ISSN 0354-9852
Pregledni rad
Overview paper

UDK 004.738.5:351.083.8
DOI 10.7251/AKT1636003K
COBISS.RS-ID 6278168

ZAŠTITA PODATAKA U GLOBALNOM LANCU SNABDEVANJA - PRIMENA SMART CM PLATFORME

DATA PROTECTION IN THE GLOBAL SUPPLY CHAIN - SMART CM PLATFORM APPLICATION

Tanja Kaurin[1], Milorad Kilibarda[2]

Sažetak

Globalni lanac snabdevanja obuhvata veliki broj učesnika, kao što su proizvođači, distributeri, logističke i transportne kompanije, brodari, granični terminali, carina i sl. Uspešno povezivanje svih učesnika u jedan sinhronizovan lanac nije moguće bez informacionih tokova, koji obezbeđuju efikasan protok informacija na različitim nivoima. Učesnici uglavnom imaju sopstvene informacione sisteme, a istovremeno su sastavni delovi različitih infomracionih i komunikacionih mreža na globalnom nivou. U takvim uslovima poslovanja od ključnog značaja je bezbednost informacija. Ovaj rad se upravo bavi problematikom zaštite podataka u globalnom lancu otpreme i isporuke kontejnera. Prvo su sagledani zahtevi kao što su: transparetnost, bezbednost, pouzdanost, pravovremenost, ekonomičnost, i efikasnost u lancu snabdevanja, a zatim je predloženo rešenje koje se zasniva na SMART CM platformi. Predstavljena je funkcionalna arhitektura platforme, ključni scenariji za uspešnu primenu i modeli funkcionisanja kroz određene blokove i slojeve. Definisani su formati poruka i izvori informacija. Na kraju su predstavljene mogućnosti i ograničenja primene platforme sa stanoviša najvažnijih učesnika u lancu otpreme i isporuke kontejnera.

Ključne reči: *Zaštita podataka, bezbednost informacija, lanac snabdevanja, SMART CM platforma*
JEL klasifikacija:L91

1 *Fakultet za pravne i poslovne studije dr Lazar Vrkatić, Novi Sad, tanja.kaurin@useens.net*
2 *Saobraćajni fakultet Univerziteta u Beogradu, miloradkilibarda@gmail.com*

UVOD

Globalni lanac snabdevanja je izuzetno složen, dinamičan i ranjiv na mnoštvo pretnji, rizika i opasnosti. Broj učesnika u lancu se svakodnevno povećava i od suštinske je važnosti obezbediti nesmetano i pouzdano snabdevanje privrede i krajnjih potrošača. Bezbednost globalnog lanca snabdevanja je preduslov za efikasno povezivanje tržišta i olakšanu međunarodnu trgovinu. Međutim, često se u lancima snabdevanja velika pažnja usmerava na brzinu izvršavanja operacija, što može otežati praćenje bezbednosti. Teško je osigurati isti nivo bezbednosti u svakom njegovom segmentu. Sistem za upravljanje bezbednošću lanca snabdevanja kombinuje tradicionalne načine upravljanja lancem snabdevanja sa merama bezbednosti, što omogućava kompanijama da zaštite svoje poslovanje od pretnji kao što su piraterija, terorizam i krađe. Antagonističke pretnje, drugi rizici i neizvesnosti mogu biti namerno izazvane, nezakonite i neprijateljske. Neophodno je uložiti značajne napore za uspostavljanje bezbednog lanca, kako bi se pretnje, rizici i opasnosti sveli na najmanju moguću meru. Svi uključeni u procese isporuke moraju biti dosledni i veoma ozbiljno shvatiti problem sigurnosti, dok pokušavaju da robu isporuče na vreme. Neophodan je interdisciplinarni pristup bezbednosti, koji uključuje dobro definisane protokole, razumevanje svetskih propisa, obuku zaposlenih, mere fizičkog obezbeđenja, temeljnu proveru različitih učesnika, video nadzor skladišta, utovara i istovara tereta, kao i korišćenje sigurnih objekata. Za one koji se bave ovim problemima postoje dva cilja: prvi je da se promoviše efikasno i bezbedno kretanje robe, a drugi je da se podstakne globalni lanac snabdevanja koji je pripremljen, može da izdrži sve veće pretnje, opasnosti i brzo se oporavi od poremećaja. Potrebno je razumeti i rešiti pretnje na početku procesa i ojačati bezbednost fizičke infrastrukture, prevoznih sredstava i informacija, uz maksimiziranje trgovine kroz modernizaciju infrastrukture u procesima.

U prošlosti su logističke kompanije i drugi učesnici u lancu snabdevanja uglavnom bili usmereni na povećavanje sigurnosti obavljanja logističkih operacija u fizičkom okruženju, ali poslednja istraživanja nesumnjivo ukazuju na sve veće opasnosti u virtuelnom okruženju. Neophodno je više pažnje posvetiti rizicima i pretnjama u informacionim tokovima i sistemima. Opravdano se očekuje da sigurnost informacija i podataka, postane ključna za bezbednost lanaca snabdevanja[3].

To je i bio osnovni motiv pisanja ovog rada, gde su autori pokušali da sagledaju različite aspekte vezane za vidljivost lanca snabdevanja, bezbednost informacija i zaštitu podataka u lancu snabdevanja. Nakon sporvedene

3 R. Banomyong. 2005. *"The Impact of Port and Trade Security Initiatives on Maritime Supply-Chain Management"*. Pra Chan Road, Thammasat Business School, Thammasat University, Bangkok 10200, Thailand. Marit.Pol.MGMT, January-March 2005, Vol 32, No1, 3-13

analize, u radu je prestavljena SMART CM platforma za protok i zaštitu podatka u globalnom kontejnerskom lancu snabdevanja.

VIDLJIVOST LANCA SNABDEVANJA

Vidljivost lanca snabdevanja je sposobnost da se proizvodi u toku isporuke prate od proizvođača do krajnjeg odredišta. Cilj je poboljšati i ojačati lanac snabdevanja tako da podaci budu dostupni svim zainteresovanim stranama, uključujući i kupca. Može se reći da vidljivost lanca snabdevanja predstavlja snimanje i integraciju podataka, kreiranje inteligencije i donošenje odluka baziranih na promenama tri funkcionalna toka (materijal, kapital i informacije) u lancu snabdevanja zajedno sa relevantnim zahtevima za očuvanje životne sredine[45]. Međutim, kompanije se često suočavaju sa problemima kao što su: gubljenje vremena zbog ručnog zakazivanja isporuka i praćenja proizvoda od kanala do kanala; propuštene prilike jer se ne zna količina robe u tranzitu i raspoloživost zaliha; poremećeni odnosi nakon isporuke jer pošiljka ne stiže na vreme. Zajednički element svih ovih problema je nedostatak vidljivosti, odnosno sposobnosti da se vide podaci o proizvodima u realnom vremenu. Mnoge kompanije brzo su reagovale i u proteklih nekoliko godina, shvatajući da vidljivost nije samo želja već nesto što se mora obezbediti. Unapređenjem vidljivosti u lancu snabdevanja postižu se konkretni ciljevi, kao što su: smanjenje broja operacija i rizika, poboljšanje vremena isporuke i pravovremena identifikacija nedostataka ili lošeg kvaliteta duž lanca snabdevanja[6].

U većini organizacija informacije su projektovane tako da služe svrsi pojedinih odeljenja u organizaciji umesto da se koriste u celom lancu snabdevanja. Tako na primer, odeljenje prodaje ima svoje projekcije i budžet, proizvodnja ima svoj raspored proizvodnje, a kupci i dobavljači imaju svoje baze podataka, koje obično ne dele sa drugim učesnicima u lancu. Cilj poboljšanja vidljivosti lanca snabdevanja jeste obezbediti kontrolisan pristup i transparentnost kako bi se osigurali tačni i blagovremeni podaci i relevantne informacije duž celog lanca[7].

Vidljvost informacija je proces deljenja kritičnih podataka koji su potrebni za upravljanje protokom proizvoda, usluga i informacija u realnom vremenu između dobavljača i kupaca. Ako je informacija dostupna, ali joj ne mogu pristupiti učesnici koji treba da reaguju na datu situaciju njena vrednost se eksponencijalno smanjuje. Povećanje informacione vidljivosti u lancu snabdevanja omogućava rast prihoda, iskorišćenost sredstava i smanjenje

4 ttp://searchmanufacturingerp.techtarget.com/definition/supply-chain-visibility-
5 http://www.gtnexus.com/solutions/supply-chain-visibility
6 http://www.mepsupplychain.org/supply-chain-visibility/
7 Handfield R., *Creating Information Visibility in the Chain*, 2002.

troškova. Kako bi se povećala odgovornost u lancima snabdevanja kompanije razmatraju upotrebu zajedničkih modela koji dele informacije na različitim nivoima svih učesnika – od dobavljača svojih dobavljača do kupaca svojih kupaca. Ovi trgovinski partneri treba da dele prognoze, upravljanje zalihama, rasporede rada, optimiziraju isporuke i na taj način smanje troškove, povećaju produktivnost i stvore veću vrednost za krajnjeg kupca u lancu. Tradicionalni lanci snabdevanja se brzo razvijaju u „dinamičke poslovne mreže" koje se sastoje od grupe nezavisnih poslovnih jedinica koje dele informacije o planiranju i izvršenju logističkih operacija, kako bi se zadovoljili zahtevi korisnika[8].

Neki od razloga koji moraju biti uzeti u obzir prilikom implementacije informacionog sistema uključuju veličinu baze podataka o dobavljačima i kupcima sa kojima se razmenjuju informacije, kriterijume za unapređenje vidljivosti, strukturu podataka koji se dele i tehnologiju koja se koristi, što omogućava svim učesnicima da imaju pristup informacijama neophodnim za efikasno kontrolisanje protoka materijala, upravljanje zalihama, da ispune uslove iz ugovora i ispoštuju potrebne standarde kvaliteta.

Jedan od koncepata koji se često pominje u poslednje vreme jeste koncept „kontrolnog tornja lanca snabdevanja". Kontrolni toranj daje ključne podatke na raspolaganje partnerima u lancu snabdevanja kako bi se olakšala koordinacija zahteva kupaca i odgovora dobavljača. Kako bi se dostupni podaci transformisali u korisne informacije neophodan je razvoj u tri oblasti:

- Procesi – Procesi treba da postanu zajednički, sa razmenom podataka i saradnjom između odeljenja ali i između organizacija. Koordinacija projekcija prodaje i lanca snabdevanja može da pomogne dobavljačima da predvide buduće potrebe. Kompanije treba da razviju podatke koji mogu da se dele između partnera da bi bilo moguće planiranje potražnje. Takođe treba realizovati upravljanje rizicima kako bi se smanjila mogućnost prekida lanca snabdevanja.
- Povezanost (veze) – Informacije se moraju deliti između procesa, različitih poslovnih funkcija i izvan kompanije pružajući svim učesnicima realan uvid u procese. Saradnja je neophodna i za povećanje nivoa poverenja između partnera.
- Tehnologija – Glavni izazov u razmeni informacija jeste problem prenosa podataka između različitih informacionih sistema. Inovacije kao što su cloud computing, baze podataka i različiti softveri danas čine kontrolni toranj mogućim. Jednom kada se podaci dizajniraju tako da pruže učesnicima sve potrebne informacije kasnije se mogu koristiti za različi-

8 Kaurin T., Kilibarda M., *Informacione i komunikacione tehnologije u globalnim lancima snabdevanja,* Treća međunarodna naučna konferencija Evropska unija – izazovi proširenja i Zapadni Balkan, Banja Luka 2016.

te analize i planiranja. Kontrolni toranj omogućava kompanijama da precizinije upravljaju tražnjom kako bi smanjile nivo zaliha i odgovorile na zahteve kupaca brže i precizinije[9].

BEZBEDNOST INFORMACIJA I RIZICI U LANCU SNABDEVANJA

Vidljivost lanaca snabdevanja je moguće obezbediti preko različiti komunikacionih mreža, sistema, servisa i platformi. Internet ima najveći potencijal da obezbedi potrebnu informacionu vidljivost i olakša saradnju i donošenje odluka između različitih učesnika u lancu snabdevanja. Internet i novi komunikacioni servisi obezbeđuju izuzetne uslove za razmenu informacija, praćenje pošiljki i vidljivosti u realnom vremenu na globalnom tržištu. Međutim, internet kao jedna velika, globalna, otvorena i javna mreža koja, pored velikih mogućnosti za poslovanje sa partnerima i klijentima širom sveta, otvara i mogućnost za brojne prevare, malverzacije, zloupotrebe i online terorističke napade. Sve to predstavlja značajne rizike koje treba izbeći ili smanjiti njihove posledice.

Smanjivanje rizika u internet logistici predstavlja kompleksan postupak, koji obuhvata uvođenje novih tehnologija, organizacionih politika i procedura, novih zakona i industrijskih standarda, na osnovu kojih će se dati ovlašćenja nadležnim organima da gone i kažnjavaju počinioce cyber- kriminalnih radnji i time obezbede i očuvaju sigurnost u logistici koja se ugovara i prati preko interneta. Naime, konkurentske kompanije mogu „provaliti" u sistem određene logističke kompanije, sa ciljem da preuzmu informacije, preusmere porudžbine ili čak u potpunosti unište njen informacioni sistem kako bi zaustavili poslovanje i naneli štetu tom preduzeću i njegovim klijentima, a na taj način se može trajno uništiti reputacija napadnute kompanije. Zbog sve učestalijih online napada, logističke kompanije bi morale posebno da vode računa o sigurnosti svojih informacionih sistema. Međutim, potpuna sigurnost ne postoji, jer svaki sigurnosni sistem može biti ugrožen ukoliko se u ostvarenje takve namere ulože dovoljna sredstva. Ali trajna sigurnost u informacionoj eri nije ni potrebna. Informacije obično imaju vrednost u određenom vremenskom periodu, tako da je podatke moguće zaštititi prema potrebi na jedan dan, mesec ili godinu.

U tradicionalnoj i internet logistici postoji sličan rizik za snabdevača, logističku kompaniju i kupca. Tako na primer, u digitalnom okruženju za sve postoji rizik vezan za naplatu robe ili usluga, ukoliko se plaćanje odvija preko interneta. S druge strane, rizik za kupca proizvoda ili naručioca logističke usluge vezuje se za situaciju da plati robu ili uslugu, a da je uopšte ne

9 Handfield R., *Creating Information Visibility in the Chain*, 2002.

dobije, ili da dobije ono što nije poručio i platio. Osim toga, postoje i rizici vezani za aktivnosti trećih lica, koja svojim delovanjem direktno ugrožavaju bezbednost transakcija na internetu. U suštini lanci snabdevanja i pojedinačni učesnici izloženi su različitim kriminalnim rizicima veznim za poslovanje u virtuelno okruženje[10]. Internet kriminal ili kako se još popularno naziva „cyber" kriminal, predstavlja bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemima i mrežama, u kompjuterskim sistemima i mrežama i protiv kompjuterskih sistema i mreža[11]. Počinioci vrše napad na funkcije, servise i sadržaje koji se nalaze na internetu. Kradu se podaci, informacije, usluge i identitet, i oštećuju se ili čak uništavaju delovi ili cela mreža i računarski sistemi ili se ometa njihovo normalno funkcionisanje. U internet kriminal spadaju sve prevare koje se izvode uz pomoć računara i preko interneta. Generalno, internet prevara je bilo koja prevara, pri čijem izvršenju se koristi jedna ili više komponenti interneta, kao što su „chat rooms", web stranice, elektronska pošta i slično. Cilj je da se pribavi protivpravna imovinska korist ili da se stvore uslovi za lažno prikazivanje ili prikrivanje činjenica, kojim bi se neki učesnik u lancu snabdevanja doveo u zabludu ili u njoj održao. Takvo stanje omogućava da se učini nešto na štetu svoje ili tuđe imovine u lancu snabdevanja. Svakako je potrebno posebnu pažnju posvetiti najčešćim oblicima pretnji i narušavanja sigurnosti u onlin e okruženju, kao što su: zlonameran kod (eng. malicious code), hakeri, sajbervandalizam, lažno predstavljanje, prisluškivanje, špijuniranje, DDoS napadi, napadi iznutra i sl.

Generalno gledano, pri obezbeđenju vidljivosti lanca snabdevanja mogu se izdvojiti dve velike grupe rizika:

- Rizici u poslovnoj komunikaciji između velikog broja učesnika u lancu snabdevanja, putem interneta ili nekih drugih komunikacionih servisa, gde podaci u poslovnim porukama mogu biti kompromitovani ili razotkriveni;
- Rizici za informacioni sistem učesnika u lancu snabdevanja, kada informacije dolaze izvan sistema preko određenih komunikacionih kanala i servisa.

Kako bi se obezbedila zaštita podataka i informacionih sistema u lancu snabdevanja koriste se različite kombinacije zaštitnih mehanizama, aplikacija, protokola i internih kontrola, sa ciljem da se osiguraju integritet, privatnost i pouzdanost podataka.

10 Kaurin, T., Skakavac, Z., *Značaj digitalne forenzike mobilnih uređaja u otkrivanju i dokazivanju krivičnih dela organizovanog kriminala*, Peta Međunarodna znanstveno-stručna konferencija, Zagreb 2016, str. 58
11 http://www.uncjin.org/Documents/congr10/10e.pdf,

ZAŠTITA PODATAKA U LANCU SNABDEVANJA

Kada je reč o bezbednosti obavljanja logističkih aktivnosti u virtuelnom okruženju, tj. na internetu, najosetljivije tačke na kojima treba postaviti zaštitne mehanizme, sa tehnološkog aspekta, jesu sledeći nivoi zaštite: zaštita na nivou telekomunikacione mreže; zaštita na aplikativnom nivou; zaštita na nivou poruke.

Sistem zaštite na nivou telekomunikacione mreže obuhvata zaštitne mehanizme pristupa određenoj prenosnoj mreži, kako bi se u mrežu mogli uključiti samo autorizovani korisnici i to na osnovu korisničkih identifikacionih kodova i lozinki. Zaštita na ovom nivou obezbeđuje se identifikacijom uključenih strana u procesu razmene, odnosno pošiljaoca i primaoca poruke. Pouzdana i nedvosmislena identifikacija se obavlja pomoću sertifikata, koji dostavlja sertifikaciono telo – treća strana u razmeni u koju sve strane imaju poverenje i koja vodi registar svih partnera u razmeni. Sertifikaciono telo garantuje identitet partnera dostavom sertifikata sa svojim digitalnim potpisom.

Sistem zaštite na aplikativnom nivou podrazumeva davanje dozvola ili uvođenje dodatnih restrikcija, vezanih za korišćenje raspoloživih podataka, koje se uvode za korisnike koji su zadovoljili uslove bezbednosnog sistema na nivou mreže. Naime, određeni podaci ili aplikacije mogu biti zabranjeni ili dostupni za korišćenje određenim korisnicima, pa tako različiti korisnici mogu imati različita prava (pravo samo na čitanje sa internet stranice, pravo samo na unošenje podataka, pravo na čitanje i izmenu podataka, pravo na slanje podataka drugim stranama u razmeni i dr.).

Sistem zaštite na nivou poruka je izuzetno važan. U globalnom lancu snabdevanja poruka prolazi kroz veliki broj rutera i servera, pa se smatra da odatle vrebaju najveće sigurnosne pretnje. Zbog toga je visok nivo zaštite na nivou poruka izuzetno značajan za digitalnu logistiku. Pretnje mogu da budu izazvane namerno, kao posledica neovlašćene manipulacije sadržajem poruka ili nenamerno, kao rezultat grešaka u komunikacionom prenosu, kojima se menja sadržaj poruka. U svakom slučaju, razvijeni su brojni bezbednosni mehanizmi za koje se koriste jedna ili više metodologija zaštite. Opšte pretnje bezbednosti poruka, mogu se najbolje sagledati analizom pet dimenzija sigurnosti obavljanja logističkog procesa[12]:

- *Poverljivost* – sposobnost da se obezbedi da informacije i podatke, koji su poslati preko interneta, može da vidi samo ovlašćeni subjekt, odnosno razmenjivani podaci treba da budu zaštićeni od neovlašćenog uvida, kopiranja ili otkrivanja;

12 K. Rethmann 2009. Logistics PEOPLE – The Rhenus Group customer magazine, „*How Does the Supply Chain Become Secure?*" No 2. Str. 11.

- *Integritet* – sposobnost da se obezbedi da informaciju koja je postavljena na internet mrežu, ili je poslata i primljena preko interneta, niko ne može ni na koji način da izmeni neovlašćeno. Integritet znači da su podaci tačni, potpuni, pouzdani i pravovremeni;
- *Autentičnost* – sposobnost utvrđivanja individualnog i poslovnog identiteta učesnika u lancu snabdevanja. Autentičnost znači da informacija zaista potiče iz navedenog izvora;
- *Dostupnost* – znači da su podaci raspoloživi, tj.dostupni u vreme i na mestu na kome su potrebni ovlašćenim licima;
- *Pravna usklađenost* – odnosi se na potrebu da interno razvijeni propisi u kompaniji, kojima se reguliše sigurnost podataka, budu unutar zakonskih okvira.

Mehanizmi zaštite podataka u lancima snabdevanja i logistici, u kompjuterskom i internet okruženju, treba da spreče narušavanje bilo kojeg od navedenih nivoa sigurnosti.

PRIMENA SMART CM PLATFORME U LANCU SNABDEVANJA

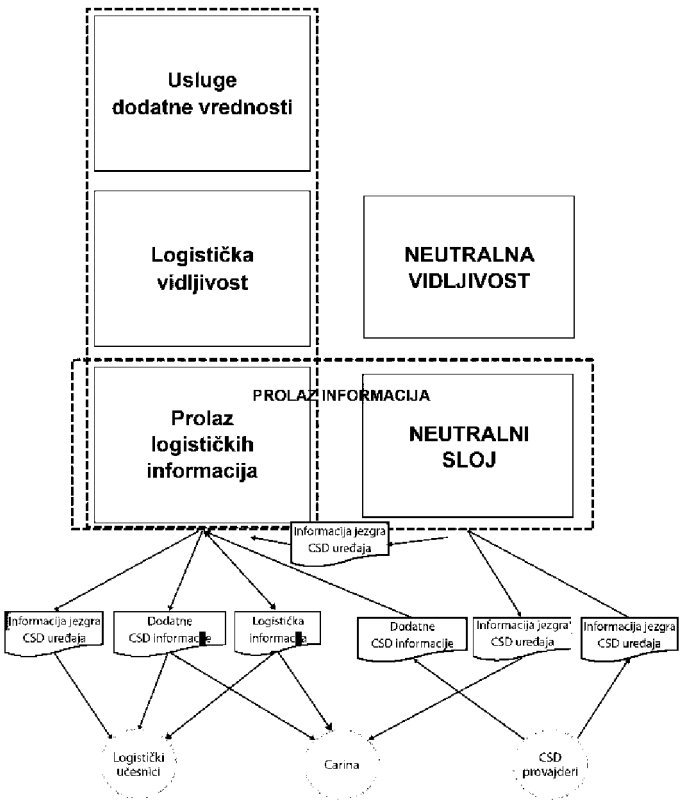
U globalnom lancu snabdevanja prisutan je veliki broj različitih učesnika, kao što su: pošiljalac, prevoznici, carina, granični terminali, brodske kompanije, logistički provajderi, inspekcije, primaoci robe i dr. (slika 1). Svi ovi učesnici realizuju različitet proce, koji su uređeni i povezani u lanac od mesta otpreme do mesta isporuke robe.

Slika 1. Učesnici u globalnom lancu snabdevanja

Učesnici obavljaju različite upravljačke aktivnosti i neophodan im je čitav niz informacija i podataka, kako bi efikasno upravljali lancem snabdevanja. Informacije imaju različite izvore, nastaju i završavaju na različitim mestima i od presudnog značaja je njihov efikasan protok i razmena između učesnika. Učesnici u lancu snabdevanja imaju različite zahteve vezane za protok informacija i podatka, kao što su: vidljivost, bezbednost, kompletnost, pouzdanost, tačnost, pravovremenost, efikasnost i dr. Navedene zahteve učesnika nije moguće uspešno realizovati, ukoliko ne postoji odgovarajuća informaciona i komunikaciona podrška. Potrebno je imati odgovarajuću platformu koja će omogućiti efikasan i siguran protok informacija i podata-

ka između učesnika u lancu. U skladu sa tim, u narednim izlganjima predstavljena je SMART CM platforma koja se koristi za razmenu informacija i praćenje kontejnera u globalnom lancu snabdevanja. Na bazi zahteva učesnika u lancu, definisana je funkcionalna struktura i arhitektura SMART-CM platforme, koja obuhvata dva polja delovanja. Prvo polje treba da zadovolji korisničke zahteve i upravljačke procedure u lancu snabdevanja, a drugo polje carinske i bezbednosne zahteve i procedure.

Platforma ima zadataka da obezbedi vidljivost i praćenje kontejnera kroz sve faze i procese lanca snabdevanja i da obezbedi bezbedan protok informacija između različitih učesnika u lancu. Informacije o kretanju i statusu kontejnera se prate preko „pametnog" sigurnosnog uređaja koji je postavljen na kontejner (CSD - Container Security Device). SMART-CM platforma je podeljena na informacioni prolaz, čija je osnovna namena prikupljanje podataka od različitih izvora i logistički sloj, gde se realizuju usluge praćenja i upravljanja procesima u lancu snabdevanja (slika 2)[13].



Slika 2. Strutkura i izgled funkcionisanja platforme

13 SMART-CM Implementation framework for global container surveillance and control, 2009.

Izvori podataka se generalno dele na tri osnovne kategorije: CSD informacije jezgra; CSD dodatne informacije i logističke informacije. U suštini se razlikuju sledeći formati poruka:

- Poruke sigurnosnog uređaja: poruke primljene direktno od CSD jedinica, a mogu biti brojevi kontejnera, CSD identifikacioni brojevi, informacije o statusu kontejnera.
- Poruke lanca snabdevanja: poruke koje su vezane za izvršavanje operacija u lancu snabdevanja ali se ne prenose putem CSD uređaja, kao što je identifikacija potrebnih dokumenata, izveštaji o prispeću kontejnera ili informacija o promeni vremena, i dr.
- Poruke i informacije dostupne u spoljnim bazama podataka, kao što su: detaljniji izveštaji o prispeću kontejnera, carinske procedure, komercijalne informacije (liste cena, liste pakovanja, fakture, tovarni listovi...).

Model protoka i razmene podataka odvija se kroz pet osnovnih blokova: blok sigurnosnih poruka, blok poruka lanca snabdevanja, blok obrade poruka, blok distribucije poruka i blok saradnje i dostupnosti. Blok sigurnosnih poruka i blok poruka lanca snabdevanja imaju mogućnost da rukuju sa „guranim" i „vučenim" porukama zbog većeg broja ulaznih kanala. Još jedna mogućnost je da se poruke učitavaju sa sigurnosnog servera. Čak i sa toliko različitih ulaznih kanala i protokola, blok poruka sigurnosnog uređaja ih sve podržava. Moraju biti dostupni najprostiji kanali i protokoli, ali mora biti moguća nadogradnja novih komunikacionih kanala unutar platforme, kao i podržana integracija različitih scenarija. Ulazni kanali sigurnosnog uređaja su odgovorni za upravljanje raznim scenarijima od nadolazećih poruka, kao i za transfer ovih poruka do bloka za dekodiranje poruka. Dekodiranje poruka sigurnosnog uređaja se primenjuje kada poruke ispune sigurnosne zahteve. Određene poruke mogu biti poslate šifrovane pa ih treba dekodirati, ili su određene poruke digitalno obrađene pa strana koja ih šalje treba samo da ih potvrdi. Kada se bezbednost i poreklo dolazeće poruke provere, poruka se dalje transformiše u poruku koja odgovara internim formatima, nakon čega se struktura i sadržaj proveravaju. Specifična pravila transformacije i provere za različite strane uglavnom su dostupne programu platforme, omogućavajući više verzija formata poruka koje se primaju u slučaju dodatnih informacija uz poruke. Nakon transformacije i provere, poruke se priključuju informaciji o kontejneru, gde je osnovna stvar odabrati pravi kontejner. Ovo obavlja blok identifikacije sigurnosnog uređaja na kontejneru. U zavisnosti od tipa poruke i količine dostavljenih informacija u sigurnosnoj poruci, ova združena informacija se može koristiti za određivanje tačnog kontejnerskog statusa i puta.

Nakon što se prime poruke lanca snabdevanja i sigurnosnog uređaja, njihov sadržaj se obrađuje u bloku za obradu poruka. To podrazumeva da se u porukama moraju poštovati poslovna pravila, sadržaj poruke se uparuje sa drugim informacijama o statusu kontejnera, te se pažljivo konstruišu poruke koje se šalju kao odgovor uključenim stranama. Svim odlaznim porukama upravlja blok za distribuciju poruka. Preko odgovarjuće matrice distribucije vrši se dostava odgovarajućim korisnicima. U slučaju da podaci koji se razmenjuju treba da budu zaštićeni, poruka će biti šifrovana zavisno od strane kojoj je namenjena. Blok za saradnju i dostupnost potrebno je da obezbedi konsolidovan pregled svih dobijenih statusa i detalja o kontejnerskom statusu, a podaci se dobijeni od sigurnosnog uređaja postavljenog na kontejner. Blok pretrage informacija o kontejneru pruža mogućnost da se preko pametnog uređaja postavljenog na sam kontejner traži određeni kontejnerski put. Potrebno je samo imati njegov identifikacioni broj. Ostali kriterijumi pretrage mogu biti definisani po određenim vrstama putovanja: identifikacija pošiljke, poslednja luka javljanja, logistički operator, itd.

ZAKLJUČAK

Internet i različiti komunikacioni servisi imaju izuzetno značajan potencijal za unapređenje globalnog poslovanja. Međutim, virtuelno okruženje prate i značajni bezbednosni rizici, koju mogu ugroziti globalni lanac snabdevanja i isporuku robe. Neophodno je da logističke kompanije i drugi učesnici u lancu snabdevanja preduzmu značajne mere i rešenja u pogledu zaštite podataka i informacionih sistema, a time i samog poslovanja. Mere i rešenja zaštite mogu da idu u više pravaca. Prvo je potrebno razvijati korporativnu bezbednosnu kulturu i politiku, uzimajući u obzir prirodu svih rizika na različitim nivoima. Drugo, potrebno je utvrditi koju vrstu podataka je potrebno zaštiti i na koji način. Treće, potrebno je odabrati odgovarajuće tehnologije i softverska rešenja, odnosno razviti procedure i protokle, kako bi se uspešno suprostavili realnim pretnjama i rizicima. U svakoj logističkoj kompaniji koja posluje na internetu i uz pomoć interneta, trebalo bi da postoji odeljenje koje sprovodi sigurnosnu politiku, obučava zaposlene, održava alate protiv sigurnosnih rizika i ukazuje menadžmentu na sigurnosne pretnje. Potrebno je sprovoditi kontrolu pristupa interentu i komunikacionim servisima, koja podrazumeva uvid u to koji spoljašnji i unutrašnji učesnici mogu da imaju pristup mreži.

Pored toga, potrebno je razvijati odgovarajuće platforme koje će obezbediti efikasno i bezbedno odvijanje tokova informacija između učesnika u lancu snabdevanja. SMART CM platforma koja je razmatrana u ovom radu pruža značajne prednosti u tom pogledu, koje se ogledaju kroz: smanje

troškova (operativnih i investicionih); skraćenje vremena obrade podataka, čekanja i isporuke; poboljšanje produktivnosti, pouzdanosti i fleksibilnosti; povećanje otpornosti lanca snabdevanja; veća zaštita i bezbednost podataka; veća zaštita robe od krađe i krijumčarenja, itd. Da bi platforma bila operativna i njena primena uspešna, mora postojati održivi poslovni model, koji bi obezbedio usluge, koje su od značaja i idu u korak sa tržištem. Potrebno je obezbediti neutralnost platforme, kroz neutralnu organizaciju koja bi je vodila.

Summary

The global supply chain comprises a large number of participants, such as manufacturers, distributors, logistics and transport companies, shippers, border terminals, customs, and the like. A successful connection of all participants in a synchronized chain is not possible without information flows, which provide an efficient flow of information at different levels. The participants generally have their own information systems and, at the same time, they are components of different information and communications networks at the global level. In such business environment, information safety is crucial. This paper discusses the issues of data protection in the global chain of container shipping and delivery. First, requirements such as: transparency, safety, reliability, timeliness, effectiveness and efficiency in the supply chain are analyzed, and then a solution based on the SMART CM platform is proposed. The functional architecture of the platform, the key scenarios to successful implementation and models of functioning through certain blocks and layers are proposed. Message formats and sources of information are defined. Finally, the possibilities and limitations of the platform application from the viewpoint of the most important participants in the chain of container shipping and delivery are presented.

Key words: *Data protection, information safety, supply chain, SMART CM platform*

LITERATURA

1. Banomyong, R., *"The Impact of Port and Trade Security Initiatives on Maritime Supply--Chain Management"*. Pra Chan Road, Thammasat Business School, Thammasat University, Bangkok 10200, Thailand. Marit.Pol.MGMT, January-March 2005, Vol 32, No1, 3-13
2. Bichou K., Bell, M., *Internationalisation and Consolidation of the Container Port*
3. *Industry: Assessment of Channel Structure and Relationships,* Maritime Economics &
4. Logistics, 2007, 9, (35–51
5. Ekwall, D. , *"On analyzing the official statistics for antagonistic threats against transports in EU: a supply chain risk perspective"*. Journal of Transportation Security, Vol. 3, No. 4, pp 213-230, 2010.

6. Handfield, R., Barnhardt, R., & Powell, N.," *Mapping the Automotive Textile Supply Chain: the Importance of Information Visibility",*Journal of textile and apparel technology and management, 3(4), 1- 19. 2004
7. Kaurin, T., Skakavac, Z., *Značaj digitalne forenzike mobilnih uređaja u otkrivanju i dokazivanju krivičnih dela organizovanog kriminala,* Peta Međunarodna znanstveno-stručna konferencija, Zagreb 2016, str. 58
8. Kaurin T., Kilibarda M., *Informacione i komunikacione tehnologije u globalnim lancima snabdevanja,* Treća međunarodna naučna konferencija Evropska unija – izazovi proširenja i Zapadni Balkan, Banja Luka 2016.
9. Rethmann 2009. Logistics PEOPLE – The Rhenus Group customer magazine, *„How Does the Supply Chain Become Secure?"* No 2. Str. 11.
10. SMART-CM Implementation framework for global container surveillance and control, 2009.
11. http://searchmanufacturingerp.techtarget.com/definition/supply-chain-visibility-
12. http://www.gtnexus.com/solutions/supply-chain-visibility
13. http://www.mepsupplychain.org/supply-chain-visibility/
14. http://www.uncjin.org/Documents/congr10/10e.pdf,