PERIODICO MARITTIMO INDIPENDENTE A DIFFUSIONE INTERNAZIONALE
A BILINGUAL SHIPPING NEWSPAPER
L'INFORMATORE NAVALE
FONDATO NEL 1964 di NAPOLI

La cyber security per il cluster marittimo nazionale

Roma, 24 maggio 2017 – Il cluster Marittimo non è immune dalle gravi minacce derivanti dagli attacchi informatici ed ormai tutte le istituzioni internazionali e nazionali si stanno attivando con indicazioni operative per fronteggiare il sempre maggiore il rischio di intrusioni informatiche nei sistemi di gestione dei traffici marittimi.

Questo il tema del Seminario "La cyber security per il cluster marittimo nazionale" organizzato il 24 maggio 2017 da Confitarma al quale sono intervenuti numerosi rappresentanti di imprese marittime ma anche esponenti delle istituzioni ed esperti tecnici informatici.

Il Seminario è stato introdotto da Cesare d'Amico, Consigliere Confitarma e presidente del Gruppo di lavoro "Operatività nave", che ha illustrato le tappe del percorso compiuto fino ad oggi dalle aziende associate a Confitarma nel campo della *maritime security,* a partire dall'introduzione dell'ISPS Code, ricordando come "la metodologia sperimentata da Amministrazione e industria per individuare ed attuare insieme le misure di contrasto alla pirateria marittima nei mari del mondo si sia rivelata vincente e debba quindi essere presa a riferimento anche nella gestione di questa nuova minaccia per il cluster marittimo".

Francesco Chiappetta, dell'Istituto Italiano di Navigazione, ha svolto una analisi della minaccia informatica per il comparto marittimo evidenziando, alla luce delle recenti direttive IMO, l'impatto strategico dei rischi e della minaccia di un attacco cyber sia ai classici sistemi informatici che ai sistemi di governo della nave.

Il Prefetto Sandra Sarti, Vice Capo di Gabinetto del Ministero dell'Interno, ha richiamato l'importanza che hanno avuto, sul piano normativo, l'architettura di sicurezza cibernetica deputata alla prevenzione degli eventi dannosi ed alla difesa dello Stato da attacchi nello spazio cyber, alla prevenzione e repressione dei crimini informatici, alla preparazione e alla risposta nei confronti di eventi cibernetici; sul piano politico, il coordinamento politico-strategico della presidenza del Consiglio e, sul piano operativo, il servizio della Polizia postale e delle comunicazioni e della Polizia di Stato competente su macro aree criminali, tra cui *hacking* e crimini informatici, *financialcybercrime* e cyberterrorismo.

cliccare per ingrandire

Nunzia Ciardi, Direttore Generale della Polizia Postale, ha parlato della minaccia cyber per la sicurezza nazionale e del ruolo delle strutture di Law enforcement nella tutela delle infrastrutture critiche nel quadro delle nuove prospettive delineate dalla Direttiva NIS. "E' fondamentale consolidare una vera e propria cultura della gestione del rischio informatico. Soltanto attraverso questa crescita sarà possibile l'effettiva implementazione di un sistema pubblico/privato per l'innalzamento dei livelli di sicurezza informatica del Paese".

Il Cv Attilio Montalto, Capo Ufficio 3°, Maritime security del VI Reparto Sicurezza della Navigazione, e il Tv Annalisa Vitale, organizzazione di sicurezza & VII Reparto, del Corpo delle Capitanerie di Porto-Guardia Costiera, hanno parlato del *Maritime cyber risk management* e del recente censimento sul livello di security della flotta italiana e delle compagnie di navigazione nazionali.

Luca Lombardi, della società ISIA Group, esperto di sistemi di sicurezza, ha affermato che "nel momento in cui le compagnie di navigazione prendono coscienza della nuova minaccia informatica, possono considerare la cyber security come un'opportunità consapevole di crescita organizzativa, tecnologica e delle competenze a terra e a bordo".

Concludendo il Seminario, Luca Sisto, vice direttore e Capo servizio Politica dei trasporti di Confitarma, dopo aver ringraziato tutti i relatori e gli intervenuti, ha ricordato l'invito rivolto da Cesare d'Amico alle Amministrazioni competenti affinché si collabori nell'individuazione degli interventi più utili a mitigare la minaccia informatica "Tale collaborazione potrebbe essere l'occasione proficua per condividere un gruppo di lavoro, in primis con il Sesto Reparto del Comando Generale delle Capitanerie di Porto, atto ad individuare un percorso condiviso per l'implementazione delle misure minime necessarie da attuare".