Progetto: SECNET

Programma: V-A Italia-Slovenia 2014-2020

Titolo del documento: **D.3.1.1.3 – Valutazione e validazione dei risultati delle attività pilota**

WP di riferimento: WP 3.1 Smart port safety transfrontaliera

Stato documento	**Autori**	**Data**
Bozza	Dejan Paliska, Peter Kopič, Mita Lazar	
Definitivo		

Indice

Introduzione

Nell'ambito del progetto una parte dei fondi è stata utilizzata per testare i sistemi di sicurezza e l'implementazione di soluzioni pilota nell'ambito della sicurezza fisica e cibernetica nei porti. In base ai rischi individuati, i porti hanno proposto soluzioni tecniche e miglioramenti, successivamente implementati con le attività pilota. Questo documento presenta una valutazione delle soluzioni tecniche implementate volte a ridurre i rischi riconosciuti per la sicurezza dei singoli porti, con la possibilità di trasferire le singole soluzioni tra i porti.

Settore della sicurezza fisica e protezione dei confini

Ogni porto organizza e regolamenta la sicurezza fisica dell'area portuale e dei confini in modo diverso con l'utilizzo di strumenti tecnici diversi. Uno studio preventivo delle best practice svolto nell'ambito del progetto ha evidenziato che i porti pongono molta attenzione ai sistemi di riconoscimento precoce dei rischi per la sicurezza. Quelli più diffusi sono: sistemi di video sorveglianza intelligenti, riconoscimenti di targhe, identificazione ai punti di accesso e sistema di allerta. Molto impegno è stato profuso nella connessione di diversi sistemi con un centro di controllo unificato e con sistemi di comunicazione in situazioni di emergenza. I porti, nei quali si trovano i terminal passeggeri, hanno dedicato ulteriore attenzione al controllo dei predetti e all'individuazione di contrabbandieri o passeggeri clandestini.

Nell'ambito delle attività precedentemetne svolte nell'ambito del progetto sono stati individuati i seguenti rischi per la sicurezza fisica:

- **Porto di Capodistria**

a) Accesso degli autotrasportatori nell'area portuale attualmente senza preavviso;
b) segnalamento per la conduzione dei visitatori e dei trasportatori all'interno del porto;
c) protezione dello spazio areo dell'area portuale (in particolare da droni);
d) sicurezza carente presso l'accesso ferroviario;
e) sicurezza carente su confini portuali marittimi e terrestri.

- **Porto di Trieste**

a) rischio di accessi di migranti, che possono arrivare con le navi provenienti dal Medio Oriente;
b) l'oleodotto ed il terminal SIOT sono maggiormente esposti al rischio di attacchi;

c) grandi superfici e dispersione geografica/configurazione dei terminal che le pattuglie controllano con difficoltà;
d) controllo difficoltoso dei confini terrestri e marittimi del porto.

- **Porto di Venezia**

a) Controllo delle superfici marittime davanti alle banchine del porto;
b) definizione dei confini interni del porto;
c) sistemi di controllo all'accesso di Sant'Andrea e presso gli accessi al porto di Chioggia obsoleti.

Settore della cyber security

Il settore marittimo, come altri settori economici, deve affrontare un numero sempre maggiore di minacce ed attacchi cibernetici. Oggigiorno un'efficiente attività del settore marittimo dipende in gran misura dal funzionamento regolare delle tecnologie dell'informazione e della comunicazione, che contribuiscono in primo luogo all'ottimizzazione dei processi commerciali e alla comunicazione rapida. L'automatizzazione moderna del porto senza sistemi di TIC non potrebbe nemmeno entrare in funzione. Sotto il profilo dell'utilizzo delle tecnologie per l'informazione e la comunicazione, il settore marittimo rappresenta un sistema estremamente complesso, composto da tecnologie molto diverse e da elementi assolutamente specifici. In pratica è quasi impossibile unificare i sistemi TIC di tutti i porti e dei relativi stakeholder, visto che possono essere distanti dal punto di vista geografico, o trovarsi in paesi con livelli di sviluppo economico diverso, oppure ancora utilizzare diverse tecnologie.

Con il sempre maggiore utilizzo di internet e dello "Internet of things", la connessione sempre presente, il commercio telematico e la crescita rapida delle reti d'informazione degli ultimi decenni, lo spazio cibernetico sta diventando una parte imprescindibile della vita quotidiana lavorativa e pubblica. Ma al contempo, con lo sviluppo dello spazio cibernetico e la crescita del numero degli utenti, aumenta anche il numero degli attacchi, che diventano sempre più sofisticati ed efficaci.

Con la somministrazione del questionario e nell'ambito dei processi di autovalutazione è stato accertato che i porti, partner del progetto, nell'ambito della cyber security presentano differenze nell'organizzazione e nelle attrezzature tecniche. Si è, perciò, potuto verificare che i porti italiani presentano un certo ritardo rispetto al porto di Capodistria soprattutto nell'ambito delle misure tecniche applicate e nell'organizzazione. I dati raccolti hanno evidenziato che i porti di Trieste e Venezia non attuano la valutazione dei rischi per il settore della cyber security (test di intrusione al sistema), il che viene riconosciuto quale carenza fondamentale e rischio potenziale.

Nell'ambito delle attività precedenti svolte nell'ambito del progetto sono stati individuati i seguenti rischi per la cyber security :

- A causa del rapido sviluppo delle tecnologie dell'informazione tutti e tre i porti, non essendo al passo con le novità del settore, sono esposti al rischio di intrusione cibernetica nei sistemi;
- i rischi sono ancora maggiori nei porti di Trieste e Venezia, dove non vengono svolti regolarmente test di intrusione.

In pratica è possibile aumentare la sicurezza cibernetica adottando misure in diversi segmenti, ad esempio in: controllo degli accessi, progettazione della rete, accertamento di intrusioni, comunicazione sicura, ripristino rapido, gestione efficace e controllo. Buona prassi è proteggere sistemi e dati con diverse misure (multilevel), in diversi settori: dipendenti, procedure e tecnologie.

Valutazione e validazione dei risultati delle attività pilota

1. Porto di Capodistria

- **Installazione di sistema radar avanzato ad infrarossi con camere termografiche aggiuntive 3 (DS 3.1.5.2)**

E' stato installato un moderno sistema radar ad infrarossi con camere termografiche aggiuntive ad alta definizione a 360° per determinate aree del porto. Con dette camere il centro di controllo è in grado di intercettare tutte le fonti di calore ed i movimenti nel raggio di 1.500 m in tutte le condizioni meteo, nelle ore diurne e notturne. Il sistema è collegato con dei server che permettono la conservazione e l'invio di grandi quantità di dati, rilevati dal sistema sopra descritto con rilievi ad alta definizione e riprese costanti. E' prevista anche la predisposizione e la compatibilità del sistema di video sorveglianza, con il quale il centro di controllo del porto sarà in grado di monitorare le condizioni di sicurezza e controllare determinate aree di Luka Koper in tempo reale e con qualsiasi tipo di condizione meteo.

Grazie ai sensori per il riconoscimento delle fonti di calore, il personale addetto alla video sorveglianza dei confini esterni del porto è in grado di intercettare le persone che accedono illegalmente nell'area del porto anche in condizioni di scarsa o ridotta visibilità, ad esempio di notte. Ma resta da dire che il solo impianto di video sorveglianza non sarebbe sufficiente se esso non fosse coordinato con il sistema complessivo di allarme e video sorveglianza di Luka Koper. Il sistema, infatti, permette alle diverse camere posizionate sul confine esterno del porto

di restringere, allargare e scegliere il campo visivo desiderato ed ottimizzare la sicurezza fisica nell'area controllata.

Valutazione

Il sistema radar ad infrarossi con camere termografiche aggiuntive azzera ovvero riduce sensibilmente i rischi indicati ai punti c, d ed e, ma ha solo impatti indiretti sul riconoscimento dei rischi di cui ai punti a e b. Il contributo maggiore è riscontrabile nella possibilità di controllare integralmente e continuamente le superfici interne ed i confini del porto. Il porto di Capodistria nel futuro dovrà affrontare e risolvere anche le prime due categorie di rischi riconosciuti.

Visti i vantaggi riscontrati è possibile implementare il sistema in modo idoneo anche negli altri porti, che affrontano difficoltà simili con i controlli delle aree interne ed esterne del porto.

- **Valutazione tecnica e verifica delle tecnologie ICT (cyber security – test di intrusione) (DS 3.1.4.2)**

Nell'ambito del progetto sono stati svolti test di intrusione nel sistema informatico del porto. E' stata testata la vulnerabilità di due applicazioni e dell'infrastruttura di supporto informatico in diverse fasi. Nel corso della verifica della sicurezza sono stati accertati 12 rischi potenziali, di cui cinque sono rischi elevati, il che significa che sfruttando la vulnerabilità, sarebbe possibile influire direttamente su disponibilità, integrità e riservatezza dei dati di Luka Koper, d.d. Inoltre sono state accertate due ulteriori vulnerabilità di classe medio alta, e cinque di classe bassa. Dopo aver accertato le vulnerabilità il sistema è stato sottoposto nuovamente ai test di intrusione. In seguito ai nuovi test non sono state evidenziate vulnerabilità o potenziali rischi.

Valutazione

I test di intrusione hanno evidenziato determinate vulnerabilità successivamente risolte. In questo modo vengono ridotti i rischi di esito positivo degli attacchi cibernetici sul porto, per tale motivo l'attività pilota si è dimostrata estremamente efficace. In ogni caso si raccomanda la ripetizione periodica dei test di intrusione.

2. Porto di Trieste

- **Installazione di quattro sirene di allarme sul tetto della torre vicino al magazzino 53 ed otto sirene d'allarme vicino alla torre dell'ex magazzino CULP (WS 3.1.5.2)**

Nell'ambito della presente attività è stata prevista la fornitura delle così dette unità di trasmissione, composte da sirene in alluminio direzionate, da installare sul tetto di due edifici diversi che si trovano nel nuovo porto, in modo tale da garantire la copertura del segnale acustico presso tutti i terminal e tutte le aree di lavoro con essi connesse. Il centro di controllo della Torre del Lloyd, che si trova all'esterno dell'area di lavoro recintata, è deputato all'attivazione ed allo spegnimento del sistema di allarme. Per tale motivo nell'attività pilota è stata prevista anche l'installazione del software con un dispositivo di accensione radio, che permette l'innesco del sistema di allarme ed il controllo delle sirene e dei ripetitori ad intervalli prestabiliti per verificare il funzionamento e la qualità delle trasmissioni radio. Per limitare l'inquinamento acustico al di fuori dell'area portuale sono state scelte sirene direzionate.

Valutazione

I dispositivi installati permettono di dare l'allarme su tutta l'area del porto il che indirettamente contribuisce ad una maggiore sicurezza sui confini esterni del porto e permette anche il funzionamento integrale del sistema di sicurezza portuale. Ma l'attività non ha nessun effetto diretto sui rischi riscontrati per la sicurezza dei confini terrestri e marittimi del porto e nemmeno sulla riduzione dei rischi di accesso degli emigrati e sull'efficacia dei controlli sull'area portuale.

- **Adattamento del drone alle necessità del porto, sistemazione del centro di controllo e formazione dei piloti (WP 3.1.5.2)**

Nell'ambito del progetto è stato fatto un adattamento dei droni alle condizioni del Porto di Trieste che AdSP MAO ha acquistato con fondi propri. L'adattamento ha compreso la rielaborazione dei droni in base alle condizioni ambientali nel Porto di Trieste (presenza di antenne, sistemi radio, navi di diverse grandezze e ostacoli, come ad esempio gru, ecc.) e l'allestimento con la camera termica ad infrarossi.

Nell'ambito delle attività è stato allestito anche il centro di controllo nella Torre del Lloyd con il software e relativo supporto tecnico, dove sarà possibile elaborare i dati della video sorveglianza invitati in formato digitale dai droni. La sala di controllo gestisce i dati raccolti ed esegue alcune funzioni che di norma vengono svolte dalle torri di controllo per il traffico aereo, le loro attività si basano su protocolli prestabiliti e sul sistema informatico per la registrazione delle attività operative in cloud.

Valutazione

L'allestimento implementato permette il sorvolo dell'area del porto e l'analisi dei rilievi video in tempo reale. In questo modo vengono garantiti controlli aggiuntivi sui confini terrestri e

marittimi di tutto il porto e la scoperta di accessi potenzialmente non autorizzati. Il sistema permette anche il rilievo termografico dell'infrastruttura ai fini della sicurezza e della valutazione tecnica. Con i droni ed il sistema di controllo nonché i rilievi si riducono tutti i rischi rilevati nel porto di Trieste.

Considerato il risultato ottenuto si propone l'implementazione di simili sistemi anche in altri porti partner.

- **Valutazione tecnica e test delle tecnologie TIC (WP 3.1.4.2)**

Nell'ambito del presente work package sono state svolte due attività pilota. La prima si riferisce all'aggiornamento della raccolta e alla connessione di raccolte dati sino ad ora non collegate di due sistemi informatici fondamentali per l'attività del porto e all'accesso a tali dati da utente esterno. Nell'ambito della presente attività, ancora, sono state pianificate anche diverse relazioni statistiche. La seconda attività pilota aveva come obiettivo il miglioramento della sicurezza dell'infrastruttura e l'armonizzazione della conservazione e del trattamento dei dati, in conformità con il regolamento GDPR. Per entrambe le attività sono state svolte vaste analisi dello stato attuale, la definizione della metodologia e l'esecuzione dell'attività. Sono stati organizzati dei corsi di formazione di cyber security per i dipendenti, il che ha contribuito profondamente alla sensibilizzazione riguardo il significato della cyber security stessa e relativo rafforzamento. Sono state elaborate delle piatteforme IT con le quali è stata migliorata e resa più efficace la gestione degli account di accesso a sistemi e dati, che vengono dati agli utenti. In questo modo è stato possibile sopprimere automaticamente gli account dei dipendenti che hanno interrotto il rapporto di lavoro. Si tratta di strumenti che hanno aumentato anche l'efficacia delle procedure di "modifica della password" che ora sono automatiche, in modo tale da non rendere più necessaria l'intercessione costante del reparto IT. E' stato creato anche un sistema, che con l'autorizzazione dell'amministratore (tanto ai dipendenti quanto ai collaboratori esterni) permette all'utente di monitorare gli accessi ai sistemi IT e ai dati. In tal modo si è garantito il completo rispetto delle misure minime di sicurezza per le pubbliche amministrazioni (che sono previste anche nel GDPR), evitando anche eventuali attacchi dovuti a *privilege escalation* in occasione degli accessi ai dati da parte di utenti o virus in rete. In conformità con i rischi accertati nella relazione della gap analysis sulle norme settoriali e standard, che tratta l'ambito legale e organizzativo, e nella relazione dell'analisi dell'infrastruttura informatica con la valutazione della vulnerabilità di tutta la rete, i rischi riscontranti sono stati eliminati con contromisure per la riduzione dei livelli di rischio informatico.

Valutazione

Le attività svolte hanno avuto impatti multilevel sull'aumento della cyber secutrity e cioè con il controllo degli accessi, la gestione efficace ed il controllo dell'infrastruttura, ma anche sulla sensibilizzazione e sulla formazione dei dipendenti, nonché su procedure e tecnologie. E' stata anche svolta la valutazione della vulnerabilità di sistema con l'accertamento di carenze. In questo modo è stato sensibilmente ridotto il rischio di eventuale riuscita di un attacco cyber sui sistemi informatici del porto.

3. Porto di Venezia

- **Implementazione del sistema di controllo dell'accesso AGS nel porto con l'utilizzo del sistema di lettura delle targhe dei veicoli OCR.**

L'obiettivo delle attività era migliorare la sicurezza fisica del porto con un sistema di controllo degli accessi nell'area portuale. Nell'ambito delle attività è stato posizionato agli accessi di Sant'Andrea e San Nicolò un sistema di lettura delle targhe OCR integrato nel sistema esistente per il controllo degli accessi. Per collegare i sistemi è stato necessario sviluppare un software particolare che rileva i dati in entrata, uscita e transito. In base ai dati raccolti il sistema computa quanti posti liberi sono disponibili nelle singole aree all'interno del porto e regolamenta in questo modo gli accessi. Presso le due entrate al porto di Chioggia (Val di Rio ed Isola Saloni) sono stati posizionati dei punti di controllo informatico, dotati di tecnologia RFID con lettore di codici a barre con i quali vengono verificate le autorizzazioni d'accesso nell'aera del porto.

Entrambi i sistemi sono stati integrati in quello già esistente presso altri punti d'accesso al porto e ora compongono il sistema integrato di controllo degli accessi nell'area portuale.

Valutazione

La tecnologia implementata insieme al software sviluppato permette di svolgere controlli sistematici integrati di entrate ed uscite dal porto e contribuisce alla riduzione dei rischi di accessi non autorizzati nell'area portuale. Il sistema contribuisce anche al regolamento ed all'ottimizzazione dei flussi logistici nel porto e di conseguenza influisce sulla sicurezza dei trasporti e sulla produttività lavorativa.

Conclusioni

Tutta l'infrastruttura critica, compresi i porti, rappresenta un obiettivo pontenziale per un attacco a causa delle funzioni e dell'importanza che riveste per la società. A paragone di altre infrastrutture critiche i porti sono maggiormente esposti agli attacchi. I motivi sono diversi: al porto hanno accesso un vasto numero di persone (agenti, spedizionieri, operatori, piloti, marittimi, ecc.), diversi mezzi di trasporto (navi, mezzi pesanti, vagoni, ecc.), molta merce, l'attività dipende dallo scambio di elevate quantità di dati, dalla presenza di numerosi stakeholder e da transazioni finanziare, ecc. Proprio per tale motivo il settore della sicurezza dei porti è estremamente diversificato, complesso, molteplice e tecnicamente sofisticato.

Nell'ambito delle attività pilota del progetto SECNET i porti partner hanno testato diversi sistemi di miglioramento della sicurezza fisica e cibernetica dei porti. **La validazione dei risultati ha dimostrato che tutti i sistemi implementati hanno contribuito alla riduzione dei rischi a diversi livelli. Per tale motivo la valutazione ha dimostrato che i sistemi implementati sono efficaci nella riduzione dei rischi riscontrati.** Ma per le caratteristiche geografiche, le diverse dimensioni dei porti, le differenze presenti in terminal e attrezzatura, infrastruttura e sovrastruttura, organizzazione, in particolare per le diversità nella tecnologia informatica non è possibile traferire tutti i risultati delle attività pilota da un porto ad un altro senza adattamenti. Sicuramente la soluzione che non necessita adattamenti e può essere implementata in tutti i porti è l'utilizzo dei droni e del radar ad alta risoluzione per il controllo dell'area del porto e dei relativi confini. Mentre nel settore della cyber security è possibile trasferire tra i porti solo l'idea, l'esecuzione tecnica è condizionata dalle caratteristiche dei singoli porti su descritte.