Polizia di Stato

“Guerra” tra istituzioni nello spazio virtuale: gli esiti della simulazione

Il 4 luglio sì è svolta a Roma, presso la Scuola di Perfezionamento delle Forze di polizia, un’importante tavola rotonda sul tema della resilienza delle infrastrutture critiche informatiche alle crisi di natura cyber, organizzata dalla Direzione centrale della polizia criminale e dal Servizio Polizia postale e delle comunicazioni.

L’evento nasce dalla volontà di condividere con tutti i più importanti stakeholders istituzionali gli esiti della prima esercitazione cyber su vasta scala finalizzata allo stress test delle difese a protezione delle Banche Dati interforze che si è svolta a Roma alla fine dello scorso mese di maggio. Nell’esercitazione, organizzata dai promotori della tavola rotonda odierna, in collaborazione con l’azienda Leonardo, è stata data vita a una vera e propria battaglia combattuta nello spazio virtuale che ha simulato un attacco informatico che potrebbe avere conseguenze molto gravi se riuscisse ad aggirare le barriere difensive esistenti. Per l’esercizio è stato centrale il ruolo del C-Soc, il Cyber security operations center della Direzione centrale della polizia criminale, presidio operante nelle 24 ore a tutela del patrimonio informativo delle Forze di polizia; strategico il ruolo della Polizia postale, organo preposto anche alla risposta a eventuali attacchi cibernetici ai danni del ministero dell’Interno. Supportata dagli esperti di Leonardo, impegnati ogni giorno nel rispondere alle minacce ibride in contesti strategici come aerospazio, difesa e sicurezza, l’esercitazione ha visto attaccanti e difensori sfidarsi utilizzando le piattaforme tecnologiche in grado di simulare scenari operativi molto complessi.

Al consesso, moderato dal giornalista Gabriele Carrer di *formiche.net,* hanno partecipato rappresentanti di tutte le Forze di polizia, dell’Agenzia per la cybersicurezza nazionale, del Comando operazioni in Rete dello Stato Maggiore della difesa, delle agenzie di intelligence, del Clusit – Associazione italiana per la sicurezza informatica e di Leonardo, partner tecnologico dell’iniziativa.

“Non basta disporre di tecnologie all’avanguardia” ha evidenziato Stefano Moni, direttore dell’Ufficio protezione dati della Direzione centrale della polizia criminale *“occorre mettersi alla prova, effettuare stress-test non solo sui sistemi, ma anche sulle procedure, sulla reattività di donne e uomini che tutelano le nostre infrastrutture critiche informatiche”*. In effetti, il tema del fattore umano e di processi efficaci è risultato centrale poiché è dimostrato che per fronteggiare la minaccia occorrono processi snelli e tempi di risposta rapidissimi: “*fare sistema tra le diverse componenti sia interne all’Amministrazione che con gli organi preposti a tale attività strategica è l’unica strada possibile”,* ha aggiunto Stefano. Moni.

A 35 anni dal primo attacco cyber mai registrato, avvenuto nel novembre del 1988, le statistiche del Clusit, illustrate dal prof. Corrado Giustozzi, mostrano che il 2022 è stato un anno particolarmente critico sul tema degli attacchi cyber in Italia, aumentati del 168 per cento rispetto all’anno precedente, e hanno avuto come primo obiettivo proprio la pubblica amministrazione centrale e locale, a riprova della necessità di un sistema ben coordinato a tutti i livelli per opporre una risposta efficace ad una minaccia così pervasiva.

L’Acn si sta muovendo anche in questa direzione, ha detto il direttore del Servizio operazioni dell’Agenzia per la cybersicurezza nazionale, Gianluca Galasso e, in particolare, il tema delle esercitazioni e della formazione è centrale nei programmi dell’Agenzia.

“In tema di esercitazioni cyber, il Comando operazioni in Rete dello Stato Maggiore difesa vanta una grande e lunga esperienza, anche in ambito internazionale, con i partner NATO. La centralità della formazione, del fattore umano e della necessità di verifiche periodiche è certamente un punto focale, oltre naturalmente ad una dotazione tecnologica d’avanguardia” ha detto il generale di brigata aerea Antonio Caruso, “*ben vengano occasioni come questa tavola rotonda in cui è possibile gettare le basi per nuove sinergie anche tra Forze armate e Forze di polizia, specie in tema di formazione e condivisione di migliori pratiche*”.

“Esercitazioni di questa portata sono essenziali per sviluppare la capacità di prevenire o rispondere ad un attacco informatico. Addestrarci alle migliori strategie e a volte anche sbagliare, in un ambiente simulato, prepara a difendersi da attività ostili di varia portata e natura che minacciano l’ambiente cibernetico, nel quale sono immerse le nostre pubbliche amministrazioni, le realtà aziendali private e anche, ormai, le vite di ogni cittadino. Misurarci sul campo permette di verificare oltretutto i nuovi modelli organizzativi e l’efficacia della formazione erogata al personale che sta costruendo la nuova struttura di sicurezza cibernetica del Ministero dell’Interno, che avrà il compito di affiancare in momenti critici le strutture all’avanguardia come il C-Soc che quotidianamente presidiano i perimetri cibernetici dell’amministrazione”, ha sottolineato Ivano Gabrielli, direttore del Servizio polizia postale e delle comunicazioni.

“*Di fronte alla minaccia cibernetica, sempre più pervasiva e sfaccettata, è fondamentale per il Paese disporre di competenze e tecnologie in grado di garantire la protezione dei dati strategici elevando il livello di sicurezza degli ecosistemi digitali. Da sempre a supporto delle Forze dell’ordine e delle Forze armate, Leonardo è fiera di mettere a disposizione le proprie competenze e tecnologie, per la protezione delle infrastrutture critiche, dei cittadini e dei territori*” ha dichiarato Tommaso Profeta, managing director della Divisione cyber & security solutions di Leonardo.

04/07/2023