Projekt: SECNET

Program: V-A Slovenija - Italija 2014 - 2020

Naslov dokumenta: **D.3.1.1.3 – Ocena in validacija rezultatov pilotnih aktivnosti**

Referenčni DS: DS 3.1 Pametna čezmejna pristaniška varnost

Status dokumenta	**Avtorji**	**Datum**
Osnutek	Dejan Paliska, Peter Kopič, Mita Lazar	
Dokončni		

Kazalo

Uvod

V okviru projekta je bil del sredstev porabljen za testiranje varnostnih sistemov in implementacijo pilotnih rešitev na področju fizične in kibernetske pristaniške varnosti. Pristanišča so na podlagi prepoznanih tveganj predlagala tehnične rešitve in izboljšave, ki so bile kasneje implementirane v sklopu pilotnih aktivnosti. Pričujoči dokument podaja oceno implementiranih tehničnih rešitev v smislu doseganja izboljšav glede na prepoznana varnostna tveganja v posameznem pristanišču in možnosti prenosa posameznih rešitev med pristanišči.

Področje fizične varnosti in varovanje meja

Različna pristanišča imajo zelo različno urejeno in organizirano fizično varovanje območja pristanišča in njegovih meja ter uporabljajo različno tehnično opremo. Predhodna raziskava dobrih praks v sklopu projekta je pokazala, da pristanišča veliko pozornosti namenjajo sistemom za zgodnje odkrivanje varnostnih groženj. Inteligentni sistemi videonadzora, prepoznavanja registrskih tablic, identifikacija na vstopnih točkah in sistem alarmiranja so najbolj pogosto uporabljeni sistemi. Veliko naporov je usmerjenih tudi v povezovanje različnih sistemov v skupnem nadzornem centru in sisteme komuniciranja v kriznih razmerah. Pristanišča, v katerih se nahajajo potniški terminali, posvečajo dodatno pozornost pregledovanju potnikov in odkrivanju tihotapcev ali slepih potnikov.

V sklopu predhodnih aktivnosti na projektu so bila prepoznana sledeča varnostna tveganja na področju fizičnega varovanja:

- **Pristanišče Koper**

a) Vstop avtoprevoznikov na območje pristanišča, ki trenutno vstopajo brez najave;
b) Signalizacija za vodenje obiskovalcev in voznikov znotraj pristanišča;
c) Varovanje zračnega prostora pristanišča (predvsem pred brezpilotnimi letalniki);
d) Pomanjkljivo varovan železniški vhod;
e) Necelovito varovanje kopenske in morske meje pristanišča.

- **Pristanišče Trst**

a) Tveganje vstopa migrantov, ki lahko pridejo z ladjami z Bližnjega Vzhoda;
b) Naftovod in terminal SIOT predstavljata povečano tveganje za napad;

c) Velike površine in prostorska razpršenost/konfiguracija terminalov, ki jih je težko v celoti nadzorovati s patruljami;
d) Težaven nadzor morskih in kopenskih meja pristanišča.

- **<u>Pristanišče Benetke</u>**

a) Nadzor nad vodnimi površinami pred operativnimi obalami pristanišča;
b) Opredelitev notranjih meja pristanišča;
c) Zastarel sistem nadzora na vhodu San Andrea in na vhodih v pristanišče Chioggia.

Področje kibernetske varnosti

Pomorski sektor se podobno kot drugi gospodarski sektorji sooča s čedalje večjim številom kibernetskih groženj in napadov. Dandanes je učinkovito delovanje pomorskega sektorja v veliki meri odvisno od nemotenega delovanja informacijske telekomunikacijske tehnologije, ki predvsem pripomore k optimizaciji poslovnih procesov in hitri komunikaciji. Sodobna avtomatizirana pristanišča pa brez uporabe IKT sistemov sploh ne morejo delovati. V smislu uporabe IK tehnologij pomorski sektor predstavlja izredno kompleksen sistem, ki ga sestavljajo zelo različne tehnologije, ki so v svojih elementih izredno specifične. V praksi je skoraj nemogoče poenotiti IKT sisteme vseh pristanišč in pristaniških deležnikov, saj so pristanišča in deležniki lahko medsebojno geografsko razpršeni in se lahko nahajajo v različno gospodarskorazvitih državah ter uporabljajo različne tehnologije.

S porastom uporabe Interneta in »Interneta stvari«, vsenavzočne povezljivosti, elektronskega poslovanja in z nenehno bliskovito rastjo informacijskih mrež v zadnjih desetih letih postaja kibernetski prostor nepogrešljiv del vsakodnevnega javnega in poslovnega življenja. Vendar se sočasno z razvojem kibernetskega prostora in rastjo števila uporabnikov povečuje tudi število kibernetskih napadov, ki postajajo čedalje bolj sofisticirani in učinkoviti.

Na podlagi anketne raziskave in v skupu samoevalvacijskih procesov se je pokazalo, da so partnerska pristanišča projekta na področju kibernetske varnosti različno organizirana in tehnično opremljena. Ugotovimo lahko, da italijanski pristanišči zaostajata za koprskim pristaniščem predvsem v tehničnih ukrepih in organiziranosti. Zbrani podatki kažejo, da pristanišči Trst in Benetke ne izvajata ocen tveganja za področje kibernetske varnosti (testov vdora), kar prepoznamo kot ključno pomanjkljivost in potencialno tveganje.

V sklopu predhodnih aktivnosti na projektu so bila prepoznana sledeča varnostna tveganja na področju kibernetske varnosti:

- Zaradi hitrega razvoja informacijskih tehnologij, ki jim pristanišča niso sledila, so vsa tri pristanišča izpostavljena tveganjem kibernetskega vdora v sisteme;
- Tveganje je primerjalno še večje v pristaniščih Trst in Benetke, kjer ne izvajajo rednih periodičnih testov vdora.

V praksi lahko povečamo kibernetsko varnost tako, da ukrepamo na različnih segmentih kibernetske varnosti npr. z nadzorom do dostopa, zasnovo mreže, zaznavo vdorov, varno komunikacijo, hitro obnovitvijo, učinkovitim upravljanjem in nadzorom. Dobra praksa je zaščititi sisteme in podatke z različnimi ukrepi (večslojno), na različnih ravneh; na ravni zaposlenih, postopkov in tehnologije.

Ocena in validacija rezultatov pilotnih aktivnosti

1. Pristanišče Koper

- **Namestitev najnaprednejšega infrardečega radarskega sistema z dodatnimi termografskimi kamerami 3 (DS 3.1.5.2)**

Nameščen je bil sodoben infrardeči radarski sistem z dodatnimi termografskimi kamerami z visoko ločljivostjo za 360-stopinjski ogled določenih območij v pristanišču. S temi kamerami lahko nadzorni center zaznava vse vire toplote in vse premike v radiju 1.500 m v vseh vremenskih razmerah, tako podnevi kot ponoči. Sistem je povezan s strežniki, ki omogočajo shranjevanje in razpošiljanje velikih količin podatkov, ki jih zajema zgoraj navedena oprema, s posnetki visoke ločljivosti, ki se snemajo neprestano. Predvidena je tudi predpriprava in združljivost videonadzornega sistema, s katerim bo nadzorni center pristanišča lahko v realnem času ter v vseh vremenskih in svetlobnih razmerah spremljal pogoje varovanja in nadzora na določenih območjih Luke Koper.

Zahvaljujoč senzorjem za prepoznavanje virov toplote lahko osebje, pristojno za videonadzor zunanje meje pristanišča, z novim radarjem zazna osebe, ki nezakonito vstopijo na območje pristanišča tudi v razmerah slabe vidljivosti, na primer ponoči ali ob zmanjšani vidljivosti. Vendar pa sama oprema za videonadzor ne bi zadoščala, če ne bi bila usklajena s celotnim sistemom alarmiranja in videonadzora v Luki Koper. Sistem namreč različnim kameram, ki so postavljene ob zunanji meji pristanišča, omogoča zoženje, razširitev ali izbiro želenega vidnega polja ter optimizacijo fizične varnosti na nadzorovanem območju.

Ocena

Implementiran radarski sistem z dodatnimi termografskimi kamerami odpravi oz. znatno zmanjša tveganja zaznana pod točko c, d in e, vendar le posredno vpliva na prepoznana tveganja pod točko a in b. Največji doprinos je moč oceniti pri možnosti celovitega in kontinuiranega nadzora notranjih površin in meja pristanišča. Koprsko pristanišče bo moralo v prihodnosti odpraviti tudi prvi kategoriji prepoznanih tveganj.

Glede na prepoznane prednosti je možno sistem smiselno implementirati tudi v drugih dveh pristaniščih, ki imata podobno težavo s celovitim nadzorom notranjega območja in zunanjih mej pristanišča.

- **Tehnična presoja in preizkušanje tehnologij IKT (kibernetska varnost – testi vdora) (DS 3.1.4.2)**

V okviru projekta so bili opravljeni testi vdora v informacijski sistem pristanišča. V več fazah je bila testirana ranljivost dveh spletnih aplikacij in podporne informacijske infrastrukture pristanišča. Med preverjanjem varnosti je bilo ugotovljenih dvanajst potencialnih tveganj. Pet od teh je bilo razvrščenih v visoko kategorijo tveganja, kar pomeni, da bi bilo z izkoriščenjem ranljivosti mogoče neposredno vplivati na razpoložljivost, integriteto ali zaupnost podatkov Luke Koper, d.d. Poleg teh sta bili ugotovljeni dve dodatni ranljivosti, ki sta bili ocenjeni kot srednje visoki, in pet nizkih. Po odpravljenih ugotovljenih ranljivostih je bil sistem ponovno testiran s testi vdora. Ponovno testiranje ni pokazalo ranljivosti ali potencialnih tveganj.

Ocena

Testi vdora so pokazali določene ranljivosti, ki so bile kasneje odpravljene. S tem se je zmanjšalo tveganje uspešnega kibernetskega napada na pristanišče, tako da lahko pilotno aktivnost ocenimo kot izredno uspešno. Vsekakor pa je priporočljivo teste vdora periodično ponavljati.

2. Pristanišče Trst

- **Namestitev štirih alarmnih siren na streho stolpa ob skladišču 53 in osmih alarmnih siren na stolpu nekdanjega sedeža CULP (DS 3.1.5.2)**

V okviru te aktivnosti sta bili predvideni dobava in namestitev dveh t.i. oddajnih enot, ki ju tvorita aluminijasti usmerjeni sireni, na strehi dveh različnih stavb v novem pristanišču, tako da bo zagotovljena pokritost zvočnega signala na vseh terminalih in z njimi povezanih delovnih območjih. Za vklop in upravljanje sistema alarmiranja je zadolžen nadzorni center v Lloydovem stolpu zunaj ograjenega delovnega območja. Zato je bila v pilotni aktivnosti predvidena tudi

namestitev programske opreme z ustreznim radijskim sprožilnikom, ki omogoča sproženje sistema alarmiranja ter nadzor siren in ponavljalnikov v vnaprej določenih časovnih intervalih zaradi preverjanja delovanja in kakovosti radijskega prenosa. Za omejitev zvočnega onesnaževanja zunaj pristaniškega območja so bile izbrane usmerjevalne sirene.

Ocena

Implementirana oprema omogoča alarmiranje na celotnem območju pristanišča, kar posredno pripomore k večji varnosti ob zunanjih mejah pristanišča in omogoča bolj usklajeno in celovito delovanje varnostnega sistema pristanišča. Vendar aktivnost nima neposrednega učinka na prepoznana tveganja varovanja morskih in kopenskih meja pristanišča, kot tudi ne na zmanjševanje tveganja vstopa migrantov in na učinkovitost nadzora nad območjem pristanišča.

- **Prilagoditev brezpilotnega letalnika (drona) potrebam pristanišča in ureditev kontrolnega centra ter šolanje pilotov (DS 3.1.5.2)**

V okviru projekta je bila izvedena prilagoditev dronov, ki jih je AdSP MAO kupila z lastnimi sredstvi, delovnim pogojem Pristanišča Trst. Prilagoditev je obsegala predelavo dronov glede na okoljske pogoje v Pristanišču Trst (prisotnost anten, radarskih sistemov, ladij različnih velikosti in ovir, kot so žerjavi ipd.) ter opremljanje z infrardečo toplotno kamero.

V okviru aktivnosti je bila izvedena tudi ureditev kontrolnega centra v Lloydovem stolpu s programsko opremo in odgovarjajočo tehnično podporo, kjer bo mogoča obdelava podatkov videonadzora, ki jih bodo v digitalni obliki pošiljali droni. Kontrolna soba upravlja zajete podatke in izvaja nekatere funkcije, ki jih običajno opravljajo kontrolni stolpi v zračnem prometu, njene dejavnosti pa temeljijo na vnaprej določenih operativnih protokolih in računalniškem sistemu za beleženje operativnih dejavnosti v oblaku.

Ocena

Implemetirana oprema omogoča preletavanje območja pristanišča in analizo zajetih video posnetkov v realnem času. Na tak način je omogočen dodaten nadzor nad kopenskimi in morskimi mejami celotnega pristanišča ter odkrivanje potencialnih nedovoljenih vstopov. Omogoča tudi termografski zajem infrastrukture za namene varnosti in tehnične presoje. Z uporabo brezpilotnega letalnika in sistema nadzora ter obdelave posnetkov se zmanjšajo vsa zaznana tveganja v pristanišču v Trstu.

Glede na dosežen rezultat se predlaga implementacijo podobnih sistemov tudi v drugih pristaniščih partnerstva.

- **Tehnična presoja in preizkušanje tehnologij IKT (DS 3.1.4.2)**

V okviru tega sklopa sta bili opravljeni dve pilotni aktivnosti. Prva se je nanašala na posodobitev zajema in povezovanje do sedaj nepovezanih podatkovnih zbirk dveh temeljnih informacijskih sistemov za delovanje pristanišča ter omogočanje dostopa do teh podatkov zunanjim uporabnikom. V sklopu te aktivnosti so bila tudi načrtovana različna statistična poročila. Druga pilotna aktivnost je imela kot cilj povečanje varnosti infrastrukture in harmonizacijo hranjenja in obdelave digitalnih podatkov, skladno z uredbo GDPR. V obeh aktivnostih je bila najprej narejena obsežna analiza obstoječega stanja, opredelitev metodologije ter izvedba aktivnosti. Opravljeno je bilo tudi izobraževanje na področju kibernetske varnosti za zaposlene, kar je bistveno pripomoglo k ozaveščanju o pomenu kibernetske varnosti in njeni krepitvi. Izdelane so bile IT platforme, s katerimi je upravljanje računov za dostopanje do sistemov in podatkov, ki se dodelijo uporabnikom, boljše in učinkovitejše. Na ta način je bilo mogoče samodejno ukiniti račune zaposlenih, ki so prekinili delovno razmerje. Ta orodja so povečala tudi učinkovitost postopkov "spremembe gesla", ki so sedaj samodejni, tako da stalni posegi oddelka IT niso več potrebni. Vzpostavljen je bil tudi sistem, ki uporabnikom z dovoljenji skrbnika (tako zaposlenim kot zunanjim sodelavcem) omogoča spremljanje dostopov do sistema IT in do podatkov. Na ta način je zagotovljeno popolno upoštevanje minimalnih varnostnih ukrepov za javne uprave (ki so predvideni tudi v GDPR) in preprečeni so morebitni napadi z eskalacijo privilegijev pri dostopanju do podatkov s strani uporabnikov ali virusov v omrežju. Skladno z ugotovljenimi tveganji v poročilu o analizi vrzeli v zvezi s področnimi predpisi in standardi, ki obravnava pravno in organizacijsko področje, in poročilu o analizi informacijske infrastrukture kot rezultata ocene ranljivosti celotnega omrežja s protiukrepi za znižanje ravni informacijskega tveganja, so bila zaznana tveganja odpravljena.

Ocena

Izvedene aktivnosti so večslojno vplivale na povečanje kibernetske varnosti in sicer z nadzorom dostopa, učinkovitim upravljanjem in nadzorom infrastrukture, na ravni ozaveščanja in izobraževanja zaposlenih ter postopkov in tehnologije. Opravljena je bila tudi ocena ranljivosti sistema ter odpravljene so bile zaznane pomanjkljivosti. S tem so se tudi bistveno zmanjšala tveganja uspešnega kibernetskega napada na informacijske sisteme pristanišča.

3. Pristanišče Benetke

- **Implementacija sistema za nadzor vstopa AGS v pristanišče z uporabo sistema za odčitavanje registrskih številk vozil OCR.**

Cilj aktivnosti je bil izboljšanje fizične varnosti pristanišča s sistemom za nadzorovanje vstopa v območje pristanišča. V sklopu aktivnosti je bilo na vhodih Sv. Andrej in Sv. Nikolaj nameščen sistem za odčitavanje registrskih tablic OCR, ki je integriran v obstoječi sistem za nadzor vstopov. Za povezovanje sistemov je bilo potrebno razviti posebno programsko opremo, ki beleži podatke o vstopu in izstopu ter tranzitu. Na podlagi zbranih podatkov sistem računa, koliko prostih mest je na voljo na posameznih območjih znotraj pristanišča in tako regulira vstope. Na dveh vhodih v pristanišče Chioggia (Val di Rio in Otok Saloni) so bile nameščene računalniško podprte kontrolne točke, opremljene s tehnologijo RFID in s čitalci črtnih kod, s katerimi se preverja vstopna dovoljenja imetnikov v območje pristanišča.

Oba sistema sta bila integrirana z že obstoječim sistemom na drugih vstopnih točkah v pristanišče in sedaj tvorijo celovit sistem nadzora nad vstopi v območje pristanišča.

Ocena

Implementirana tehnologija skupaj z razvito programsko opremo omogoča sistemsko celovit nadzor nad vstopi v in izstopi iz pristanišča ter tako pripomore k zmanjševanju tveganj nepooblaščenih vstopov na območje pristanišča. Sistem pripomore tudi k regulaciji in optimizaciji logističnih tokov v pristanišču in posledično vpliva na prometno varnost in produktivnost dela.

Zaključek

Zaradi svoje funkcionalnosti in pomembnosti za družbo predstavlja vsa kritična infrastruktura, vključno s pristanišči, potencialno tarčo napada. V primerjavi z drugo kritično infrastrukturo so pristanišča še bolj izpostavljena napadom. Razlogov je več; v pristanišče vstopa veliko različnih ljudi (agenti, špediterji, delavci, piloti, pomorci itd.), veliko različnih prevoznih sredstev (ladje, tovornjaki, vagoni itd.), različno blago, njihovo poslovanje je odvisno od izmenjave velike količine podatkov, vpletenih je veliko deležnikov, veliko je finančnih transakcij itd.. Prav zaradi tega je področje pristaniške varnosti izredno raznoliko, kompleksno, večplastno ter tehnično zahtevno.

V okviru pilotskih aktivnosti znotraj projekta SECNET so partnerska pristanišča testirala različne sisteme za izboljšanje fizične in kibernetske varnosti pristanišč. **Validacija rezultatov je**

pokazala, da so vsi implementirani sistemi pripomogli k zmanjševanju tveganj na več različnih ravneh. Implementirane sisteme zato ocenjujemo kot učinkovite pri zmanjševanju prepoznanih tveganj. Vendar zaradi geografskih značilnosti, različnih velikosti pristanišč, razlik v terminalih in njihovi opremljenosti, infrastrukturi in suprastrukturi, organiziranosti, predvsem pa zaradi raznolikosti informacijskih tehnologij ni možno prenašati vseh rezultatov pilotnih aktivnosti iz enega pristanišča v drugo pristanišče brez prilagoditev. Med tiste, ki jih lahko brez posebnih prilagoditev implementiramo v vsa pristanišča, sodita zagotovo uporaba brezpilotnih letalnikov in visokoločljivega radarja za nadzor območja pristanišča in njegovih meja. Medtem ko lahko na področju kibernetskega varovanja prenašamo med pristanišči le koncepte, tehnična izvedba pa je pogojena z omenjenimi značilnostmi posameznega pristanišča.