Verso una Nuova Agenzia Nazionale di Cybersecurity

- 27 aprile 2021 -

La recente proposta del Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri Franco Gabrielli che vede la creazione di un'Agenzia di sicurezza cibernetica, facente capo alla Presidenza stessa ma slegata completamente dal Ministero della Difesa e dal Dipartimento per le Informazioni della Sicurezza della Repubblica, apre a diversi spunti riflessivi che partono dalla dichiarazione di intenti dello stesso Gabrielli:

"*È arrivato il tempo di creare un'Agenzia che tratti in maniera olistica il tema della sicurezza cibernetica. Dobbiamo affrancarci da una modalità emergenziale. (...) Tale Agenzia deve attuare le capacità di resilienza, cioè reggere e resistere di fronte a minacce e attacchi di varia natura pur staccandosi dai nostri Servizi Segreti, quindi DIS e servizi informativi nazionali e internazionali. In questo modo si otterrebbe anche quell'approccio olistico e trasversale in uno scambio di competenze tra le varie forze dell'ordine, cercando una metodologia di contrasto comune. Una struttura presso la Presidenza del Consiglio con una partnership più forte tra pubblico e privato*".

Nell'intenzione di Gabrielli questa iniziativa dovrebbe da un lato dotare il Paese di una struttura difensiva del perimetro digitale nazionale e contestualmente liberare tempo e risorse agli organismi facenti capo al DIS e alle Forze Armate per consentire agli stessi di concentrarsi sulle attività di cyber-difesa e Intelligence.

[1]

Alla luce della volontà di tale separazione e al di là delle prime interviste e dichiarazioni preventive rilasciate da Gabrielli, sorge spontaneo domandarsi quale potrebbe essere il disegno complessivo dell'architettura che governerà questo nuovo organismo, soprattutto se nelle dichiarazioni di intenti viene fatto riferimento specifico alla natura olistica che esso dovrà avere. Ciò perché è sempre più chiaro che la veicolazione di attacchi nel cyber-mondo sia uno strumento utilizzato di volta in volta con maggiore frequenza da parte di organizzazioni criminali, organizzazioni con finalità terroristica, stati nemici ma anche stati amici. Echelon lo insegna, con le sue intercettazioni avvenute negli anni passati condotte dai servizi americani ai danni dei governanti di vari Paesi europei. Siamo nel terzo millennio, è sempre più chiaro che le guerre si conducono con modalità asimmetriche e quella cyber è tra le più efficaci, oltre a essere indubbiamente anche la più economica e immediata.

A seguito della dichiarazione di Gabrielli, secondo cui questa nuova Agenzia dovrà sviluppare una partnership più forte tra pubblico e privato, alcuni esperti di settore si sono posti diversi interrogativi. Ad esempio, ci si è domandato se lo scopo di questa Agenzia di Cyber-sicurezza nazionale potrebbe essere quello meramente di informare le aziende italiane allertandole con dei bollettini di sicurezza. Se così fosse, parrebbe piuttosto improbabile nella grande maggioranza dei casi che le aziende italiane siano in grado di interpretare e implementare correttamente le contromisure identificate nei bollettini di sicurezza stessi.

Se invece l'intento fosse quello di supportare attivamente le aziende italiane con interventi che vadano al di là della mera formazione e informazione, viene da chiedersi quali saranno sia la dimensione di tale Agenzia che la sua capacità di interagire proattivamente con un numero di aziende certamente più alto di quelle normalmente gestite dai Security Operation Center dei provider di sicurezza non governativi più blasonati.
In merito a questa problematica, risultano chiare le parole di Gabrielli: "(...) *diventerà preponderante una cooperazione tra pubblico e privato, in cui la capacità*

di segnalare in real time, proprio in base all'attuazione del perimetro cibernetico, i problemi di attacco delle singole aziende, dalla più piccola alla più grande, porterebbe un valore aggiunto fondamentale".

Sarebbe anche da chiarire quali potrebbero essere le difficoltà, le limitazioni tecniche, l'impegno finanziario, gestionale, strutturale e non ultimo di risorse umane necessario per fornire alle aziende italiane un servizio che a tutti gli effetti prevedrebbe la costituzione e il relativo dimensionamento di un SOC (Security Operation Center) ma anche di un NOC (Network Operation Center) nazionale. Non ultimo, resterebbe il nodo dell'eventuale disponibilità delle aziende private a lasciare gestire la propria sicurezza, almeno in parte, da un organismo statale.
Perché se dalle parole di Gabrielli si evince la volontà di costituire un perimetro cibernetico e se tale perimetro dovrà contenere anche le aziende italiane allora significa che la loro sicurezza digitale dovrà, quanto meno in parte, essere gestita da questa nuova Agenzia e che essa dovrà avere un ruolo proattivo piuttosto che passivo o meramente informativo.
A maggior ragione se da tae organismo, come dagli intenti indicati da Gabrielli, ci si aspetterà anche la capacità di valutare i rischi derivanti dalle installazioni di apparecchiature 5G che provengano da Paesi non alleati; oggi si pensa giustamente alla Cina anche se la questione Echelon è sempre dietro l'angolo come scomodo promemoria.

Per disporre di una tale capacità di valutazione si renderebbe necessaria la costituzione di sotto reparti specializzati, come vedremo più avanti. Qualche perplessità potrebbe sorgere in merito all'opportunità di separare quest'Agenzia nascente dal resto dell'ambito militare ed Intelligence, alla luce del fatto che in ambito cyber le stesse vulnerabilità utilizzate per condurre cyber attacchi alle aziende sono spesso vettori di attacco denominati "zeroday" ovvero ancora sconosciuti ai produttori di software e patch di sicurezza, che vengono utilizzati anche ai fini di spionaggio o militari.

In ogni caso, una struttura con tale importante vocazione nazionale, oltre al rilascio di corsi di formazione e bollettini di sicurezza alle componenti di tutto il perimetro protetto, dovrebbe avere anche la più ampia capacità proattiva di analisi e difesa. Conseguentemente sarebbe necessario saper progettare prima e implementare poi tutti i seguenti reparti:

1) Un team per l'analisi tecnica, in grado di eseguire un reverse engineering delle apparecchiature di telecomunicazione di fabbricazione non italiana. Se l'intento di questa nuova Agenzia fosse anche quello di valutare in autonomia (ovvero senza dipendere dalle informative di Paesi stranieri) i rischi derivanti dall'installazione di apparecchiature di rete telefonica 5G, è chiaro che sarebbe necessario dotarla di un pool di esperti sia riguardo l'hardware che il software di dispositivi elettronici. La stessa agenzia dovrebbe possedere la capacità di acquistare in proprio esemplari di tali apparecchiature, eventualmente tramite una società-ponte, ad essa non riconducibile;

2) Un team di esperti in indagini forensi incaricato di analizzare ex post il comportamento di eventuali intrusori informatici a seguito di un loro eventuale accesso ai sistemi protetti nel perimetro di competenza, risalendo sia al modus operandi (da catalogare in un archivio consultabile anche successivamente) che al processo di mappatura della rete dell'entità attaccata;

3) Un SOC il cui compito sia quello di monitorare in tempo reale i tentativi di attacco alle risorse protette entro il perimetro. Rimane aperta la questione circa la fattibilità della realizzazione di tale SOC, in virtù proprio della dimensione di carattere nazionale del perimetro di attività dell'Agenzia, che traspare dalle prime dichiarazioni di Gabrielli;

4) Un NOC con competenze gestionali dei segmenti di rete monitorati. Anche in questo caso permangono le stesse perplessità organizzative evidenziate per il SOC;

5) Un team di policy compliance, preposto sia alla formazione delle aziende private e degli organismi statali protetti, sia alla verifica della corretta implementazione delle policy di sicurezza emanate di volta in volta dall'Agenzia;

6) Un Tiger Team composto da hacker esperti il cui compito sia quello di simulare attacchi esterni per verificare lo stato di sicurezza dei sistemi analizzati. In tale team oltre al personale prettamente tecnico dovrebbero essere integrati anche alcuni esperti di social engineering;

7) Un team in grado di svolgere attività di Early Warning, composto da hacker esperti, il cui scopo sia quello di allertare tutte le componenti della stessa Agenzia dell'esistenza di nuove vulnerabilità pubblicamente dichiarate e di eventuali patch/contromisure segnalate dal produttore di software a cui la vulnerabilità si riferisce, sia per il mondo consumer che per il mondo SCADA. Il team inoltre dovrebbe impiegare personale tecnico di diverse etnie e relative lingue madre il cui task principale sarebbe quello di infiltrarsi nei più comuni ambienti virtuali di comunicazione come chat, forum e canali di disucssione (IRC e simili) o altri ambienti frequentati da hacker, allo scopo di tessere relazioni per poter entrare in possesso preventivamente di notizie relative a cyber attacchi pianificati oppure di accedere allo scambio/compravendita di vulnerabilità di tipo zeroday.

In questo senso, il distacco dell'Agenzia dal comparto militare e dal comparto Intelligence potrebbe rivelarsi una scelta controproducente, poiché verrebbe a mancare qualsiasi copertura legale alle attività di infiltrazione che spesso necessitano di elevata "elasticità giuridica" e libertà di azione.

La capacità di entrare in possesso preventivamente di notizie relative ad attacchi pianificati oppure di vettori di attacco di tipo zeroday rappresenta un vantaggio fondamentale per il successo di un'Agenzia con la vocazione esplicitata da Gabrielli. Infatti entrare in possesso di un vettore di attacco zeroday consente non solo la proattività nella "securizzazione" dei sistemi (es: produzione di firme degli zeroday da implementare in sistemi di Intrusion Detection) ma anche la produzione di armi digitali da destinare ad attività di carattere militare o del comparto Intelligence.
L'attività di infiltrazione di tale Early Watning Team appare inoltre strategica alla costituzione di un vivaio di giovani risorse umane qualificate, da reclutare per l'inserimento in organico.

Nel caso fosse possibile realizzare tutti i reparti sopracitati, rimarrebbe aperta la problematica relativa alla separazione dell'Agenzia dal mondo

militare/Intelligence. A meno di duplicare il comparto Early Warning presso gli ambienti di Intelligence e militari, soprattutto nella sua funzione di vivaio, infiltrazione e produzione di armi digitali, sarebbe preferibile integrare all'interno di tale Agenzia anche due ufficiali di collegamento per consentire al mondo militare e di Intelligence di reperire con facilità gli strumenti necessari all'espletamento delle proprie funzioni di attacco e difesa cyber.

In conclusione, in virtù degli intenti espressi dalle dichiarazioni iniziali di Gabrielli l'auspicio è che l'Agenzia in progetto possa integrare tutte le componenti sopraelencate, dotandosi di risorse operative efficienti e pienamente funzionali allo scopo di protezione prefissato, individuate e reclutate secondo criteri squisitamente tecnici scevri da legami o appartenenze politiche di alcun genere.

Roberto Preatoni
(CISINT Research Analyst)