Interreg
ITALIA-SLOVENIJA

UNIONE EUROPEA
EVROPSKA UNIJA

SECNET

Progetto standard co-finanziato dal Fondo europeo di sviluppo regionale
Standardni projekt sofinancira Evropski sklad za regionalni razvoj

SECNET Newsletter #3

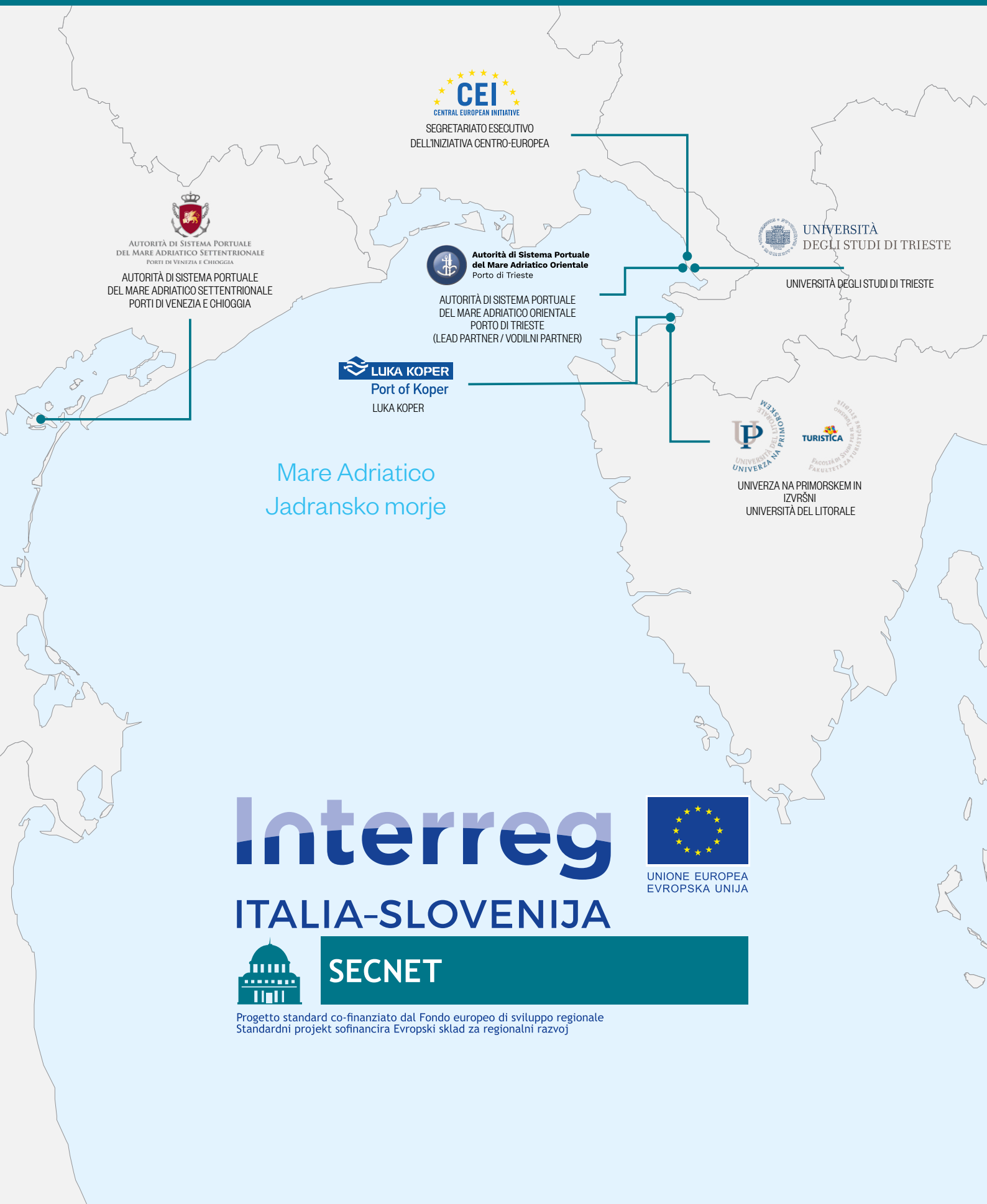
1. NOTA SINTETICA SU SECNET

2. EVENTI DI DISSEMINAZIONE E CONSULTAZIONE

3. LA SECURITY MARITTIMA DEL PORTO DI TRIESTE VALUTATA BUONA PRATICA EUROPEA

4. AVANZAMENTO DELLE AZIONI PILOTA

5. 3° E 4° COMITATO DI PILOTAGGIO SECNET A VENEZIA E A TRIESTE



Interreg

ITALIA-SLOVENIJA

UNIONE EUROPEA
EVROPSKA UNIJA

SECNET

Progetto standard co-finanziato dal Fondo europeo di sviluppo regionale
Standardni projekt sofinancira Evropski sklad za regionalni razvoj

1. NOTA SINTETICA SU SECNET

SECNET mira a **rafforzare la capacità operativa e la governance transfrontaliera della sicurezza portuale** al fine di soddisfare le raccomandazioni dell'UE per la protezione delle infrastrutture critiche e la relativa gestione del partenariato pubblico-privato.

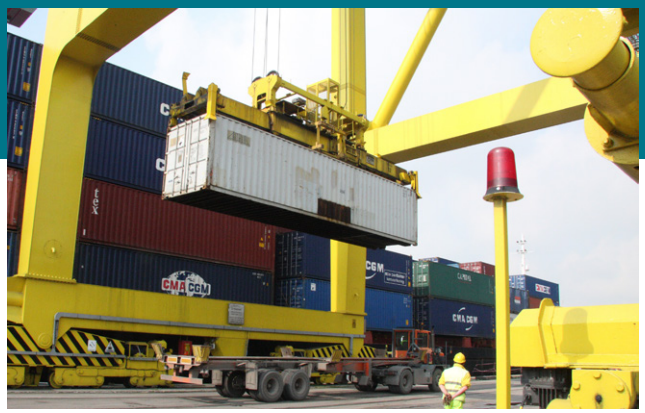
Il progetto identifica punti di forza e debolezza delle strutture marittime dell'Alto Adriatico e offre applicazioni ICT innovative, **fornendo competenza tecnica e coordinamento**. La nuova capacità viene testata attraverso **due azioni pilota: miglioramento della sicurezza informatica e sicurezza dei perimetri dei porti.**

Sarà istituita **una rete istituzionale transfrontaliera**, firmando un memorandum d'intesa che riunisce autorità portuali, istituzioni e amministrazioni pubbliche competenti anziché il settore privato dei territori interessati.

La strategia di sicurezza portuale trasformerà i risultati SECNET in polizze a lungo termine che coinvolgono Trieste, Capodistria e Venezia, ma anche altri hub marittimi come Monfalcone, Porto Nogaro e Chioggia.

La Conferenza Finale del progetto SECNET si terrà a Trieste, presso la Stazione Marittima la mattina del 28 marzo 2019.

Per saperne di più sul progetto SECNET >>



2. EVENTI DI DISSEMINAZIONE E CONSULTAZIONE

Presso la sede dell'Autorità di Sistema Portuale del Mare Adriatico Orientale a Trieste (Torre del Lloyd) lunedì 18 febbraio si è svolto il primo incontro SECNET con gli operatori economici e le istituzioni rilevanti per la sicurezza portuale. Ricordati gli obiettivi del progetto, sono state presentate le azioni pilota ed altri risultati, e le linee guida della Strategia Transfrontaliera sulla quale sono stati raccolti importanti commenti e contributi. Analoghi incontri di consultazione avranno luogo a Koper / Capodistria ed a Venezia nelle prime settimane di marzo.

La Strategia così condivisa sarà poi presentata nella Conferenza Finale del progetto.

Più informazioni sulla nostra pagina web:
www.ita-slo.eu/it/secnet

3. LA SECURITY MARITTIMA DEL PORTO DI TRIESTE VALUTATA BUONA PRATICA EUROPEA

Dal 19 al 23 novembre 2018 la Commissione Europea ha condotto un'ispezione al porto di Trieste al fine di monitorare la corretta implementazione, da parte dell'Italia, delle norme in materia di *maritime security* sia per quanto attiene le navi e gli impianti portuali (Regolamento 725/2004) sia per l'intero comprensorio portuale (Direttiva 2005/65/EC).

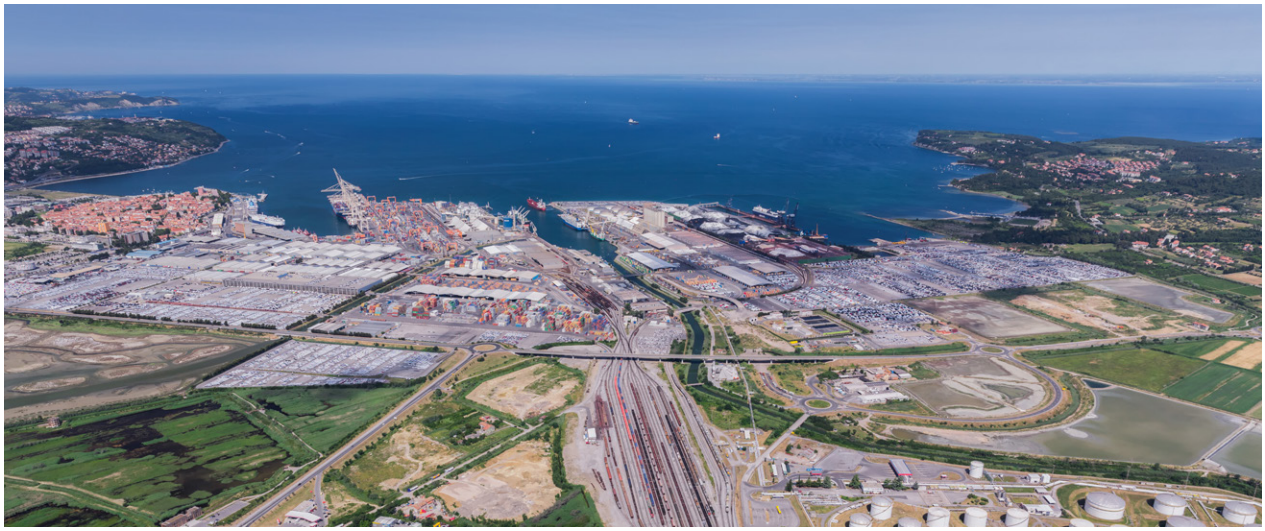
Gli esiti dell'ispezione sono stati estremamente positivi ed il rappresentante leader della Commissione Europea, nel suo discorso di chiusura, ha espresso parole di elogio sia per la Guardia Costiera che per la Prefettura, la Polizia di Frontiera, l'Autorità Portuale e tutte le altre amministrazioni che, a vario titolo, partecipano alla implementazione della normativa di settore.

Il documento di *assessment* prodotto nell'ambito del progetto SECNET è stato ulteriormente riutilizzato e, visti i risultati raggiunti, si è rilevato molto utile per la valutazione complessiva dello stato di security del Porto di Trieste.

Più informazioni sulla nostra pagina web:
http://ita-slo.eu/it/tutte-le-notizie/news/secnet-la-security-marittima-del-porto-di-trieste-valutata-buona-pratica

4. AVANZAMENTO DELLE AZIONI PILOTA:

a. Luka Koper



CYBER SECURITY PENETRATION TESTS

Questa azione pilota è finalizzata a verificare e successivamente a prevenire attacchi informatici al sistema portuale ed a tutti i sistemi ad esso collegati, verificandone le vulnerabilità ed aggiornandone il database.

In particolare, l'azione prevede lo svolgimento di cosiddetti test di penetrazione del sistema che consistono in: un controllo di sicurezza secondo il principio della "Scatola Nera" in cui vengono inclusi i controlli sulle possibilita di accesso non autorizzato ai dati o alla loro modifica; l'adeguatezza della conservazione dei dati presso postazioni di lavoro locali, per evitare ulteriori abusi del sistema; assunzione di identita degli utenti esistenti nel sistema; modifiche dei privilegi degli utenti e valutazione delle funzionalità.

Inoltre, vengono inclusi anche controlli di sicurezza dei sistemi operativi del server con l'applicazione MS Windows Server. In questo caso sono stati presi in cosniderazione tutte le certificazioni di sicurezza IT applicabili, verificando lo stato del punto di controllo e di Microsoft GOLD.

È inoltre previsto entro fine febbraio 2019 lo svolgimento di ulteriori test del sistema, con lo scopo di verificare se le vulnerabilità riscontrate durante i test di penetrazione siano state eliminate efficacemente e secondo i criteri previsti.

SICUREZZA PERIMETRALE RADAR

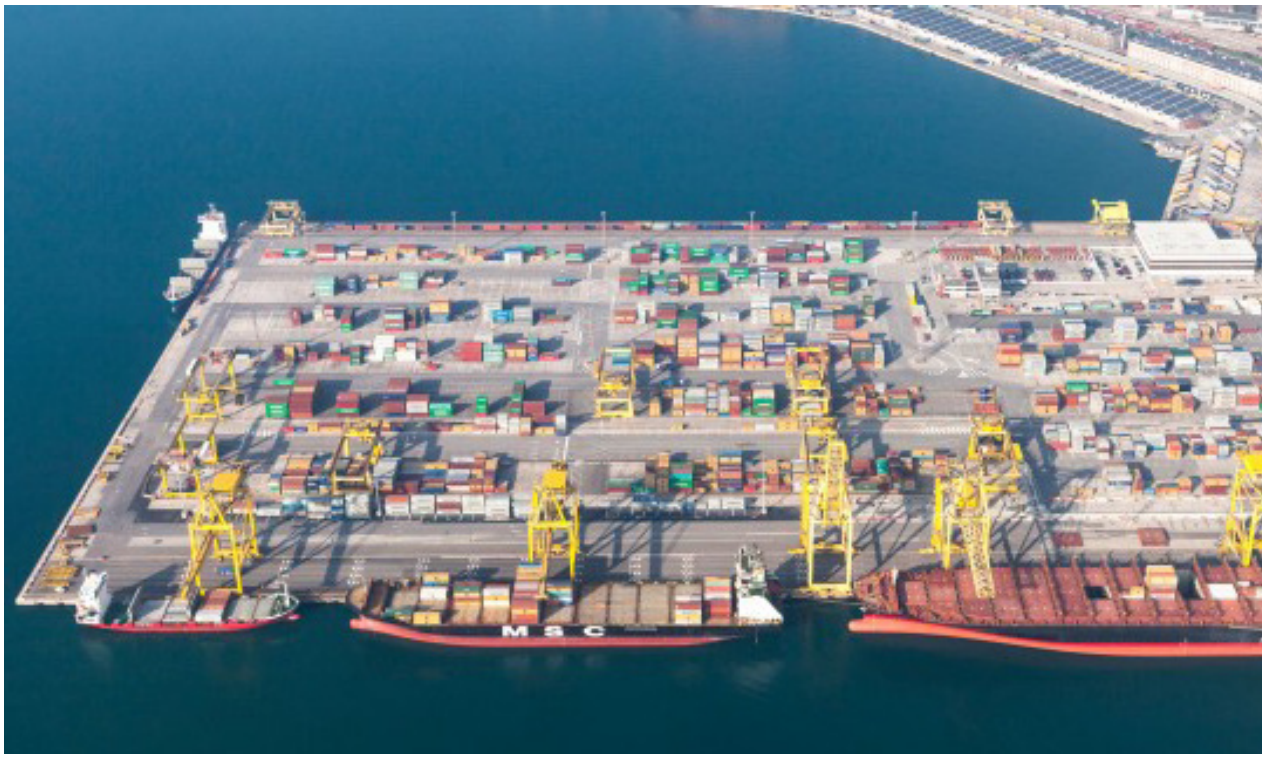
Questa azione pilota è finalizzata a dotare l'area del porto di Capodistria, nella quale si concentra la maggior parte dei passaggi di merci, mezzi di trasporto e persone, di un sistema sofisticato di allertamento radar da utilizzare in caso di necessità. Con l'evoluzione delle varie tecnologie sulla sicurezza si sviluppano parallelamente anche tutta una serie di tecnologie atte a superare o ad eludere le barriere poste per salvaguardare la sicurezza e l'integrità del sistema portuale. A tal proposito, Luka Koper d.d. ha dotato punti strategici all'interno dell'area portuale di un moderno sistema radar ad infrarossi, con l'integrazione di videocamere termografiche ad alta risoluzione, per la visione a 360° di aree specifiche nella zona portuale. Con queste videocamere, si permette al Centro di controllo di rilevare tutte le fonti di calore e movimenti nel raggio di 1.500m, in tutte le condizioni meteo, sia con visione diurna, sia con quella notturna.

Il sistema viene integrato con il collegamento a dei server in grado di immagazzinare e distribuire le grandi quantità di dati acquisite dalle attrezzature di cui sopra, con i filmati ad alta risoluzione generati 24h su 24h.

È inoltre prevista la predisposizione e compatibilità del sistema di video sorveglianza, per consentire alla postazione del Centro di controllo portuale, di visionare in tempo reale e in ogni tipo di condizione meteo e di luminosità, quelle che sono le condizioni di sicurezza e sorveglianza, nelle specifiche aree del porto di Capodistria.

4. AVANZAMENTO DELLE AZIONI PILOTA:

b. Autorità di Sistema Portuale del Mare Adriatico Settentrionale (Porto di Trieste)



CYBER SECURITY PORT IN NUMBERS

Questa azione pilota nasce dall'esigenza dell'Autorità di Sistema Portuale di dotarsi di una consolle di gestione dei dati provenienti da sistemi eterogenei. Tale piattaforma mira a permettere al fruitore di avere una esatta visione, in tempo reale, di quanto accade nelle aree portuali e nelle aree di sosta esterne al porto (c.d. buffer).

Attualmente, l'AdSP MAO dispone di due sistemi informatici: i) il Port Community System – Sinfomar; ii) il sistema di controllo degli accessi, Igate, che a breve si evolverà nel sistema Vigate.

Queste due piattaforme contengono un elevato e complesso set di dati, il cui studio correlato permetterebbe di massimizzare il controllo delle presenze in porto, anche nell'ottica di un supporto alle decisioni gestionali e di trattamento delle emergenze.

Il progetto SECNET permetterà lo sviluppo di tale portale, denominato PIN - Port In Numbers, che, in linea con la normativa vigente e in particolare con il Codice dell'Amministrazione Digitale, dovrà permettere all'utente, attraverso meccanismi di drag & drop o di trascinamento di tipo touch (in caso di accesso da tablet o smartphone) di creare una propria schermata di sintesi delle informazioni.

Questa piattaforma rappresenta uno strumento di forte comunicazione verso la collettività, intesa non solo come comunità portuale, ma anche come tessuto cittadino integrato con le aree portuali. Ha inoltre l'obiettivo di esporre i dati attraverso interfacce di semplice lettura e di facile comprensione. I dati elaborati sono, ad esempio, il numero di soggetti che hanno fatto accesso in porto, i mezzi associati e contemporaneamente quelli gestiti nell'ambito del Port Community System, provenienti dalle buffer areas, oppure direttamente dalle arterie autostradali, il dettaglio delle merci a bordo dichiarate, comprensivo di quelle pericolose, e divise per destinazione internazionale.

Il software applicativo genererà output grafici riproducibili su tv connesse ad internet, anche non appartenenti al mondo portuale, tali da poter per-

mettere ad un cittadino comune di percepire i numeri ed i grafici preconfezionati ad hoc. Per tutte le funzioni utente le pagine saranno disponibili in lingua italiana ed inglese.

CYBER SECURITY - GDPR

Questa azione pilota è focalizzata sui servizi di Security & Compliance Consulting e in particolare mira ad assicurare l'adeguamento dell'infrastruttura IT del Porto di Trieste rispetto alle previsioni di cui a:

I. il Regolamento (UE) n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (c.d. GDPR);

ii. il D. Lgs. n. 196/2003 (c.d. Codice della Privacy), in particolare per quanto riguarda la direttiva sul monitoraggio degli accessi degli amministratori di sistema.

L'azione pilota è strutturata in due aree principali:

1. **Servizi On Demand:** ossia tutti i servizi di supporto ad alto valore aggiunto definiti per le seguenti aree di intervento:

- •istruzioni operative per governare il processo di analisi e gestione del rischio (Security Risk Management);
- verifica dell'attuale stato di implementazione e coerenza con le normative esistenti in materia di cyber security (Gap Analysis);
- adeguamento dei punti di criticità emersi per l'innalzamento della sicurezza applicativa (Remediation Consulting).

2. **Servizi Continuativi:** ossia tutti i servizi che assicurano la continuità operativa presso la sede dell'Autorità di Sistema Portuale, al fine di offrire un servizio di presidio e/o di supporto dedicato a specifici ambiti della sicurezza/compliance, quali:

- •gestione del mantenimento dello stato di conformità raggiunto dai sistemi dell'AdSP, al fine di supervisionare la garanzia nel tempo dello stato di adeguatezza di quanto implementato (Compliance Maintenance Support);
- •gestione delle campagne di audit di sicurezza e conformità rispetto alle normative vigenti o agli standard interni definiti (Security & Compliance Audit).

Grazie al progetto SECNET è stato quindi redatto un importante documento di assessment, la ''Valutazione di Sicurezza del Porto di Trieste – Allegato 4 Approfondimento, Cyber Risk Management'', che ricostruisce lo stato di fatto del Porto di Trieste. Questo elaborato è stato utilizzato anche dal Data Protection Officer (DPO) dell'AdSP MAO per le fasi propedeutiche all'applicazione del GDPR di recente entrato in vigore.

In occasione di un'ispezione della European Maritime Safety Agency (EMSA), svoltasi a novembre 2018, il CIO (Chief Information Officer) dell'AdSP MAO ha illustrato le componenti del documento e gli sviluppi successivi alla stesura, che si sono rivelati molto utili per la valutazione complessiva dello stato di security del Porto di Trieste e ha riscontrato grande apprezzamento da parte della Commissione europea

SICUREZZA PERIMETRALE SIRENA

Questa azione pilota è finalizzata a dotare le aree portuali nelle quali si concentra la maggior parte delle operazioni di un sistema di allertamento da utilizzare in caso di emergenze, di cui finora il Punto Franco Nuovo risultava sprovvisto.

In particolare l'azione prevede la fornitura e l'installazione di due c.d. gruppi di emissione, costituiti da sirene elettroniche direzionali in alluminio, sui tetti di due diversi edifici del Porto Nuovo, in modo da garantire la copertura del segnale acustico in tutti i terminal e le aree operative ivi compresi.

Il sistema di allertamento è attivato e gestito dalla sala di controllo ubicata nel complesso della Torre del Lloyd, esterno al perimetro delle aree operative. Pertanto, l'azione comprende anche l'installazione di un software applicativo, con relativo attivatore via radio, in grado di azionare il sistema di allertamento e controllare le unità sirene e ripetitori ad intervalli di tempo prestabiliti per verificare lo stato funzionale (stato alimentazione, stato batterie e stato trombe) e la qualità della tratta radio.

È inoltre prevista la predisposizione di un sistema volto a consentire agli utenti il completo controllo da remoto delle sirene tramite la rete dati dell'Autorità di Sistema Portuale.

Sono state scelte trombe direzionali per limitare l'inquinamento acustico all'esterno dell'area portuale.

SICUREZZA PERIMETRALE DRONI

Questa azione pilota mira a rendere più efficienti ed efficaci le operazioni di verifica diretta del funzionamento degli impianti portuali e quindi migliorare la capacità di intervento dell'Autorità di Sistema Portuale di nello svolgimento dei propri compiti di manutenzione e security portuale, in particolare attraverso periodiche azioni di vigilanza dell'ambito portuale svolte con l'ausilio di droni (in gergo tecnico, sistemi di pilotaggio a controllo remoto – SAPR).

I droni sono stati acquistati dall'Autorità di Sistema Portuale con fondi propri (30.000 euro) e in seguito adattati alle condizioni ambientali operative del Porto di Trieste (presenza di antenne, sistemi radar, navi di varia dimensione e stazza, sovrastrutture come le gru, ecc.), grazie ai fondi del progetto SECNET. Tali sistemi acquisiscono dati di videosorveglianza in formato digitale che vengono poi elaborati da una postazione di controllo situata nella sede della AdSP MAO e il cui allestimento, comprensivo della dotazione software e della relativa assistenza tecnica, è stato reso possibile dai fondi del progetto SECNET.

L'AdSP MAO ha inoltre promosso iniziative di formazione rivolte ai propri dipendenti, e strutturate in due corsi, in parte finanziati dalla Regione Friuli Venezia Giulia mediante il Fondo Sociale Europeo (10.000 euro).

in due corsi, in parte finanziati dalla Regione Friuli Venezia Giulia mediante il Fondo Sociale Europeo (10.000 euro).

4. AVANZAMENTO DELLE AZIONI PILOTA:

c. Autorità di Sistema Portuale del Mare Adriatico Settentrionale (Porto di Venezia)

SICUREZZA PERIMETRALE

L'azione pilota avviata da AdSP MAS nasce dalla necessità di incrementare la sicurezza fisica e il monitoraggio dell'utilizzo di alcuni varchi dell'area portuale, attraverso l'implementazione dell'attuale sistema di controllo accessi con l'aggiunta di una componente per la lettura delle targhe e l'aggiornamento dell'attuale componente di richiesta e gestione del rilascio dei permessi di accesso temporaneo. I varchi interessati dall'azione pilota sono i varchi dell'area portuale di Venezia e precisamente il varco Sant'Andrea, il varco 34/17 e il varco San Nicolò.

Con l'intervento realizzato in SECNET, il sistema di controllo accessi sarà dotato di una componente per il controllo del traffico veicolare che permetterà di validare il transito dei mezzi sia attraverso la lettura automatica delle targhe sia attraverso i più tradizionali "badge" nonché di gestire e monitorare l'impiego delle aree di parcheggio a disposizione all'interno dell'area portuale.

A livello operativo, l'azione pilota si è articolata nell'implementazione della parte software dell'intervento e nell'installazione fisica di telecamere e dispositivi per permettere il monitoraggio.

Con le automazioni apportate dal progetto SECNET, AdSP MAS ha migliorato le modalità di monitoraggio degli accessi nell'area portuale veneziana, garantendo al contempo la riduzione dei tempi amministrativi per il rilascio dei permessi nonché un maggiore controllo dei transiti.

5. 3° e 4° Comitato di Pilotaggio SECNET a Venezia e a Trieste

Gli ultimi Comitati di pilotaggio dei partner del progetto SECNET si sono svolte il 18 settembre 2018 e l'8 gennaio 2019 presso le sede del Porto di Venezia e quella del Porto di Trieste. I partner hanno discusso sullo stato di avanzamento delle attività pianificate e sullo stato di avanzamento delle due azioni pilota previste in ogni porto prima della conferenza finale.

Interreg
ITALIA-SLOVENIJA
UNIONE EUROPEA
EVROPSKA UNIJA
SECNET
Progetto standard co-finanziato dal Fondo europeo di sviluppo regionale
Standardni projekt sofinancira Evropski sklad za regionalni razvoj

PARTNER

Autorità di Sistema Portuale del Mare Adriatico Orientale – Porto di Trieste,
Autorità di Sistema Portuale del Mare Adriatico Settentrionale – Porti di Venezia e Chioggia,
Università degli Studi di Trieste,
Luka Koper,
Università del Litorale e Segretariato Esecutivo dell'Iniziativa Centro-Europea InCE.

Durata: 18 mesi – 01/10/2017-31/03/2019

Budget: circa 1,3 milioni di euro

CONTATTACI

Autorità di Sistema Portuale del Mare Adriatico Orientale – Porto di Trieste
Dott. Alberto Cozzi
acozzi@porto.trieste.it
+39 040 673.26.17

seguici su: