Faktablad

Avdelningen för cybersäkerhet och säkra kommunikationer

Publ.nr MSB1522 – mars 2020

Informationssystem för transport av farligt gods – en hotanalys

Arbetsgruppen WG Telematics inom FN:s ekonomiska kommission för Europa (UNECE) har tagit fram ett förslag på ett för Europa gemensamt informationssystem för information om transporter av farligt gods. Detta faktablad syftar till att ge intressenter kunskap om informationssystemet, samt en säkerhetsanalys av densamma. Analysen har genomförts på ett preliminärt förslag, det har i dock inte antagits några förändringar vilka påverkar säkerhetsanalysen i sak. Notera även att enbart logiska hot mot informationssystemet har analyserats, och ej fysiska hot mot transport eller IT-system.

Systembeskrivning

Ett gemensamt informationssystem är tänkt att möjliggöra elektronisk överföring av godstransportinformation. Detta får som följd av information aggregeras för att förenkla kartläggningen av transporter av farligt gods. Den förenklade kartläggningen gäller även för obehöriga och antagonister, vilket medför ökad exponering och behov av säkerhetskrav på informationssystemet.

Det gemensamma systemet har två huvudkomponenter: Trusted Party 1 (TP1) och Trusted Party 2 (TP2). TP1 är en nationell resurs som förmedlar information. TP2 är systemet som ägs eller används för att lagra information. Det kan inte utifrån det analyserade förslaget uteslutas att fordon kommer att kunna kontinuerligt skicka information under den aktiva transporten. För att möta de säkerhetskrav som uppstår föreslås ömsesidig autentisering mellan alla noder som huvudsaklig teknisk säkerhetsfunktion.

En ömsesidig autentisering innebär att TP2:or och myndighetsaktörer måste skicka sina certifikat till den TP1:a de är anslutna till. Nytillkomna TP1:or måste skicka sina certifikat till samtliga TP1:or på TP1 Trusted List.

Farligt gods

Avser huvudsakligen gods med för omgivningen farliga egenskaper, exempelvis explosivt eller radioaktivt. Vad som utgör farligt gods definieras i *Lag 2006:263* om transport av farligt gods.

Transport av farligt gods är internationellt reglerad och gäller även vid tid inrikes transporter. Reglerna kräver dokumentation vilken ska kunna uppvisas vid tillsyn och vara tillgänglig i händelse av en olycka.

Informationssystemet

Säkerhetsanalysen har genomförts på ett preliminärt förslag, vilket definieras av *Memorandum of Understanding* (MoU) vilket framarbetats av UNECE. Detta förslag har under 2019 reviderats och bilagts UNECE.

Idag går förslaget under beteckningen: **Guidelines for the use of 5.4.0.2 in RIN/ADR/ADN**.

Aktörer vid transport

Utöver de aktörer som hanterar gods vid exempelvis packning, lastning och lossning finns

- **Avsändaren** är den part som vill få det farliga godset transporterat
- **Mottagare** är den som är mottagare av gods.
- **Transportör** är den som expedierar transport. Kan vara allt från mindre åkeri till kedja av speditörer, åkerier och förare.

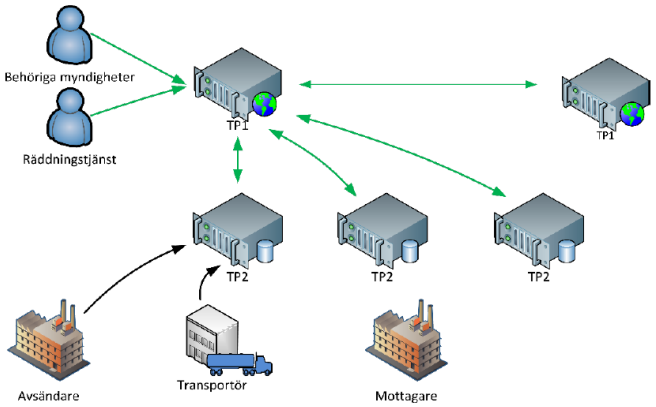
Hela studien
Hotanalys av ett informationssystem för transport av farligt gods

Rapportnr: MSB 2018-10654, finns att tillgå via www.msb.se

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap

En översikt av informationssystemet återges i figuren nedan.



De gröna pilarna ovan indikerar vilka kanaler som är upprättade med ömsesidig autentisering. Kommunikationen mellan TP1:or och dess registrerade parter sker över HTTPS. Det innebär att en krypterad kanal mellan autentiserade parter upprättas innan innehållet kommuniceras.

Säkerhetsanalysens slutsats

Det fastslås i säkerhetsanalysen att det i förslaget saknas information kring viktiga områden som kan påverka informationssäkerhet i det föreslagna systemet.

- Förslaget specificerar inte hur revokering av certifikat ska hanteras. Specifikation för revokering bör finnas på plats redan i den initiala fasen av planeringsarbetet. Att implementera funktionalitet i efterhand kan vara komplicerat.

- I förslaget framgår inga krav på hur kommunikation mellan TP2:an och dess underliggande system (avsändare, transportör och mottagare) ska hanteras. För att it-säkerhet ska kunna upprätthållas i ett gemensamt informationssystem bör kravställningen behandla hela TP2:ans funktionalitet, samt dess underliggande system.

- Det är i förslaget otydligt vilken funktionalitet en terminal i ett fordon ska ha. Dessa enheter kommer att ha störst exponering, och dess funktionalitet bör tydliggöras. Är funktionaliteten otydlig är det svårt att specificera och inkludera säkerhetsmässiga grundkrav för terminalerna.

Avslutningsvis, till följd av avsaknaden av information kring ovan områden anses förslaget inte täcka in alla viktiga säkerhetsaspekter. Det är därmed svårt att avgöra huruvida systemet är adekvat eller inte för tänkta intressenter.

Trusted party 1

Part vilken för register över aktuella transporter. Deras primära funktion är att ta emot och förmedla svar. Här lagras följande data:

- Chassinummer för vägfordon
- BIC-kod för containers
- Registreringsnummer för dragfordon och dess släp, samt ENI- och UIC-nummer
- Transportens status
- Fordonstyp

Trusted party 2

Här sker den huvudsakliga datalagringen. TP2:an ansluter till en TP1:a och svarar på frågor från denna. Här lagras information från deklaration av farligt gods samt statusuppdateringar från transportören.

Digitala certifikat

Används för att verifiera motpartens identitet. Digitala certifikat används för att koppla publik nyckel till en identitet. Denna koppling säkerställs och signeras av en tredje part.

Det finns ingen given standard för hur certifikat ska se ut eller hanteras. Dock är ITU-standarden X.509 mycket vanlig och används exempelvis *i Transport Layer Security* (TLS).

Revokering av certifikat

Vid behov att avsluta certifikat krävs att det att denna ogiltigförklaras – revokera certifikat.

Vilket innebär att certifikatet sätts upp på en lista mot vilken ett certifikats giltighet kan verifieras. Revokeringslistor hanteras oftast av en så kallad Certification Authority (CA), vilket är den enhet som utfärdat certifikatet.

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

MSB Myndigheten för samhällsskydd och beredskap