga inställningar eller felaktig datainsamling;
  - avlyssnas och på så sätt röja information för obehöriga.

- Välj utrustning specifikt för ändamålet och konfigurerat för att följa frekvensregleringen.
- Använd den trådlösa och den trådbundna kommunikationen som komplement till varandra (trådlöst är bra när kabeln är trasig och trådbundet är bra när den trådlösa är störd).
- Använd tillgängliga säkerhetsåtgärder i den trådlösa kommunikationen, t.ex. kryptering, autentisering, segmentering av nätverk och övervakning.

Exempel på risker och problem:
Trådlös uppkoppling innebär risk för flera typer av hot. Data som skickas kan avlyssnas och analyseras av obehörig part samt manipuleras och störas ut. Radioutrustning som kan kontrolleras av datorer (SDR, Software Defined Radio) är idag billig att införskaffa vilket innebär att alla aktörer, oavsett syfte, kan införskaffa denna utrustning som sedan kan användas för att både lyssna, sända och störa.
Två exempel på angrepp mot den trådlösa kommunikationen är passiv avlyssning och återuppspelningsattack. Den passiva avlyssningen innebär att kommunikationen samlas in i en radiomottagare. Återuppelningsattacker kan antingen vara att tidigare inspelad radiotrafik återutsänds eller att det inspelade innehållet återutsänds med modifierat innehåll. Om sådana attacker kan lyckas är helt beroende på radioutrustningens egen förmåga att kunna detektera dessa eller att kommunikationsprotkollen har säkerhetsåtgärder mot dessa attacker.
Alla hot mot trådlös kommunikation är inte antagonistiskt relaterad. Trådlös kommunikation kan störas av naturliga händelser (exempelvis rymdväder såsom solstormar), handhavandefel eller att den egna eller annan utrustning är felkonfigurerad eller trasig. Två exempel på det sistnämnda är:

- I närheten av hamnen i Moss Landing, Kalifornien, USA, störtes GPS signaler ut. Efter att störningarna analyserats visade det sig att olika TV antenner i närheten hade trasiga förstärkare vilket resulterade i störningen.
- I en fabrik slogs det interna trådlösa nätverket (WiFi) ut vid lunchtid i direkt närhet av matsalen. Det visade sig att anställda hade försökt laga mikrovågsugnar men avskärmningen hade skadats och blivit undermålig när enheterna öppnats och förslutits.

Någon som använder otillåten radioutrustning, t.ex. sådan som är inköpt i en annan region, kan också vara en källa till störning.

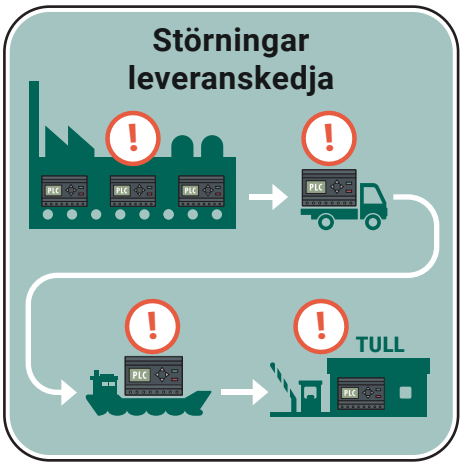
RIKTMÄRKEN FÖR SÄKERHETSARBETET

Det ska finnas en dokumenterad policy som anger vilken kommunikationsteknik som ska användas, till vad kommunikationstekniken (trådbunden eller trådlös) ska nyttjas samt vilka säkerhetsåtgärder som ska införas inom respektive område.

Det ska finnas rutiner som hanterar anskaffning, installation, konfiguration, nyttjande och kontroll av trådlös utrustning.

Det ska finnas dokumentation på all trådlös utrustning, hur den nyttjas och vilka parametrar (exempelvis frekvenser, bandbredd, kanaler, m.m.) som är konfigurerade.

19 Riskhantering inom leveranskedjor för utrustning & mjukvara i industriella informations- och styrsystem.



NERC CIP 013-1
NIST 800-161
27036-1, 27036-2, 27036-3
27002 kap 15.1.2 - 15.1.3
28000
28004

Med en leveranskedja menas alla de steg som finns mellan tillverkning och leverans till slutkunden. I kedjan finns tillverkare, leverantörer, transportörer, distributörer, slutkundsförsäljning och alla de underleverantörer som ingår i kedjan. Det är viktigt att organisationen kan ha förtroende till alla de ingående delarna.

I och med globaliseringen är mycket av utveckling, design, tillverkning och lager ofta förlagd utomlands och i olika länder. Beroendet till hård- och mjukvarutillverkare, tjänsteleverantörer och transportörer medför att riskerna ändrar karaktär jämfört med att organisationen hanterar processen helt själv. Ett exempel på detta är att material eller produkter beställs så att dessa levereras precis innan de ska nyttjas. Genom att ha ”lagret” hos leverantören och transportören kan organisationens lagernivå vara lägre, men med risken att vid vissa tillfällen stå utan en korrekt leverans.

En leveranskedja kan delas in i olika områden.

- Design och utveckling
- Produktion och konstruktion
- Logistik och transport
- Drift och förvaltning
- Avveckling och destruktion

Varje område har risker som behöver hanteras utifrån att information och utrustning sprids till obehöriga, går förlorad eller blir förvanskad.

En organisation som kontrakterar ut sin tillverkning, reservdelshantering, lagerhållning och leverans behöver vara säker på att leverantören har möjlighet att leverera i utsatt tid och överenskommen mängd. Detta inkluderar alla leverantörens underleverantörer samt övriga ingående aktörer i leveranskedjan. Alla krav som behöver uppfyllas bör vara inskrivna i kontrakten så att kraven kan följas upp och granskas.

Att använda sig av olika leverantörer och underleverantörer kan medföra en risk genom att olika versioner (och ibland end-of-life, utdaterade) komponenter används vid tillverkningen. Äldre komponenter stödjer inte samma säkerhetsåtgärder som nya och uppdateringar är inte alltid garanterade. För att minska riskerna att få avsiktligt

inbyggda sårbarheter i komponenter så kan varorna köpas genom en distributör för att på så sätt dölja den verkliga kunden gentemot producenten. Undvik även att dela information med t.ex. underleverantörer om varornas ändamål och verklig slutkund.

Rekommendationer:

- Identifiera vad som behöver skyddas i leveranskedjan.
- Välj leverantörer med en adekvat riskhantering. Detta gäller alla delar i leveranskedjan: från design, utveckling, produktion, logistik och transport till support och garantiåtaganden.
- Se till att kraven kan uppfyllas av alla aktörer i leveranskedjan. Ta med krav på informationssäkerhet i avtal och kontrakt.
- Verifiera kontinuerligt att införda åtgärder utförs och utvärdera dessa regelbundet.
- Verifiera att produkters och tillverkares godkännanden och certifieringar är korrekta, valida och inom korrekt sakområde.

Exempel på risker och problem:
Så kallade ”bakdörrar” har påträffats i flera produkter. Dessa är svåra att upptäcka då de integreras i komponenters hård eller mjukvara. Bakdörrar är ett sätt att möjliggöra obehörig åtkomst till system t.ex. genom att införa hårdkodade (och odokumenterade) inloggningsuppgifter i mjukvaran. En sådan upptäcktes av ett företag som hade märkt att mycket data överfördes nattetid till en server utomlands vid tidpunkter då de själva inte använde nätverket. Detta hade pågått i flera år innan upptäckt.

En organisation valde efter flera år att byta leverantör av material som används i kärnverksamheten. Organisationen hade valt att ha ett mycket litet lager av material i sitt eget lager, vilket gjorde att man var beroende av kontinuerliga leveranser. Detta hade under tiden med den tidigare leverantören fungerat mycket bra och organisationens arbetssätt hade byggts upp kring detta. Med den nya leverantören så uppstod det genast problem med att inget eller bara lite material levererades. Eftersom organisationen inte hade något eget lager så uppstod det följdproblem i processen med höga kostnader och brister i förtroendet som följd.

Ett företag beställde att en industriprodukt skulle tillverkas i en fabrik utomland. I kontraktet mellan beställaren och utföraren uppfördes krav att företagshemlig information inte skulle hamna hos obehöriga. Det visade sig sedan att utföraren nyttjade en molntjänst för backup av information som inte uppfyllde dessa informationssäkerhetskrav och beställarens information kom obehöriga till del.

RIKTMÄRKEN FÖR SÄKERHETSARBETET
Organisationen arbetar regelbundet med att identifiera vad som är skyddsvärt inom organisationen och hur detta ska skyddas.
För dialog med leverantör om lämplig praxis redan tidigt under upphandling.
Vid upphandling inkludera säkerhetskrav som är relevanta baserat på arbetet med identifiering av skyddsvärden och skydd av dessa.
Genom kontroll och uppföljning säkerställa att hela leveranskedjan följer rutiner som uppfyller de avtalade kraven på riskhantering/säkerhet.