Myndigheten för samhällsskydd och beredskap

VÄGLEDNING

Cybersäkerhet i tunga räddningsfordon

Cybersäkerhet i tunga räddningsfordon

Enhet: RO-BR

Foto omslag: Johnér
Text: MSB i samarbete med FOI

Publ nr: MSB2122 - januari 2023
ISBN: 978-91-7927-330-9

Förord

Den tekniska utvecklingen och digitaliseringen går snabbt. Arbetet med cybersäkerhet har inte följt med i samma tempo. Det innebär att både enskilda organisationer och hela samhället blir sårbart för olika cyberhot. För att uppnå en så god cybersäkerhetsnivå som möjligt är det viktigt att arbeta både proaktivt och reaktivt.

Antalet datorsystem i ett typiskt modernt tyngre fordon är stort och antalet radiouppkopplingar som installeras ökar, vilket även ökar fordonens sårbarhet för cyberangrepp på distans. Räddningstjänstens fordon är anpassade specialfordon med påbyggnader och extrautrustning som är specifika för räddningstjänstens verksamhet. Dessa påbyggnader är inte sällan tredjepartssystem, det vill säga system som är installerade i fordon av en leverantör som inte är originaltillverkaren. Dessa installationer gör att de potentiella attackytorna blir fler och risken för framgångsrika cyberangrepp ökar. Det, i kombination med den långa livslängden hos fordon för räddningstjänst som riskerar att medföra att säkerhetsbrister kvarstår under lång tid, gör det angeläget att höja beställares och användares kompetens inom detta område.

Syftet med vägledningen är att ur perspektivet cybersäkerhet ge stöd vid upphandling av fordon till räddningstjänsten, samt att öka medvetenheten om vad man behöver ta i beaktande vid drift, underhåll och ombyggnationer av denna typ av fordon.

Vägledningen är framtagen i samarbete mellan MSB och Totalförsvarets forskningsinstitut (FOI) och har sin grund i standarder, forskningsartiklar och branschspecifika vägledningar. Inom ramen för arbetet har även ett antal intervjuer och studiebesök på räddningstjänster samt intervjuer med påbyggnadsleverantörer och med fordonstillverkare genomförts.

Karlstad, 2022-12-30

Patrik Perbeck

Stf. avdelningschef

Avdelningen för räddningstjänst och olycksförebyggande

Innehåll

Introduktion

Fordon blir alltmer uppkopplade mot nätverk, som mycket annat i dagens samhälle. Fordon består inte längre bara av en samling mekaniska delar, utan även av elektroniska komponenter och datorer. Detta ökar risken att något kan gå fel, exempelvis uppdateringar. Fokus i denna vägledning ligger dock på antagonistiska hot. Cybersäkerhetsangrepp mot fordon kan få allvarliga konsekvenser, eftersom de kan påverka fordon under färd. En sådan händelse kan få stora följdverkningar för både förare, passagerare och övriga trafikanter. För tunga lastbilar kan det även leda till samhällspåverkan, som till exempel olyckor vid transport av farligt gods. Allvarlig samhällspåverkan skulle även ske om cyberangrepp kan försätta blåljusfordon eller dess specialfunktioner ur spel. Särskilt för tunga räddningsfordon, då tillgänglighet av fordon med brandbekämpande och livräddande funktioner är kritiska för att räddningstjänsten ska kunna ingripa effektivt.

Tunga räddningsfordon är anpassade specialfordon med påbyggnader och extrautrustning som är specifika för räddningstjänstens verksamhet. De innehåller dock samma teknik som andra typer av tunga lastbilar. I och med det kommer tunga räddningsfordon att innehålla många av de sårbarheter som finns i andra tunga lastbilar. Att många räddningstjänster använder fordon från ett fåtal leverantörer innebär dessutom att många fordon kan antas ha samma sårbarheter. Ett cyberangrepp (riktat eller inte) kan alltså drabba många räddningsfordon samtidigt.

Vid uppdateringar är det viktigt att följa kommunens policy för informationssäkerhet, för att säkerställa bland annat att skadlig kod inte sprids från ett fordon till ett annat vid mjukvaruuppdateringar med exempelvis USB-stickor.

Sammantaget innebär detta att informationssäkerhet och cybersäkerhet behöver genomsyra utveckling, tillverkning, användande och underhåll av tunga räddningsfordon för att minimera antalet sårbarheter. Därmed kan man undvika att cyberattacker påverkar tillgängligheten.

Syfte och målgrupp

Syftet med denna vägledning är att ge stöd inom cybersäkerhet till kommunala räddningstjänster i arbetet med kravställning, inköp och ombyggnation av tunga räddningsfordon. Stödet kan också vara relevant för andra typer av blåljusfordon. Vägledningen riktar sig främst till kommunala räddningstjänster, men också till alla som arbetar med upphandling av eller använder räddningsfordon.

Förklaring av begrepp

Tabell 1. Förklaring av begrepp som används.

Begrepp	Förklaring
Cybersäkerhet	All verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot möjliga handlingar, omständigheter, eller händelser som på ett negativt sätt påverkar nätverks- och informations-systemen och människor. Cybersäkerhet handlar främst om att möta antagonistiska hot.
Extrautrustning	Allt som installeras, utöver påbyggnader. Det kan exempelvis vara kommunikationssystem, blåljus, elverk och pumpar.
FMS	Flottledningssystem (eng. Fleet Management System). FMS är ett standardgränssnitt för fordonsinformation från kommersiella fordon. Informationen från systemet hjälper företag att bättre använda fordonen genom att sända prestanda, positionering samt drift- och underhållsinformation från fordonet till företaget.
Grundfordon	Olika typer av fordon med chassi, drivlina, hytt och liknande, som sedan kan byggas på med olika påbyggnader.
Halta-hem-läge	Halta-hem är en motorfunktion som möjliggör att fordonet förflyttas med begränsad kapacitet vid vissa problem som annars kunde innebära totalt stopp.
Informationssäkerhet	Att skydda information så att den alltid finns när vi behöver den (tillgänglighet), att vi kan lita på att den inte är manipulerad eller förstörd (riktighet), att endast behöriga personer får ta del av den (konfidentialitet). Informationssäkerhet handlar om att skydda informationen i sig, oavsett vilket medium den förmedlas på. Informationssäkerhet uppnås genom att vidta administrativa, organisatoriska, tekniska och fysiska åtgärder.
Infotainmentsystem	Infotainmentsystem i fordon avser den utrustning som i första hand associeras med underhållning i fordonet. I moderna fordon innebär detta vanligen någon typ av integrerad pekskärm, men i vissa fall även en digital instrumentdisplay.
Lastbil	Ett fordon som huvudsakligen är till för att köra gods eller en bil som varken går att definiera som personbil eller buss.
Påbyggnad	Något stort (och huvudsakligen mekaniskt) som monteras fast på fordonets chassi, exempelvis tankar, skåp och lastväxlare. Normalt monteras påbyggnader där flaket skulle suttit på en vanlig flaklastbil.
Tung lastbil	En lastbil som har en totalvikt över 3,5 ton.
Tunga räddningsfordon	Tunga räddningsfordon är i grunden tunga lastbilar som har anpassats. Räddningstjänstens tunga räddningsfordon kan delas in i olika kategorier eller typer. Primärt finns tre olika typer av tunga räddningsfordon: 1. släckbil 2. tankbil 3. höjdfordon. Det finns även andra typer av specialiserade fordon, exempelvis räddningsfordon för kemikalieolyckor eller för utryckning som kräver vattendykning.

Avgränsningar

Vägledningen omfattar stöd för att skydda tunga räddningsfordon mot cyberangrepp. Fokus ligger främst på skydd mot antagonistiska hot, men genom att följa rekommendationerna kommer man även i hög grad att minska riskerna för incidenter orsakade av exempelvis handhavandefel. Alla typer av fordon som faller utanför definitionen av tung lastbil, exempelvis personbilar, bussar, terrängfordon, släpfordon, efterfordon och motorredskap, faller utanför omfånget av denna vägledning. Det finns dock beröringspunkter med andra fordon, som mindre transportfordon, befäls- och ledningsfordon och mindre räddningsfordon, där delar av denna vägledning kan nyttjas.

Det finns också andra risker och sårbarheter relaterade till fordon som inte direkt har med cybersäkerhet att göra, exempelvis fysiska sabotage och elektromagnetisk störning. Dessa omfattas inte av denna vägledning.

Bakgrund

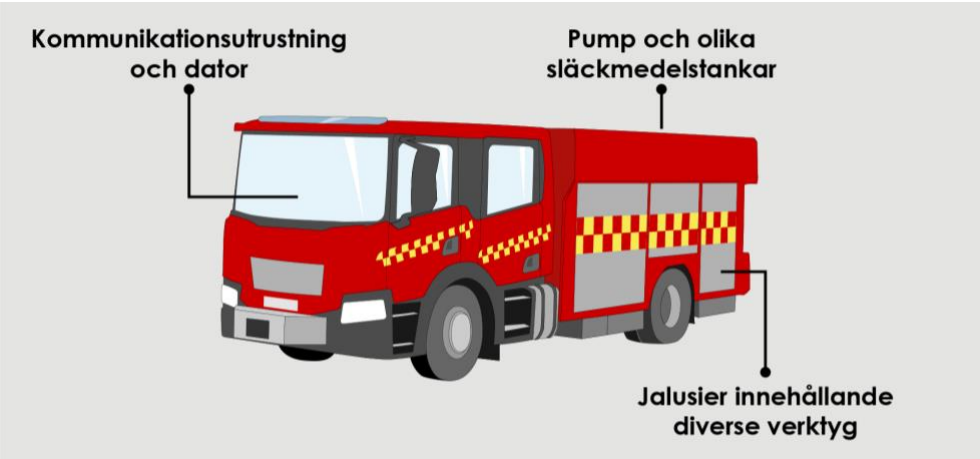
Digitaliseringen och utvecklingen av fordon har lett till att de numera är komplexa system med stora mängder kod.[1] Inom fordon kommunicerar olika informationssystem med varandra för att styra grundläggande funktioner och ge avancerad funktionalitet för att bland annat stödja föraren (förarassistans). Strålkastare kan till exempel styras genom datakommunikation, istället för med en mekanisk strömbrytare.

Detta kapitel ger en introduktion till tunga räddningsfordon och hur de skiljer sig från andra typer av fordon. Dessutom beskrivs hur fordonen beställs samt hur service och underhåll genomförs efter ett fordon tagits i bruk. Slutligen ges en introduktion till grunderna i cybersäkerhet gällande fordon, samt ett resonemang kring hot och risker som gäller för tunga räddningsfordon.

Tunga räddningsfordon

Tunga räddningsfordon är tunga lastbilar som anpassas för räddningstjänsten. Till exempel skulle en cementbil och ett tungt räddningsfordon kunna byggas på samma grundfordon, men deras respektive verksamhetsområde och utseende är väldigt skilda. Grundfordonet inreds med påbyggnader och extrautrustning som ger fordonet de funktioner som räddningstjänsten behöver. Från ett grundfordon kan exempelvis en släckbil, tankbil, höjdfordon eller andra specialfordon skapas. Det kan dock krävas olika typer av grundfordon för olika typer av specialfordon.

Ett räddningsfordon av typen släckbil utrustas med olika släckmedelstankar, pumpar och slangar, se figur 1. Förutom det finns även verktyg och utrustning för livräddning bakom fordonets olika jalusier. I fordonshytten finns sambandsutrustning, bland annat kommunikationssystemet Rakel, och i vissa fall finns även skärmar med ledningsinformation.



Figur 1. Räddningsfordon med påbyggnader.

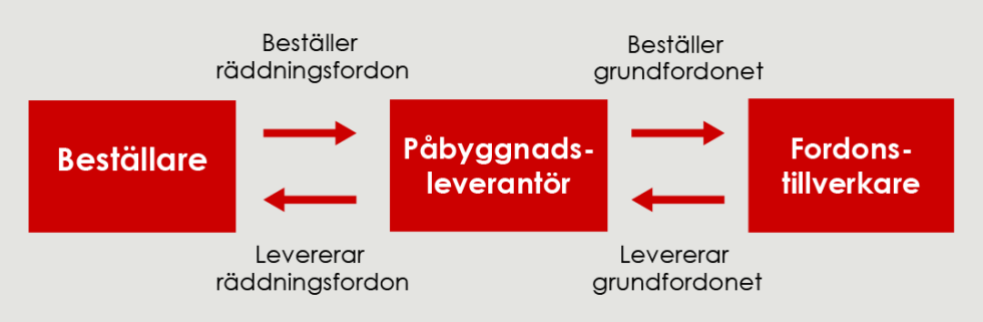
[1] Enligt en undersökning av Vard Antinyan (2020) hade ett fordon från Volvo omkring 100 miljoner rader kod.

Tunga räddningsfordon har generellt en lång livslängd i förhållande till andra typer av tunga lastbilar. Detta beror främst på att de inte används så frekvent och därmed blir miltal och slitage på fordonen lågt. Då det är en stor investering för den kommunala verksamheten att införskaffa sådana fordon behöver de också hålla länge och underhållas väl. Det är av stor vikt för verksamheten att räddningsfordon och tillhörande räddningsrelaterad utrustning har hög prestanda och tillgänglighet, vilket innebär att de ska gå att använda och fungera när de behövs.

Beställningsprocessen

Tillverkning av ett tungt räddningsfordon utgår som tidigare beskrivits från ett grundfordon. Grundfordonet tillverkas i sin helhet av en lastbilstillverkare (exempelvis Scania eller Volvo). Grundfordonet skickas sedan till en påbyggnadsleverantör, som bygger och installerar påbyggnader och extrautrustning på fordonet. Räddningstjänsten kan också själva installera extrautrustning i räddningsfordon, bland annat sambandsutrustning.

En typisk, men förenklad beställningsprocess visas i figur 2.



Figur 2. Beställningsprocess.

Många påbyggnationer behöver interagera med enheter i grundfordonet. Släckmedelspumpar i räddningsfordon behöver till exempel integreras med fordonets motor för att kunna drivas. I syfte att minimera riskerna vid integration implementerar fordonstillverkare generellt så kallade påbyggnadsgränssnitt i grundfordonet, även kallade gateways eller nätslussar. Dessa typer av gränssnitt förenklar påbyggnadsleverantörens arbete genom att sättet som leverantörens utrustning kommunicerar med utrustning hos grundfordonet är tydligt specificerat.

Fordonstillverkare ger instruktioner som måste följas när grundfordonet byggs om eller anpassas. Om instruktionerna inte följs så gäller inte fabriksgarantin för fordonet.

Exempel: Scanias anvisningar

Scania har instruktioner kring på- och ombyggnationer som påbyggnadsleverantörer måste följa. En auktoriserad representant hos Scanias återförsäljare måste godkänna på- och ombyggnationer som inte finns beskrivna i Scanias påbyggnadsinstruktioner. Efter varje påbyggnadsarbete eller ombyggnation ska påbyggaren intyga att påbyggnaden och påbyggnadsarbetet är utfört enligt Scanias instruktioner.

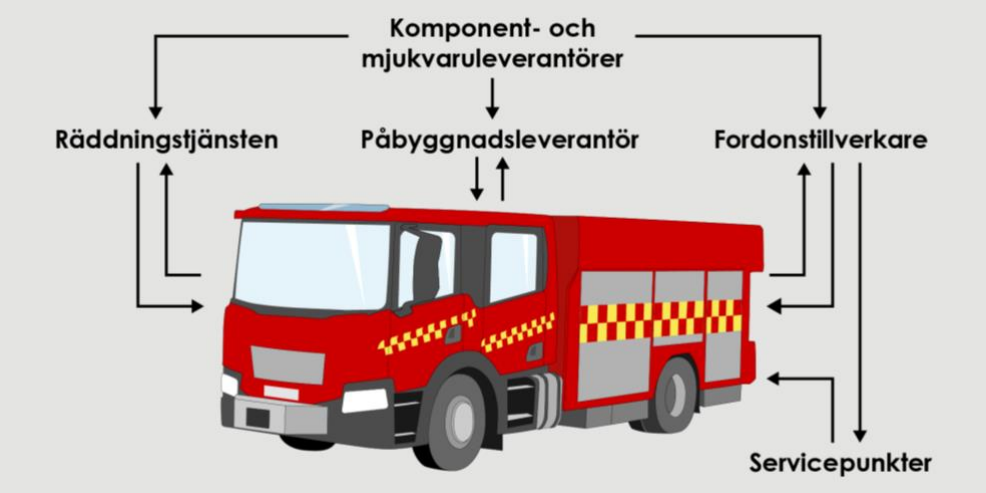
Påbyggaren ansvarar också bland annat för:

- att chassikomponenternas ursprungliga funktion och kvalitet kvarstår efter slutfört påbyggnadsarbete
- det kompletta fordonets egenskaper, i den mån egenskaperna påverkas av påbyggnaden
- att påbyggnadsarbetet uppfyller lag-, säkerhets- och lämplighetskrav
- att nödvändiga instruktioner och information om funktion och skötsel av påbyggnaden medföljer fordonet vid leverans till kund
- att artiklar som påbyggaren har satt dit på chassi är tydligt märkta med leverantörens namn och artikelnummer.

Både Scanias återförsäljare och påbyggaren ansvarar för att nödvändiga instruktioner och uppgifter följer med fordonet vid leverans till kund.

Service och underhåll

Efter ett räddningsfordon tagits i drift fortsätter fordonet att få hårdvaru- och mjukvaruuppdateringar genom service och underhåll. Figur 3 visar de olika aktörerna som interagerar med ett räddningsfordon efter det har tagits i drift.



Figur 3. Räddningsfordonets interaktioner med aktörer i omgivningen.

Uppdateringar av hårdvara eller mjukvara i fordonet installeras av olika parter, beroende på vilken typ av uppdatering och vilken komponent som berörs. Gäller det grundfordonet är det fordonstillverkarens ansvar att komma med uppdateringar. Dessa uppdateringar installeras normalt hos serviceverkstäder som även utför regel-

bunden service. Om trådlös uppdatering är aktiverat kan vissa typer av mjukvaruuppdateringar installeras direkt av fordonstillverkaren. Även påbyggnader och extrautrustning kan behöva uppdateringar, eftersom de också kan innehålla mjukvara och komponenter som kan behöva bytas ut. Dessa uppdateringar utförs av påbyggnadsleverantören. I de fall räddningstjänsten själva installerat extrautrustning så är det normalt de själva som uppdaterar dessa komponenter.

All mjukvara och hårdvara konstrueras inte av fordonstillverkaren eller påbyggnadsleverantören, utan kan komma från underleverantörer. Underleverantörer kan därför leverera uppdateringar som sedan installeras av fordonstillverkaren, påbyggnadsleverantören eller serviceverkstäder. Det är därför viktigt att det i avtalet framgår när leverantörens serviceavtal löper ut samt när säkerhetsuppdateringar inte längre kommer att tillhandahållas. Det bör finnas en plan på hur risker som då kan uppkomma ska hanteras, till exempel genom att fordonet ska gå att använda bortkopplat.

För att övervaka att fordonen fungerar bra kan flottledningssystem (Fleet management system, FMS) förekomma i fordonen. Information som samlas in kan exempelvis inkludera sensordata, position, körsträcka och rutt. Fordonstillverkaren kan ha ett internt inbyggt flottledningssystem i grundfordonet. Ibland installerar påbyggnadsleverantörer eller räddningstjänsten sina egna flottledningssystem. Dessa flottledningssystem kan ha en egen trådlös uppkoppling.

Cybersäkerhet i fordon

Informationssäkerhet

Informationssäkerhet är en förutsättning för cybersäkerhet och beskrivs ofta utifrån de tre aspekterna konfidentialitet, riktighet och tillgänglighet. Tillgänglighet är den viktigaste aspekten för räddningsfordon, eftersom fordonen är nödvändiga för den livräddande verksamheten. Riktighet är viktigt att beakta i relation till fordonets mjukvara och elsystem, som är viktiga delar för fordonets funktionalitet. Riktighet och konfidentialitet är också viktiga att beakta i relation till den information som hanteras i anslutning till fordonen. Det kan till exempel handla om räddningsobjekt, individer och personal. Information som kan behöva skyddas är exempelvis:

- position för skyddsvärda objekt
- information som räddningstjänst behöver för sitt arbete, exempelvis information om vattenledningsnät och pumpstationer
- information om utryckningstider
- ritningar över skyddsobjekt
- information om brandmän
- räddningsfordons position
- hastighet under utryckning
- annan information som kan ge en bild av räddningstjänstens samlade förmåga och agerande.

Aspekter för informationssäkerhet

- **Konfidentialitet** – att information inte röjs till obehörig part.
- **Riktighet** – att information eller funktionalitet inte förändras eller förstörs av obehörig part.
- **Tillgänglighet** – att information och funktionalitet ska vara tillgängliga när de behövs.

Cybersäkerhet

Cybersäkerhet är all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot möjliga handlingar, omständigheter, eller händelser som på ett negativt sätt påverkar nätverks- och informationssystemen och människor.

Tidigare hade de enheter som användes i fordon begränsad funktion och framför allt hade fordon inte samma möjligheter att kommunicera med omvärlden. Fordonsutvecklingen de senaste 10–15 åren har dock inneburit en allt bredare funktionalitet, samtidigt som kommunikationsmöjligheterna blivit fler. Detta innebär i sin tur att det finns en ökad risk att fordon kan påverkas av angripare. Den ökade risken har gjort cybersäkerhet till en viktig aspekt att ta hänsyn till och ställa krav på i både utveckling, användning och förvaltning av fordon.

Säkerhetsfunktioner som normalt används inom traditionella datorsystem och nätverk kan vara svåra att använda i fordon. Detta beror dels på begränsningar i den teknik som används i fordonen, men också på att det finns funktioner med höga krav på realtidskommunikation. Säkerhetsfunktioner som förs in behöver därför vara anpassande för ändamålet.

Hot mot räddningstjänsten

I allmänhet finns två typer av hot: avsiktliga och oavsiktliga. Avsiktliga hot involverar en aktör med aktiv vilja att orsaka skada. Oavsiktliga hot involverar istället misstag eller handhavandefel som kan leda till allvarliga sårbarheter, som i sin tur kan utnyttjas av en angripare.

Hotaktören, den som genomför angreppet, kan kategoriseras på olika sätt men det är vanligt att indelningen är efter teknisk och ekonomisk förmåga samt motivation. Indelat efter hur stort hotet är från hotaktörerna kan dessa kategoriseras in i fyra olika nivåer:

- script-kiddies
- hacktivister
- kriminella grupper
- statliga aktörer.

Script-kiddies är opportunistiska angripare, vars kompetens och ekonomiska tillgångar är relativt låga. Dessa angripares motivation varierar och kan bland annat utgöras av ekonomisk vinning eller vilja att testa något de lärt sig.

Hacktivister har varierande kompetens och ekonomiska medel. Det som framförallt skiljer denna typ av hotaktör från script-kiddies är motivationen. Hacktivister är generellt politiskt eller ideologiskt motiverade och drivs sällan av aspekter som ekonomisk vinning.

Kriminella grupper är i denna kontext nästan uteslutande motiverade av ekonomisk vinning och har ofta även den kompetens som krävs för att utgöra ett relativt stort hot.

Statliga aktörer är de som har den största budgeten och kompetensen för att utföra cyberangrepp, varför de utgör den farligaste hotaktören. Motivationen för statliga aktörer kan variera men består i regel av att på något sätt vilja underminera den som angrips.

Räddningstjänsten är ofta förskonad från angrepp då den verksamhet som utförs av räddningstjänsten generellt upplevs som god och viktig, även av individer som inte alltid uppskattar samhällets lagar och regler. Det finns dock hotaktörer som är motiverade att rikta angrepp mot räddningstjänsten. För de kriminella organisationerna kan det vara mycket lukrativt att använda utpressning, genom så kallade utpressningsvirus (eng. ransomware), för att komma över pengar från samhällsviktiga funktioner. Statsaktörer kan motiveras av att underminera verksamhetens funktion, indirekt påverka annan samhällsviktig verksamhet eller för insamling av konfidentiell information.

Angrepp som inte är riktade specifikt mot räddningstjänsten kan också innebära problem. Kriminella organisationer kan använda olika typer av breda angrepp (exempelvis med trojaner eller annan skadlig kod) för att skaffa sig tillgång till olika system. Åtkomsten kan sedan säljas vidare till en tredje part som är specifikt intresserad av räddningstjänsten. Hotaktören kan också vara ute efter att använda de övertagna enheterna för att angripa någon annan, exempelvis i överbelastningsattacker (eng. denial of service, DoS) på internet.

Räddningstjänsten kan även drabbas indirekt av angrepp som riktas mot någon leverantör i leverantörskedjan. Sådana angrepp kan spridas genom exempelvis mjukvaruuppdateringar och fjärrinloggningar, där leverantören har tillgång till system ute hos användarna.

Potentiella attackytor

Fordon är exponerade mot sin omgivning genom sina funktioner och de gränsytor som finns mot omgivningen. Cyberangrepp kan antingen utföras på distans eller via fysisk tillgång till fordonet. Om fordonet är uppkopplat mot internet via trådlösa länkar kan en angripare försöka påverka fordonet på distans. Olika fysiska gränssnitt

kan användas för att föra in skadlig kod. Den skadliga koden kan föras in direkt av angriparen eller indirekt, exempelvis via kod som en servicetekniker installerar.

I detta avsnitt ges en introduktion till de olika gränsytor som finns på ett fordon som en angripare kan försöka utnyttja.

Fysiska gränssnitt

Gränssnitt som medger dataöverföring utgör attackytor för en angripare som vill föra över skadlig kod. Om de är anslutna till det interna kommunikationsnätverket kan skadlig kod som kommer in via gränssnittet få stor påverkan på fordonets kritiska funktioner. Grundfordonet har flera olika typer av fysiska gränssnitt för datakommunikation. Det kan även finnas fysiska gränssnitt på påbyggnader och extrautrustning för exempelvis uppdateringar.

Fordon har ett diagnostikuttag (OBD-II/EOBD[2]) som framför allt används för att läsa av felkoder och meddelanden från fordonets styrenheter. Uttaget kan även användas för att uppdatera mjukvara. Denna typ av uttag möjliggör kommunikation direkt till fordonets interna kritiska styrenheter. Fordonet kan då vara helt exponerat mot inkopplad utrustning, men kompletteras ofta med någon form av behörighetskontroll. Det finns också OBD-II-adaptrar för övervakning och hantering av fordonsflottan som kommunicerar över internet, vilket ökar exponeringen ytterligare. När fordon genomgår regelbunden fordonsservice inkluderas ofta olika mjukvaruuppdateringar. Dessa utförs oftast genom att en dator ansluts till fordonet via OBD-II-porten. Det är tänkbart att IT-systemen hos servicestationer eller verkstäder utsätts för angrepp, där en angripare söker tillgång till servicedatorer.

Det finns även andra fysiska gränssnitt i ett fordon. Ett exempel är de USB-uttag som finns tillgängliga för föraren för att ladda mobiltelefonen eller för att koppla in sig till infotainmentsystemet.

Det är tänkbart att en angripare tar över en mobiltelefon och installerar skräddarsydd skadlig kod i den. När mobiltelefonen sedan ansluts till fordonet via exempelvis USB angriper den skadliga koden fordonets infotainmentsystem. Ett annat exempel på uttag som kan förekomma är SD-kortläsare som används för infotainmentsystemet. Det är lätt att tro att hot mot infotainmentsystemet inte skulle ge några allvarliga konsekvenser för fordon som helhet, men infotainmentsystem kan vara anslutna till det interna kommunikationsnätverket. Detta innebär att det kan gå att nå fordonets mer kritiska styrenheter via infotainmentsystemet.

Eventuella åtkomliga nätverksuttag kan användas för att utföra angrepp mot de av fordonets enheter som använder nätverket. Vissa fordonstillverkare har börjat använda Ethernet för snabbare informationsöverföring i fordonet, vilket förenklar angrepp då det är en allmän standard.

[2] EOBD är den Europiska varianten av OBD-II – de båda är mer eller mindre identiska och används ofta synonymt. OBD-II är den vanligast förekommande av de två.

Trådlös kommunikation

Fordon kan ha enheter för trådlös kommunikation, exempelvis Bluetooth och mobila nätverk. Bluetooth kan till exempel nyttjas för sammankoppling av mobiltelefon med infotainmentsystemet. Mobila nätverk kan nyttjas för distansuppdateringar (eng. over-the-air, OTA) eller för att skicka diagnostikinformation. En del påbyggnadsfunktioner och extrautrustning har en trådlös kommunikationslänk. Sådana kommunikationslänkar kan exempelvis användas av leverantörer för att se status, uppdatera och undersöka problem i funktionen eller till och med styra funktionen.

Angripare kan vilja utnyttja trådlös kommunikation för att påverka fordon på distans. Finns en koppling till fordonets kritiska styrenheter kan det innebära stora risker då en angripare exempelvis kan försöka överföra skadlig kod som försätter kritiska funktioner ur spel.

Sensorer

Sensorer för exempelvis däcktryck, Global Positioning System (GPS), kameror och radar kan vara anslutna till det interna kommunikationsnätverket. Angrepp mot sensorer utgör därmed också en attackyta mot det interna kommunikationsnätverket.

Mottagare för Global Navigation Satellite Systems (GNSS) (för exempelvis amerikanska GPS eller europeiska Galileo) tar emot radiosignaler med mycket låg effekt från satelliter i omloppsbana runt jorden och kan därför relativt lätt bli utstörda. Det är i nuläget relativt lätt, om än olagligt, för privatpersoner att införskaffa störsändare som kan störa ut GNSS-signaler. I samband med militärövningar i Sveriges närområde har stora geografiska områden drabbats av GNSS-störningar, särskilt i norr. Räddningstjänsten bör därför i sin kontinuitetsplanering ha inövade rutiner för hur verksamheten ska bedriva sin verksamhet när positioneringsstöd inte finns tillgängligt.

Påbyggnader och extrautrustning

Påbyggnader och extrautrustning behöver skyddas mot angrepp och kan även utgöra attackvägar mot fordonets kritiska funktioner eller andra kritiska påbyggnader eller extrautrustning. Attackvägen är mer direkt om den inte går via påbyggnadsgränssnittet, utan istället via fordonets interna kommunikationsnätverk. Anslutningar ska därför alltid göras enligt fordonstillverkarens instruktioner.

Eftersom fordon kan innehålla funktionalitet från olika aktörer är det viktigt att se till att en komponent eller funktion inte påverkar en annan negativt. En påbyggnad kan vid installation vara isolerad, inte nåbar med en extern kommunikationslösning och därmed säker mot angrepp. Om en ny komponent med extern kommunikation sedan ansluts bryts isolationen och cybersäkerheten kan försvagas. I förlängningen kan detta påverka funktionen hos fordonet som helhet.

Det är alltså viktigt att säkerställa både att individuella komponenter eller funktioner i fordon fungerar korrekt och är säkrade ur cybersäkerhetssynpunkt och att implementation och interaktion mellan komponenter och system inte påverkar varandra negativt vid eftermontering av komponenter. Utöver detta

är det även viktigt att se till att påverkan hos en leverantörs egna IT-system för service och underhåll inte kan leda till en påverkan hos fordonen, eller att den potentiella påverkan minimeras. Detta gäller under hela systemets livslängd.

Säkra komponenter med säker interaktion

Följande är viktigt att säkerställa:

- Varje enskild komponent eller funktion ska fungera korrekt och vara säker ur cybersäkerhetssynpunkt.
- Ingen oönskad påverkan ska kunna ske i samverkan med övriga komponenter och funktioner. Detta är särskilt viktigt att vara uppmärksam på vid eftermontering av komponenter.

För tunga lastbilar är tillverkningsår relevant i förhållande till cybersäkerhet. Detta beror på att många tunga lastbilar, oavsett tillverkare, har samma delkomponenter från samma underleverantörer. Det betyder att en sårbarhet i en specifik modell också troligtvis finns i andra tillverkares modeller från samma år. En cybersäkerhetsmässig sårbarhet i ett tungt fordon kan därför få mycket stor spridning och påverkan.

Tillverkningsår och cybersäkerhet

Tunga lastbilar tillverkade samma år, oavsett märke, använder ofta delkomponenter från samma leverantör. Samma sårbarheter kan därför finnas i flera olika lastbilsmodeller från olika tillverkare.[3]

[3] Wiemerskirch, Becker & Hass 2017; Jonson 2018; Tollefson 2019, samt Valassi, C och Karressand, M. (2020). Cyberfysiska sårbarheter i tunga fordon – Med inriktning mot tunga fordon av vikt för civilförsvaret. FOI-R--5067—SE.

Organisatoriska rekommendationer

I detta kapitel presenteras vägledningens organisatoriska rekommendationer för att öka cybersäkerheten i tunga räddningsfordon. Här beskrivs sju områden med rekommendationer och exempel på hantering av relaterade risker. Rekommendationerna har sammanställts utifrån material från standarderna ISO 21434:2021 och ISO 27000-serien samt från intervjuer med fordonstillverkare, påbyggnadsleverantörer och räddningstjänsten.

Kapitlet innehåller organisatoriska rekommendationer inom följande områden:

- planering, krav och design utifrån livscykelperspektiv
- styrning och avtal för samarbete
- granskning och kvalitetssäkring
- systemuppdateringar
- konfigurationsledning
- säker leveranskedja
- utbildning.

Planering, krav och design utifrån livscykelperspektiv

Ett räddningsfordon har lång livslängd och kan utsättas för en mängd olika situationer som behöver hanteras ur ett cybersäkerhetsperspektiv. Cybersäkerhet behöver tas med redan i planeringsstadiet inför anskaffning av nya räddningsfordon. Att göra så ger en mer kostnadseffektiv och genomtänkt design än om säkerheten byggs på i efterhand. Cybersäkerhet behöver finnas med från början även vid anskaffning av nya kringliggande system, det vill säga de datorer som interagerar med fordonen för exempelvis uppdateringar och datakommunikation.

En utmaning för system med lång livslängd är att den mjukvara de använder efter några år inte längre underhålls, eller att system de är beroende av inte längre är tillgängliga. Ett exempel är om fordons- eller komponenttillverkare går i konkurs, så att tillverkarens FMS inte längre är tillgängligt. Detta måste hanteras och kan lösas på olika sätt.

Kampen mellan angripare och försvarare pågår ständigt och det kommer att dyka upp nya risker och sårbarheter även efter att fordonen tagits i bruk. Därför behöver det finnas processer för att identifiera nya risker och sårbarheter samt för att upprätthålla säkerheten under fordonets livstid. Vid avveckling behöver utrustning som innehåller känslig information avlägsnas så att den inte hamnar i orätta händer.

Genom att ta med cybersäkerhet genom hela livscykeln kan organisationen identifiera åtgärder som möter de utmaningar som kan uppstå under fordonets hela livslängd, inklusive vid avveckling.

Rekommendationer

- Beskriv fordonsfunktioner och deras interaktioner med omgivningen under hela livscykeln, vilket bland annat inkluderar driftsättning, underhåll och serviceuppdateringar. Med interaktion avses i sammanhanget kommunikation till och från fordonet både fysiskt och på distans. Identifiera vilka funktioner och komponenter i räddningsfordonet och stödsystemen som kräver cybersäkerhet och därmed behöver särskilt skydd och hantering.
- Specificera övergripande mål för cybersäkerhet för räddningsfordonet och dess interagerande system för exempelvis uppdateringar och övrig datakommunikation.
- Genomför riskanalyser i syfte att identifiera risker kopplade till fordonet och stödsystemen det interagerar med. Värdera och bedöm riskernas konsekvenser, identifiera mildrande åtgärder samt utse ansvarig personal som hanterar risken. Riskanalys bör genomföras i början av anskaffningsprocessen samt vid varje systemförändring som kan ha en påverkan på cybersäkerheten. Riskanalyser ska även ske på fordonet som helhet utifrån fordonets påverkan på räddningstjänstens förmåga. Som stöd i arbetet kan löpande omvärldsanalyser göras i syfte att ta reda på vilka risker och hot som finns mot fordonet och mot verksamheten.
- Hantera identifierade cybersäkerhetsrisker genom lämpliga åtgärder. Åtgärder kan exempelvis bestå av kravändringar, tekniska förändringar eller ändringar av processer och rutiner beroende på riskernas karaktär. I många fall finns det flera olika sätt att hantera en risk. Organisationen måste därför ta ställning till vilka åtgärder som är lämpligast för verksamheten.
- Specificera krav utifrån verksamhetens behov. Kraven kan röra tekniken, hur organisationen ska arbeta med räddningsfordonet och dess interagerande system samt samarbete med leverantörer. Säkerställ sedan att kraven möter behoven och att alla risker är hanterade.
- Avlägsna fordonets informationsbärande utrustning när fordonet avvecklas, så att konfidentiell data inte kommer i orätta händer och utrustningen inte kan användas för att komma åt räddningstjänstens system.

Styrning och avtal för samarbete

Ett räddningsfordon och dess stödsystem består av många olika delkomponenter. Ansvaret för cybersäkerhet är utspritt på flera olika aktörer. Fordonstillverkaren har ansvar för själva grundfordonet med de basala fordonsfunktionerna. Påbyggnadsleverantören har ansvar för de påbyggnader och den extrautrustning som de installerat. Räddningstjänsten har ansvar för den extrautrustning de

installerar själva. Ansvaret för att ställa krav och säkerställa att inblandade aktörer hanterar sin del av cybersäkerheten ligger på beställaren av fordonet.

Det är viktigt att reda ut vem som ansvarar för vad och att reglera förväntningar och ansvar kring samarbetet i avtal med leverantörerna. Utan en beställare som ser till att alla inblandade förstår sitt ansvar kan viktigt arbete hamna mellan stolarna. Det är även viktigt att utse personer inom organisationen som ansvariga för cybersäkerheten och se till att de har en budget som möjliggör cybersäkerhetsrelaterade aktiviteter och att upprätthålla nödvändiga relationer för kommunikation mellan aktörer. Alla relevanta aktörer behöver samarbeta för ett effektivt cybersäkerhetsarbete.

Rekommendationer

- Utse personal som är sammanhållande och ansvarig för cybersäkerheten i verksamheten.
- Möjliggör aktiviteter relaterade till cybersäkerhet genom att exempelvis avsätta ekonomiska medel.
- Tydliggör vem, både organisation och roll, som har ansvar för respektive aktivitet i arbetet med cybersäkerhet. När arbetet inkluderar flera organisationer bör parterna även identifiera relevanta beroenden och definiera hur interaktionen mellan parterna ska ske.
- Ta hjälp av den egna organisationens experter inom upphandling och cybersäkerhet för att ge råd kring kravformuleringar som ger tillräcklig säkerhet.

Granskning och kvalitetssäkring

Det finns direktiv och föreskrifter som fordonstillverkare och påbyggnadsleverantörer behöver följa. Beställare bör även försäkra sig om att påbyggnadsleverantörer följer fordonstillverkarens instruktioner för påbyggnader. Om föreskrifter och avtal inte följs riskerar påbyggnader och extrautrustning att installeras på ett sätt som leder till att cybersäkerhetsrisker introduceras i fordonet. Sådana risker kan sedan utnyttjas av en angripare för att påverka fordonet. I grunden handlar det om att fordons- eller chassitillverkaren exempelvis ska ha processer i sin mjukvarudesign som säkerställer cybersäkerheten hos fordonet och minimerar cybersäkerhetsrisker hos externa gränssnitt. Det ligger i fordons- eller chassitillverkarens intresse att ha en dialog med påbyggnadsleverantörer kring detta och att i avtal säkerställa att lagstadgad funktionalitet inte ska påverkas vid om- eller påbyggnation.

FN-regelverken som nämns under ”Rekommendationer” gäller för vissa typer av fordon och beroende på vilka komponenter som ingår i dem. För fordon som är EU-godkända gäller kraven genom förordning EU 2022/545 på tillverkare för nya fordonstyper från juli 2022, och från juli 2024 för samtliga producerade fordon.

Alla fordon oavsett typ granskas på ett eller annat sätt ur trafiksäkerhets- och personsäkerhetssynpunkt, exempelvis genom typbesiktning och kontrollbesiktning. Dessutom behöver granskning ske ur ett cybersäkerhetsperspektiv. Sådan granskning

syftar till att säkerställa att räddningsfordonets påbyggnader och extrautrustning inte medför cybersäkerhetsrisker. Detta inkluderar även kringliggande system som interagerar med fordonet och de gränsytor som fordonets system använder för att kommunicera med omvärlden. En granskning ur detta perspektiv sker inte rutinmässigt. Det är beställaren som ansvarar för att detta görs.

Rekommendationer

- Fordonstillverkaren och/eller påbyggnadsleverantören bör dokumenterat kunna visa att:
    - Fordonstillverkaren uppfyller cybersäkerhetsrelevanta föreskrifter och standarder, bland annat UNECE-föreskrifterna UN Regulation No. 155, UN Regulation No. 156 och ISO 21434, vid tillverkningen av fordonet.
    - Påbyggnadsleverantören uppfyller cybersäkerhetsrelevanta föreskrifter och standarder, bland annat UNECE-föreskrifterna UN Regulation No. 155, UN Regulation No. 156 och ISO 21434, vid modifieringen och anpassningen av fordonet.
    - Påbyggnadsleverantörer vid om- eller påbyggnad följer fordonstillverkarens instruktioner och anvisningar för cybersäkerhet.
    - Påbyggnadsleverantörer vid om- eller påbyggnad säkerställer att lagstadgad funktionalitet hos fordonet inte påverkas.
    - Fordonstillverkare och påbyggnadsleverantör reglerat i avtal vilken modifikation som får ske och hur denna får genomföras.
    - Påbyggnader uppfyller räddningstjänstens cybersäkerhetskrav.
- Ansvarig funktion för cybersäkerhet på kommun- eller räddningstjänstnivå bör:
    - Säkerställa att granskning ur ett cybersäkerhetsperspektiv sker av extrautrustning som räddningstjänsten själva installerat i fordonet. Detta kan göras med hjälp av intern kompetens eller med hjälp av en extern granskare.
    - Säkerställa att granskning ur ett cybersäkerhetsperspektiv sker av mjukvaror och kommersiella standardprodukter (eng. COTS, Commercial-off-the-shelf), innan produkterna används i fordonen eller i kringliggande system. Detta gäller även programvara som används för drift och uppdatering av fordon.
    - Säkerställa att granskning sker av uppdateringar och förändringar i fordonets hård- och mjukvara, i syfte att upptäcka förändringar som kan ge negativ påverkan på cybersäkerheten. Detta går även att lägga på leverantören/ombyggaren/förvaltaren och sker i så fall genom kravställning vid upphandling av ansvarig funktion. Ansvarig funktion behöver också utföra kontroller av att detta utförs.

Exempel på risk

En missnöjd anställd hos en leverantör går med på att mot betalning införa skadlig kod i en uppdatering som ska installeras hos räddningstjänsten. Eftersom det inte finns någon granskningsprocess så installeras uppdateringen. Detta resulterar i att en funktion i räddningsfordonet blir obrukbar vid en av angriparen vald tidpunkt.

Systemuppdateringar

Uppdateringar är nödvändiga både för att förbättra funktionaliteten och för att öka säkerheten för system. Säkerhetsuppdateringar behöver ske regelbundet och snabbt när de rör allvarliga sårbarheter, så att inte angripare hinner utnyttja sårbarheterna. Vid en cybersäkerhetsincident är det också viktigt att snabbt nå ut med uppdateringar för att täppa till sårbarheter så att inte vidare skada kan ske.

En uppdatering kan manipuleras av en angripare så att den ger oönskad förändrad funktion eller innehåller skadlig kod. Det är därför viktigt att kontrollera att uppdateringen kommer från en tillförlitlig källa och att den inte har manipulerats under leverans. Det är även viktigt att betrodd personal utför uppdateringarna.

På samma sätt som man för mekaniska system lagerför reservdelar, eller ser till att de kan ersättas med nytillverkade system, måste man ha ett livscykelperspektiv för mjukvaruuppdateringar, helst över hela fordonets planerade livslängd. Även de verktyg som behövs för uppdateringar behöver förvaltas under hela den tid fordonet ska nyttjas.

Rekommendationer

- Uppdatera kontinuerligt och skyndsamt fordonet och stödsystemen när det finns nya versioner av mjukvara eller säkerhetsuppdateringar. Det ska dock finnas en process för att identifiera och prioritera uppdateringar. Att bara uppdatera direkt är inte att rekommendera i kritisk verksamhet, utan varje uppdatering måste hanteras korrekt. Säkerställ att funktionaliteten inte påverkas negativt av uppdateringen. När uppdateringarna är gjorda ska de funktionstestas.
- Säkerställ att endast speciellt tillägnade servicedatorer, med gott grundskydd och rutiner för användning, används för att föra in uppdateringar i fordonet. Om servicedatorerna även används för annat, som exempelvis privat webbsurfning så ökar risken att skadlig kod smittar datorn.
- Genomför säkerhetsuppdateringar av operativsystem och andra programvaror samt uppdateringar av signaturer för antivirusprogram regelbundet på kringliggande system och servicedatorer. Uppdatera endast en dator i taget. Servicedatorer och verktyg kan i vissa fall vara lika kritiska som fordonet. Dessa måste då också skyddas.

- Överväg om trådlösa uppdateringar är nödvändiga eller om det är möjligt att installera dessa trådburet eller med portabelt lagringsmedia. Sker uppdateringarna av fordonet över en trådlös uppkoppling så kan detta ge en ökad exponering av fordonets system som en angripare kan försöka utnyttja. Oavsett vad som väljs ska uppdateringar ske över en säker kommunikationskanal.
- Se till att räddningstjänsten kan välja tidpunkt för trådlösa uppdateringar om sådana tillåts. På så vis undviks det att fordonet uppdateras så att det stör räddningstjänstens pågående verksamhet, exempelvis vid en utryckning.
- Se till att inte samtidigt uppdatera flera fordon av samma modell. Om flera fordon av samma modell uppdateras samtidigt så kan ett fel i en uppdatering exempelvis leda till att alla fordonen blir obrukbara. Genomför en funktionskontroll efter uppdatering av det första fordonet innan uppdatering av övriga fordon görs.
- Se till att det i avtalet framgår när leverantörens serviceavtal löper ut samt när säkerhetsuppdateringar inte längre kommer att tillhandahållas. Då kan man i tid hantera de risker detta innebär. Kravställ att fordonets huvudsakliga funktion inte ska äventyras när serviceavtal har löpt ut.
- Avtala att leverantörer vid upptäckt av sårbarheter skyndsamt informerar och levererar uppdateringar eller systemförändringar för att motverka sårbarheternas effekter.
- Uppdateringar till fordon eller kringliggande system bör levereras så att det går att upptäcka manipulation. Detta kan exempelvis göras genom att jämföra hashvärden för programvara före och efter leverans samt genom plombering av hårdvara. Ha en process för att kontrollera att manipulation inte skett innan uppdatering genomförs.

Exempel på risk

En servicetekniker ansluter trådburet till ett räddningsfordon för att se status på fordonet och för att utföra serviceuppdateringar till fordonets mjukvara. Förutom den trådburna anslutningen har servicedatorn även en trådlös internetanslutning. En angripare har genom en sårbarhet berett sig möjlighet till fjärrstyrning av servicedatorn och kan därmed föra över skadlig kod till fordonet när servicedatorn är inkopplad, exempelvis för att sätta fordonet eller någon av dess funktioner ur funktion.

Konfigurationsledning

Det krävs kunskap om vilka komponenter och programvaror som fordon och kringliggande system består av för att kunna förstå vilka risker och sårbarheter som finns. Det krävs även kunskap om vilka versioner av mjukvaror som används, då olika versioner av mjukvara har olika sårbarheter.

Ibland går det fort för en sårbarhet att bli känd och att angripare börjar använda den. För mjukvaruleverantörerna innebär detta en kapplöpning, där säkerhetsuppdateringar behöver levereras innan sårbarheten utnyttjas. Genom att organisationen håller reda på vilka versioner som finns kan organisationen snabbt bedöma viktiga sårbarheter som de är drabbade av och där de behöver arbeta för att snabbt installera säkerhetsuppdateringar eller vidta andra åtgärder i väntan på att uppdateringarna finns tillgängliga. Notera dock att även om en sårbarhet är allvarlig kanske den är svår att exploatera. Den kanske finns i en komponent som inte är direkt ansluten till yttervärlden eller något annat internt system och är därför inte nödvändigtvis tidskritisk att åtgärda.

Organisationen behöver föra logg över vad som uppdateras, samt vilken uppdatering och programversion som installeras. Loggen bör också innehålla när uppdateringen genomförs och av vem, för att hålla koll på att nödvändiga uppdateringar utförs. Icke-godkända förändringar kan då också lättare upptäckas.

Rekommendationer

- Gör en komplett sammanställning över räddningsfordonets hårdvara och mjukvara. Listan bör inkludera leverantörens namn, hårdvarans modell samt ingående mjukvaror och deras versioner.
- Håll en uppdaterad lista över vilka versioner och konfigurationer av hård- och mjukvara som används i fordonet eller i dess kringliggande system. Uppdatera listan när ändringar utförs.

Exempel på risk

En sårbarhet i en gammal version av en mjukvara i servicedatorn gör att en angripare lyckas föra in ett utpressningsvirus som krypterar alla filer på datorn. Olyckligtvis sprider den sig till flera av kommunens datorer som också blir krypterade.

Säker leveranskedja

Ett räddningsfordon byggs upp av ett stort antal elektronikkomponenter i grundfordonet, påbyggnaderna och extrautrustningen. Dessa komponenter tillverkas i sin tur av olika leverantörer, som ofta har underleverantörer i flera led. Det blir därför snabbt svårt att följa vilka aktörer som ingår i leveranskedjan. Det räcker att en enskild person hos en leverantör smyger in något skadligt i en produkt för att det ska kunna bli konsekvenser för fordonets drift och funktion. Vissa förändringar kan visserligen upptäckas i inspektioner och tester av produkter, men inte alla. Därför bör man försäkra sig om att leverantören uppfyller relevanta standarder för säkerhet och kvalitet, t.ex. ISO 9001 och att man kan säkerställa spårbarhet rörande produkter fram till installation i fordonet.

Rekommendationer

- Utvärdera fordonstillverkare, påbyggnadsleverantörer och leverantörer av extrautrustning ur ett lämplighetsperspektiv.
- Fastställ avtal och regler för samarbete med leverantörer. I dessa avtal bör det bland annat specificeras att leverantören ska skydda sina produktions- och utvecklingsmiljöer, hur leveranskontroll och informationsutbyte ska ske med avseende på cybersäkerhet samt hur snabbt säkerhetsuppdateringar ska levereras från det att sårbarheter upptäckts.
- Säkerställ att produkter under leverans inte kan manipuleras. Detta kan exempelvis ske genom att jämföra hashvärden för mjukvaran före och efter leverans och hårdvara kan plomberas före leverans.
- Både under fordonets utveckling och under påbyggnadsfasen (till brandbil) bör produktions- och utvecklingsmiljöer ha det skydd som krävs så att inga sårbarheter byggs in i fordonet.
- Vid utveckling av mjukvara bör en metodik för säker utveckling användas, exempelvis någon av metoderna från CIS, NIST, SAFECode, BSA eller OWASP.[4]

Utbildning

Cybersäkerheten för ett system är beroende av användarna och hur de använder systemet och funktionen i fråga. Detta gäller både räddningstjänstens personal och andra aktörer som interagerar med fordonet, exempelvis för service och underhåll. Det är därför viktigt att personalen förstår cybersäkerheten och vilka konsekvenser ett bristande cybersäkerhetsarbete kan få för räddningstjänsten. För att göra rätt behöver organisationen utbilda personalen i informationssäkerhet och i de rutiner för detta som finns inom räddningstjänsten. Dessutom är det relevant att utbilda berörd personal i specifika rutiner för cybersäkerhet gällande räddningsfordonet. Utbildning leder till en ökad kunskap vilket i sin tur minskar riskerna för hand-havandefel som kan äventyra cybersäkerheten.

Det är även viktigt att utbildningarna är anpassade för den personalkategori som utbildas. Exempelvis behöver en brandman förstå hur denne ska hantera system och komponenter i fordonet medan en tekniker behöver djupare kunskap om hur systemen fungerar och hur de bör hanteras samt om rutiner och system för exempelvis service och uppdatering.

[4] Center for Internet Security Critical Security Controls (CIS),
National Institute of Standards and Technology Secure Software Development Framework (NIST),
Software Assurance Forum for Excellence in Code (SAFECode),
Software Alliance BSA Framework for Secure Software,
Open Web Application Security Project (OWASP).

Rekommendationer

- Ta fram policyer och rutiner för cybersäkerhet i verksamhetens användning, för användare av systemen och för drift och underhåll av räddningsfordon och dess kringliggande system.
- Utbilda personalen i rutiner för cybersäkerhet vid användning, drift och underhåll av fordon och dess kringliggande system. Utbildningen bör även ta upp vilka konsekvenser ett felaktigt eller oaktsamt användande kan få.
- Kravställ att leverantör av grundfordon och installatörer av påbyggnader och extrautrustning tar fram en utbildning för hur dessa ska användas och underhållas för att upprätthålla en hög cybersäkerhet. Utbildningen bör även ta upp vilka konsekvenser ett felaktigt eller oaktsamt användande kan få.

Tekniska rekommendationer

I följande avsnitt presenteras vägledningens tekniska rekommendationer för att öka cybersäkerheten i tunga räddningsfordon. Här beskrivs fem områden med rekommendationer. För varje område ges en beskrivning av området, exempel på möjliga risker samt specifika rekommendationer.

Rekommendationerna baseras på de intervjuer som genomförts med fordonstillverkare, påbyggnadsleverantörer och räddningstjänsten.

Kapitlet innehåller tekniska rekommendationer inom följande områden:

- begränsning av funktion och komplexitet
- trådlös kommunikation
- separation av kommunikation inom fordonet
- fysisk säkerhet
- nödkörning.

Begränsning av funktion och komplexitet

Ökad funktionalitet innebär inte alltid högre produktivitet eller prestanda. Ökad funktionalitet leder ofta till ökad komplexitet för användaren, vilket i sin tur ökar risken för handhavandefel. Dessutom innebär ett större antal funktioner att produkten i sig blir mer komplex, vilket medför en ökad risk för sårbarheter, problem eller fel. Notera att ökad användning av mjukvara kan förlänga uppstartstiden för fordonet.

Rekommendationer

- Utrusta bara räddningsfordonen med funktioner och extrautrustning som är nödvändiga för verksamhetens behov. På så vis begränsas komplexiteten och därmed cybersäkerhetsriskerna.

Exempel på risk

Räddningstjänsten upphandlar ett räddningsfordon med pekskärmar för att styra diverse påbyggnadsfunktioner. Det visar sig att dessa pekskärmar har extern kommunikation för uppdatering. En angripare utnyttjar detta och lyckas få in en skadlig uppdatering som blockerar funktionen hos pekskärmen, vilket leder till att den funktion pekskärmen styr inte längre är tillgänglig. Som tur var gick funktionen att nödköra, men det kostade dyrbar tid.

Trådlös kommunikation

Räddningsfordon kan använda trådlös kommunikation för att förenkla, förbättra och snabba på räddningsarbetet. Trådlös kommunikation kan även användas för andra syften, som exempelvis att uppdatera eller diagnostisera fordonet eller dess funktioner på distans.

Trådlös kommunikation medför ökad exponering, som angripare kan utnyttja för att komma åt fordonets olika system. Det kan medföra en rad olika konsekvenser beroende på hur fordonets interna system ser ut. Om en angripare kan komma åt kritiska funktioner i fordonet kan angreppet ge konsekvenser för personsäkerhet och räddningsverksamhet. På grund av risken för externa angrepp är det mycket relevant att begränsa antalet trådlösa kommunikationslänkar från räddningsfordonet och bara inkludera dem som bedöms som absolut nödvändiga.

Vid höjd beredskap kan trådlösa uppkopplingar användas för att spåra räddningsfordonet i syfte att kinetiskt bekämpa det. Vid höjd beredskap eller användning i främmande land har trådlös kommunikation sannolikt lägre tillgänglighet. Det är därför viktigt att ha kännedom om alla kommunikationsberoenden, exempelvis om fordonet riskerar att försättas i halta-hem-läge vid interndiagnostik som inte får kontakt med chassitillverkarens FMS. Ett annat exempel är att en funktion stängs av om komponenten inte får kontakt med en licens- eller abonnemangsserver.

TSFS 2016:22 – undantag från beskaffenhetskrav

I Transportstyrelsens föreskrifter (TSFS 2016:22) och allmänna råd om bilar och släpvagnar som dras av bilar undantogs bilar som används av Försvarsmakten, Försvarets materielverk och Försvarets radioanstalt från beskaffenhetskraven, då ett inbyggt spårnings- och kommunikationssystem i fordonen (exempelvis e-Call), som inte är under egen kontroll eller säkerhetsklassat, innebär en mycket stor begränsning för den verksamhet som bedrivs på dessa myndigheter.[5]

Rekommendationer

- Fordonet ska vid behov kunna framföras utan aktiva trådlösa anslutningar, till exempel till ett FMS. Detta läge ska kunna aktiveras lokalt.
- Håll trådlösa kommunikationslänkar till ett minimum. Skriv för varje trådlös kommunikationslänk en motivering som beskriver varför anslutningen är nödvändig.
- Begränsa trådlösa anslutningar mot fordonet för att minska exponeringen. Exempelvis kan endast godkända användare och kringliggande system få ansluta.
- Skydda konfidentiell och kritisk datakommunikation över trådlösa länkar genom att använda krypteringsskydd. På så vis skyddas kommunikationen mot obehörig avlyssning och manipulation.

[5] https://www.transportstyrelsen.se/globalassets/global/regler/remisser/vagtrafik/tsf-2022-137/remissmissiv.pdf.

Exempel på risk

En påbyggnadsleverantör har installerat ett påbyggnadssystem med trådlös kommunikation för att skicka diagnostikinformation och för uppdateringar. En angripare utnyttjar den externa länken för att kommunicera med påbyggnadssystemet. Angriparen lyckas föra över skadlig kod som gör påbyggnadssystemet obrukbart.

Separation av kommunikation inom fordonet

Med separation menas en mjukvaruavgränsning, eller fysisk avgränsning mellan olika enheter eller grupper av enheter. Genom att separera enheter i fordonet minskas risken att en angripen enhet kan påverka andra delar av fordonet.

Fordonstillverkare tillhandahåller anvisningar för hur anslutningar till det interna kommunikationsnätverket får göras och vilka fysiska krav som påbyggnader måste uppfylla. Exempelvis måste alla ombyggnationer och påbyggnationer som inte finns beskrivna i Scanias påbyggnadsinstruktioner godkännas av en auktoriserad representant hos Scanias återförsäljare. Alla tänkbara anslutningar eller påbyggnationer specificeras dock inte i sådana instruktioner. Det är därför viktigt att ha en dialog med grundfordonets tillverkare angående påbyggnationens anslutningar.

Rekommendationer

- Påbyggnader och extrautrustning ska endast använda för ändamålet typgodkända interface av grundfordon. För varje påbyggnad eller extrautrustning som är ansluten direkt till fordonets interna kommunikationsnätverk ska en motivering skrivas som förklarar varför anslutningen är nödvändig och hur den är gjord. Dessutom ska anslutningen analyseras så att eventuell påverkan på fordonets cybersäkerhet, typgodkännande eller liknande är känd.
- Anslut inte påbyggnadsutrustning och extrautrustning som har trådlösa kommunikationsgränssnitt till annan utrustning om det inte är nödvändigt.
- Anslut inte påbyggnader och utrustning som har trådlösa kommunikationsgränssnitt till sådana påbyggnader och extrautrustning som bär konfidentiell information. På så vis minskar sannolikheten att konfidentiell information läcker ut.

Exempel på risk

En påbyggnadsleverantör har installerat ett påbyggnadssystem som är kopplat direkt till fordonets interna kommunikationsnätverk. En insider eller obehörig användare uppdaterar mjukvaran i påbyggnadssystemet, som i sin tur påverkar fordonet så att fordonet blir obrukbart när en extraordinär händelse inträffar.

Exempel på risk

En brandman ansluter sin mobiltelefon till räddningsfordonets USB-kontakt för el då telefonen börjar få slut på laddning. Dessvärre finns skadlig kod på telefonen som förs över till fordonets infotainmentsystem. Infotainmentsystemet har otillräcklig separation till det interna kommunikationsnätverket, vilket resulterar i att den skadliga koden kan kommunicera med andra enheter i fordonet och därmed påverka kritiska fordonsfunktioner.

Fysisk säkerhet

Om en angripare har fysisk tillgång till fordonet har angriparen stora möjligheter att manipulera eller orsaka skada. Därför är det även viktigt att begränsa den fysiska tillgången till fordonens system.

På räddningsfordon finns vanligen jalusiförsedda skåp som innehåller utrustning som verktyg, slangar och pumpar. På grund av tillgänglighetskrav är dessa jalusier olåsta, vilket kan utnyttjas av en angripare. Det är därför viktigt att inte exponera datakommunikationskablage eller fysiska gränssnitt i dessa skåp eller på andra enkelt nåbara ställen.

Rekommendationer

- Skydda kablage och portar för datakommunikation mot otillåten tillgång från fordonets utsida, från fordonets hytt samt bakom jalusier. På så vis försvåras åtkomsten för angripare.
- Portar som är åtkomliga från fordonets hytt ska förses med envägs-USB (för elladdning) eller endast tillåta att godkänd utrustning ansluts.
- Inför inbrottslarm för jalusier som innesluter kablage för datakommunikation. Larmen ska aktiveras när hytten låses. Inför dessutom en funktion som i hytten visar om en jalusi är öppen.

Exempel på risk

Räddningsfordonet står obevakat på tomgång under en räddningsinsats, vilket leder till att en angripare kan arbeta ostört vid fordonet. Angriparen ansluter sin laptop till ett fysiskt gränssnitt på en av påbyggnaderna och för över skadlig kod. När brandmännen senare återvänder till fordonet för att köra iväg har påbyggnadsfunktioner slutat fungera.

Nödkörning

Vissa delar av räddningssystemen är kritiska för att den livräddande verksamheten ska kunna upprätthållas. Om normala funktioner för styrning av sådana system-delar slutar fungera behövs det därför alternativa styrningsfunktioner. Sådana alternativa sätt för styrning benämns nödkörning.

Rekommendationer

Säkerställ att

- nödkörning finns för kritiska funktioner i fordonet
- nödkörning är oberoende av ordinarie system
- instruktioner för nödkörning finns tillgängliga
- verksamheten övar på nödkörning.

Exempel på risk

Brandmännen åker ut till en befarad brand i ett bostadshus. Dessvärre har släck-systemet slutat fungera på grund av en hackerattack. Brandmännen tvingas skicka in ett annat räddningsfordon, vilket tar värdefull tid som gör att branden utvecklas och huset brinner ner till grunden. Nödkörning av släcksystemet genom en annan metod hade kunnat vara behjälpligt i denna situation.

Teknisk fördjupning

Detta kapitel presenterar en teknisk fördjupning av fordonets interna kommunikationsnätverk och de protokoll som används i fordon. Syftet är att ge en grundläggande förståelse för hur framför allt tunga fordon är uppbyggda. Beskrivningarna bidrar till att det blir enklare att förstå de hot, risker och möjliga angrepp som beskrivs i vägledningen.

Fordon består idag av en mängd olika kommunicerande elektroniska styrenheter, snarare än strikt mekaniska eller elektromekaniska funktioner som det var förr. Dagens kommunicerande elektroniska styrenheter benämns vanligen ECU, efter engelskans Electronic Control Unit. De operativsystem som används för denna typ av enheter är vanligen mycket enkla och är designade för att vara driftsäkra, men ofta utan att ta höjd för cybersäkerhetsaspekter. Styrenheterna hanterar mer eller mindre hela fordonets funktion, från styrning och framförande till underhållning och komfort. För att dessa styrenheter ska fungera korrekt krävs kommunikationskanaler mellan dem i fordonet. Den interna kommunikationen mellan personbilars styrenheter går ofta via en central nätsluss (eng. gateway). Det kan förenkla segmentering av nätverket, avgränsningar som till exempel minskar risken för spridning av skadlig kod. Tunga lastbilar har däremot ofta plattare arkitekturer, utan centrala nätslussar för segmentering.[6] Däremot implementeras i regel en nätsluss mellan fordonschassit och eventuella påbyggnadsgränssnitt. Utvecklingen går dock allt mer mot centrala arkitekturer med fler nätslussar för att förenkla segmentering.

Fordon använder olika protokoll för kommunikation mellan olika delkomponenter i det interna kommunikationsnätverket. För kritiska delkomponenter baseras vanligen lågnivåkommunikationen på standarden ISO11898 för CAN (Controller Area Network). Standarden definierar hur enheter i kommunikationsnätverket ska kommunicera på datalänklagret[7]. För CAN sker detta med broadcast, vilket betyder att alla mottagare ser alla paket och själva väljer vilken trafik de lyssnar på och vilken de ignorerar. Ett alternativ till CAN är FlexRay, som också används för lågnivåkommunikation mellan kritiska delsystem inom det interna kommunikationsnätverket i fordon. FlexRay är designat för att vara snabbare och mer pålitligt än CAN, men har inte fått stort genomslag. I dagsläget används FlexRay bara som ett komplement i säkerhetskritiska delsystem av fordon som kräver realtidskommunikation och redundans.

För att kommunicera över CAN krävs ett högnivåprotokoll som fastställer hur paketens innehåll ska tolkas och hur kommunikationen struktureras. På denna nivå skiljer sig tunga fordon och personfordon åt. Tunga fordon följer vanligen standarden SAE J1939, som definierar högnivåprotokoll över CAN. Personfordon använder istället vanligen tillverkarspecifika högnivåprotokoll. Tunga fordon kan också använda tillverkarspecifika högnivåprotokoll, men det görs vanligtvis bara för isolerade delsystem. Jämfört med tillverkarspecifika högnivåprotokoll kan J1939

[6] Valassi, C och Karressand, M. (2020). Cyberfysiska sårbarheter i tunga fordon – Med inriktning mot tunga fordon av vikt för civilförsvaret. FOI-R--5067—SE.
[7] Se OSI-modellen.

vara mer lättillgänglig för möjliga angripare, eftersom det finns större möjlighet för insyn i protokollets funktion och uppbyggnad. Det förenklar möjliga angrepp mot utrustning som följer J1939. Samtidigt innebär den större insynen att fler kan granska standarden i syfte att upptäcka sårbarheter.

Utöver CAN-baserad kommunikation finns det även andra kommunikations-protokoll i fordonen, exempelvis local interconnect network (LIN) och media oriented systems transport (MOST). Dessa används i första hand för icke-kritiska system och har stora likheter mellan olika fordonstyper.

LIN är ett seriellt nätverksprotokoll med relativt låg dataöverföringskapacitet. Protokollet är framtaget för användning i delar av fordon med lägre krav på robusthet och prestanda. LIN används därför i icke-kritiska delsystem som inte kräver överföring av större mängder data, som elektroniskt styrda backspeglar, säten och klimatsystem samt för diverse funktionsknappar på ratten.

MOST är ett multimediaprotokoll som används för video, ljud och liknande data-signaler i fordon. Protokollet har en relativt hög överföringshastighet och lämpar sig därför väl för hantering av media. Protokollet är även anpassningsbart och har plug-and-play-integration som underlättar.

I takt med att fordon utrustas med allt fler avancerade funktioner för förarassistans ökar också kraven på bandbredd för kommunikation inom fordon. Ethernet är därför ett protokoll som börjar användas mer och mer i fordonsindustrin.

Referenser

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Schacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. I USENIX Security Symposium, vol. 4, s. 447–462.

Gustafsson, T. och Valassi, C. (2018). NCS3 – Kartläggning av elektroniska styrsystem i tunga fordon. FOI Memo 6358.

ISO 21434:2021 Road Vehicles – Cybersecurity engineering.

ISO 27000-serien.

Jonson, U. (2018). Heavy Vehicle Cybersecurity Program (presentation vid Auto-ISAC Monthly Community Call 2018-04-04). https://www.automotiveisac.com/wp-content/uploads/2018/05/03_29_18_Auto-ISAC-April-4-Community-Call-_FINAL.pdf [2021-12-17].

Kennedy, J., Holt, T., & Cheng, B. (2019). Automative cybersecurity: accessing a new platform for cybercrime and malicious hacking. I Journal of Crime and Justice, 42:5, 632–645. DOI: https://doi.org/10.1080/0735648X.2019.1692425.

Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015, 91.

Mukherjee, S., Van Etten, J. C., Samyukta, N. R., Walker, J., Ray, I., och Ray, I. (2019). TruckSTM: Runtime Realization of Operational State Transitions for Medium and Heavy Duty Vehicles. I ACM Transitions on Cyber-Physical Systems Vol. 4, Nr. 1, Artikel 4. Oktober.

Norte, J., K. (2016) Hacking industrial vehicles from the internet. http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html.

Scania (2021). Användning och ansvar. https://til.scania.com/groups/bwd/documents/bwm/mdaw/mdaw/~edisp/064094.pdf [2021-12-17].

Stachowski, S., Bielawski, R., och Weimerskirch, A. (2018). Cybersecurity Research Considerations for Heavy Vehicles. DOT HS 812 636. Washington, DC: National Highway Traffic Safety Administration (NHTSA).

Svensk Författningssamling (SFS)(2001). Lag (2001:559) om vägtrafikdefinitioner.

Tollefson, R. (2019). As the connectivity of trucking fleets grows, so do cybersecurity risks. Infosec. https://resources.infosecinstitute.com/topic/as-the-connectivity-of-trucking-fleets-grows-so-do-cybersecurity-risks/ [2021-12-17].

Valassi, C och Karressand, M. (2020). Cyberfysiska sårbarheter i tunga fordon – Med inriktning mot tunga fordon av vikt för civilförsvaret. FOI-R--5067—SE.

Vard Antinyan (2020). Revealing the complexity of automotive software. Proceedings of the 28th ACM Joint Meeting on European Software Engineering, Conference and Symposium on the Foundations of Software Engineering.

Weimerskirch, A., Becker, S., och Hass, B. (2017) Commercial Vehicle vs. Automotive Cybersecurity – Commonalities & Differences. http://www.weimerskirch.org/files/WeimerskirchBeckerHass_CommercialVehicleVsAutomotiveCybersecurity.pdf [2020-11-10].

Fler lästips

Här finns ytterligare stöd:

- Metodstöd för LIS – Informationssäkerhet.se (https://www.informationssakerhet.se/metodstodet/)
- Upphandla informationssäkert – en vägledning från MSB (https://rib.msb.se/filer/pdf/28742.pdf)
- Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarsmakten, och Säkerhetspolisen har tillsammans upprättat ett nationellt cybersäkerhetscenter, inom vilket myndigheterna bland annat ska förmedla råd och stöd avseende hot, sårbarheter och risker. Nationellt cybersäkerhetscenter (https://www.ncsc.se/).

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

FOI

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2122 - januari 2023 ISBN 978-91-7927-330-9