Il Sole 24 ORE

diffusione:87661
tiratura:129277

Una rete nazionale di centri di competenza

Regia integrata per la cybersecurity nazionale

Rocco De Nicola*
Paolo Prinetto**

La difesa di un moderno e avanzato Stato sovrano contro gli attacchi cyber, perpetrati da organizzazioni criminali sempre più strutturate e articolate, richiede la realizzazione di un complesso mosaico (il cosiddetto eco-sistema cyber nazionale), che, grazie al contributo di soggetti e attori diversi, si deve urgentemente comporre per supportare la politica nazionale cyber. La struttura portante di questo eco-sistema è costituita da una solida e consolidata rete di Centri di competenza di varia tipologia e natura.

Questa rete deve ruotare attorno al Centro nazionale di ricerca e sviluppo in cybersecurity che costituisce uno dei pilastri basilari di tutto il processo di implementazione del Piano nazionale per la protezione cibernetica e la sicurezza informatica, così come definito nel Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017. Questo Centro di ricerca e sviluppo, caratterizzato da una struttura centralizzata, multidisciplinare, con adeguata massa critica, in parte governativa e in parte legata al mondo della ricerca sia pubblica sia privata, ha come compito principale la ricerca avanzata, lo sviluppo di piattaforme e di adeguate soluzioni architetturali, di applicazioni e di azioni di varia natura, tutte di respiro ampio e di interesse nazionale. Il Centro avrà ovviamente anche il compito di assistere i *policy-maker* e i vari *stakeholder* pubblici nelle attività di analisi, ricerca scientifica, sviluppo, scouting tecnologico e ingegnerizzazione dei sistemi, tenendo conto del panorama internazionale.

In termini di personale, il Centro dovrà essere in grado di attrarre ricercatori e investitori pubblici e privati (nazionali) per sviluppare ricerche di punta su tematiche di interesse strategico nazionale nel settore cyber. Al riguardo, è auspicabile che vengano definiti e resi operativi con urgenza meccanismi agili e flessibili che permettano a ricercatori e docenti di università e di enti di ricerca pubblici di ottenere il distacco temporaneo presso il Centro, senza penalizzazioni né per il personale distaccato né per i rispettivi enti di provenienza. Seguendo l'esempio dei Federally funded research and development center (Ffrdc) statunitensi, il Centro dovrà essere la punta di diamante nel panorama nazionale, mentre, a livello internazionale, dovrà attivarsi per implementare le necessarie sinergie con omologhi centri presenti nei principali paesi e, a livello nazionale, con altri centri di ricerca presenti sul territorio.

Dal punto di vista dell'ecosistema cyber nazionale, il Centro dovrà essere il punto di riferimento di una costellazione di altri Centri territoriali di competenza in cybersecurity, distribuiti sul territorio con valenza di citta metropolitana, regionale o interregionale e da un insieme di Centri verticali di competenza in cybersecurity.

I Centri territoriali di competenza in cybersecurity dovranno essere caratterizzati da (almeno) due *mission* ben definite connesse con il supporto all'economia e all'amministrazione locale e quello della sensibilizzazione dei cittadini. Per gli aspetti economico-amministrativi, questi centri territoriali dovranno contribuire a mettere in grado le imprese e la Pubblica amministrazione locale di fronteggiare le sfide poste dall'evoluzione della minaccia cyber, curando in particolare il trasferimento tecnologico, la formazione, la consulenza e aiutandoli sia a proteggere il know-how e gli asset fisici e virtuali, sia a migliorare offerta e competitività. Questi centri potranno anche gestire osservatori locali sulla cybersecurity per condividere informazioni sugli attacchi tra i diversi enti, garantendo la dovuta riservatezza, e potranno contribuire all'identificazione e alla gestione di progetti di ricerca e di trasferimento tecnologico di interesse strategico locale, nonché organizzare corsi e seminari sul territorio e promuovere attività di formazione permanente, a diversi livelli di approfondimento, per le imprese e le Pa locali. Per gli aspetti di sensibilizzazione, i centri territoriali dovranno identificare e mettere in atto le strategie più adatte per far crescere, in tutti i cittadini, la consapevolezza dei rischi cyber.

Dal punto di vista della sostenibilità economica, ciascuno di questi centri territoriali dovrà avere, da parte degli enti pubblici di riferimento, un supporto finanziario iniziale garantito per almeno cinque anni per af-frontare le spese per il personale e quelle delle infrastrutture. Tale supporto potrà poi andare a scalare, assumendo che, a partire almeno dal terzo anno, il centro abbia acquisito una capacita di cofinanziamento significativa grazie ai servizi verso le imprese e la Pa e alle attività di trasferimento tecnologico. Anche nel caso dei centri territoriali potrebbero essere previsti meccanismi di distacco temporaneo per ricercatori e docenti di università ed enti di ricerca.

** Docente di Informatica Imt Scuola Alti Studi Lucca*
*** Politecnico di Torino, Presidente del Cini*

RISCHIO ITALIA

L'impatto economico
Il rapporto Clusit indica una stima di 10 miliardi di euro di danni da attacchi informatici per l'Italia nel 2017. Il 62% degli attacchi ha provocato danni superiori a 80mila euro ciascuno: il 17% delle violazioni ha comportato il coinvolgimento di oltre la metà dei sistemi di un'azienda

La complessità
Il 92% delle aziende intervistate nel Cisco Security Capabilities Benchmark Study 2018 ha ammesso di aver subito un attacco. Il 12% delle aziende gestisce più di 21 fornitori, la percentuale più bassa in Europa. Ma in Italia solo il 58% delle segnalazioni di sicurezza viene investigato. Il 50% delle aziende ha dovuto gestire un'interruzione di oltre cinque ore nell'ultimo anno a causa di una violazione

Carenza di preparazione
Per il 24% delle organizzazioni italiane, secondo Cisco, la mancanza di personale specializzato è uno dei maggiori ostacoli alla sicurezza

90%

LE AZIENDE FRODATE
Oltre il 90% delle aziende è stato colpito da frodi via mail nei primi t5re mesi di quest'anno, con un iincremento del 103% su base annua, secondo le stime di Proofpoint


L'operatore vigila sul mobile aziendale