COMUNICATO STAMPA

ADSPMAM: LA SICUREZZA NEI PORTI DIVENTA ANCHE DIGITALE. ACCORDO INNOVATIVO E PIONIERISTICO TRA ADSPMAM E POLIZIA DI STATO PER PREVENIRE E CONTRASTARE I CRIMINI INFORMATICI.

Questa mattina, nella sede di Bai dell'Autorità di Sistema Portuale del Mare Adriatico Meridionale (AdSPMAM), il presidente, Francesco Mastro, e il dirigente del Centro Operativo per la Sicurezza Cibernetica Puglia (C.O.S.C.) della Polizia di Stato, Marco De Bartolis, hanno sottoscritto un Protocollo d'Intesa per la "*Prevenzione e il contrasto dei crimini informatici sui sistemi informativi critici dipendenti dall'Autorità del Sistema portuale del Mare Adriatico Meridionale*".

L'obiettivo è quello di rendere i porti del Sistema dell'Adriatico meridionale (Bari, Brindisi, Manfredonia, Barletta, Monopoli e Termoli) ulteriormente schermati e protetti rispetto ai crimini informatici che possono colpire i sistemi digitali e le infrastrutture tecnologiche dell'Ente.

Alla sottoscrizione dell'accordo erano presenti il questore di Bari, Annio Gargano, e il direttore del Dipartimento Sviluppo e Innovazione Tecnologica dell'Ente portuale, Mario Paolo Mega.

L'accordo, che introduce un modello strutturato di collaborazione per la tutela di sistemi considerati "critici" per il funzionamento dei porti si colloca in un contesto normativo nazionale ed europeo in continua evoluzione, anche alla luce della recente direttiva NIS2 (misure per un livello comune elevato di cybersicurezza nell'Unione) che punta sul rafforzamento della *cybersecurity* a livello europeo. Con la NIS2, l'Autorità di Sistema, infatti, non è più solo un ente amministrativo, ma diventa un soggetto essenziale, responsabile della postura di *cybersecurity* dell'intera area portuale, considerata infrastruttura strategica.

Tra i principali interventi previsti dal documento: la condivisione e l'analisi di informazioni utili a prevenire attacchi informatici e tentativi di accesso illecito; l'attivazione di canali di comunicazione tempestivi per la gestione di eventuali situazioni di crisi; la segnalazione e il monitoraggio di vulnerabilità, minacce e incidenti *cyber*; il supporto nell'individuazione dell'origine di eventuali attacchi ai sistemi dell'Autorità portuale.

Tra le infrastrutture tecnologiche da proteggere, per via della sua funzione strategica e della complessità delle informazioni trattate, vi è il *Port Community System GAIA*, la piattaforma digitale, implementata e attivata dall'AdSPMAM, che gestisce, tra le altre funzioni, i processi di imbarco e di bigliettazione nei porti di Bari e di Brindisi, il monitoraggio dei flussi di passeggeri e mezzi e l'interoperabilità tra i diversi soggetti istituzionali che operano in ambito portuale, integrando processi e flussi informativi con le Forze di polizia, l'Autorità marittima, l'Agenzia delle Dogane e gli altri enti di controllo.

GAIA, quindi, rientra tra le infrastrutture digitali "critiche" dell'Ente e costituisce uno degli ambiti prioritari di applicazione del protocollo, in termini di prevenzione, monitoraggio e risposta a potenziali minacce informatiche.

L'accordo prevede, inoltre, attività di formazione congiunta, finalizzata a rafforzare le competenze del personale e migliorare la capacità di prevenzione e di risposta agli incidenti informatici, nonché lo sviluppo di eventuali soluzioni tecnologiche condivise.

"*I nuovi scenari di crisi internazionale ci stanno insegnando con chiarezza che tra i primi obiettivi sensibili ci sono le architetture tecnologiche*- commenta il presidente Francesco Mastro. *Per un Sistema portuale, questo significa proteggere i dati, ma soprattutto garantire la continuità e la sicurezza delle operazioni di transhipment, di imbarco e di sbarco. Un attacco informatico ai porti non avrebbe effetti limitati a una singola realtà, ma rischierebbe di mettere in seria difficoltà l'intero sistema Paese. Per questo*- conclude il Presidente- *abbiamo scelto di rafforzare la collaborazione con la Polizia di Stato, puntando su prevenzione, tecnologia, condivisione delle informazioni e capacità di risposta immediata"*.

Elemento qualificante dell'intesa è l'adozione di un approccio basato sulla "sicurezza partecipata" che punta a mettere a sistema competenze e risorse per garantire la continuità operativa dei servizi portuali e la protezione dei dati e delle infrastrutture digitali.

Il protocollo ha durata triennale, contribuisce al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati attraverso sistemi informatici e di telecomunicazioni, non comporta nuovi oneri a carico ne dell'Ente portuale ne della Polizia di Stato e si inserisce tra le prime esperienze di collaborazione strutturata tra un'Autorità di Sistema Portuale e la Polizia per la Sicurezza Cibernetica, configurandosi come un modello di riferimento a livello nazionale.