La Cyber Intelligence a protezione del sistema Paese

In un mondo in cui la rete internet lega indissolubilmente aziende, cittadini e governi, non si può pensare di affrontare la protezione di una nazione senza coinvolgere gli organismi militari, le infrastrutture critiche e la pubblica amministrazione. Ogni singolo attore, facendo la sua parte, aiuta a innalzare la sicurezza del sistema paese ma per farlo ogni attore deve disporre di tutte, o almeno di parte, delle informazioni a lui utili per proteggersi al meglio.

Queste informazioni provengono dall'ormai nota area della Cyber Intelligence e vengono veicolate tramite la condivisione dell'informazione, o parte di essa – "Information Sharing".

Per facilitare la condivisione delle informazioni, il FIRST[1] ha creato un protocollo definito **TLP (Traffic Light Protocol)[2]**. Il TLP è basato su uno schema semplice e intuitivo che, utilizzando quattro colori (RED, AMBER, GREEN, WHTE), garantisce che le informazioni sensibili siano condivise con il pubblico appropriato. Esso fornisce uno schema semplice e intuitivo per indicare quando e in che modo le informazioni sensibili possono essere condivise, facilitando una collaborazione più frequente ed efficace.

Ad oggi, se si vuole realizzare un piano valido di Sicurezza Nazionale, bisogna vincere una sfida senza precedenti, cioè riuscire a consentire "l'Information Sharing" tra le infrastrutture critiche, i principali attori del settore tecnologico e l'intelligence militare. Per certo non è un compito semplice; non tutte le informazioni d'intelligence provenienti dall'area militare possono essere condivise, quindi bisogna attuare un piano strategico e ben orchestrato

che permetta di condividere almeno parte di queste informazioni, privandole di dati sensibili e/o riservati. Questa è la chiave di volta per un approccio corretto in termini di Cyber Security a protezione del sistema, definita anche “CyberSecurity Nazionale”.

Verso la tematica di Sicurezza Nazionale si sono mossi vari attori, in primis la NATO, con il **National Cyber Security Framework Manual**[3], l’Unione Europea con **la riforma della cyber security**[4] e anche lo stato italiano con il **piano di sicurezza nazionale**.

Ma andiamo per ordine. La NATO, come pubblicato nella pagina dedicata alla Cyber Defence[5], ha preso atto che gli attacchi cyber fanno parte di quella che viene definita “**guerra ibrida**”. Ogni alleato deve avere difese cibernetiche forti e resilienti per adempiere ai principali compiti previsti dell’alleanza, tra le quali difesa collettiva, gestione delle crisi e sicurezza cooperativa.

La Cyber Defence è stata integrata con l’iniziativa di **Smart Defence** per consentire ad ogni nazione una facile cooperazione al fine di sviluppare e mantenere capacità cyber di alto livello. Attraverso il “**National Cyber Security Framework Manual**” la NATO fornisce agli alleati informazioni sui vari aspetti della sicurezza informatica nazionale; inoltre, per far fronte alle nuove e sempre più insidiose minacce del mondo cyber, è stata istituita una struttura per rispondere tempestivamente agli incidenti di natura cyber “**NATO Computer Incident Response Capability (NCIRC)**”, al fine di protegge le reti della NATO, fornendo un supporto di difesa cibernetica centralizzato.

Tornando alla questione dell’information sharing, il settore privato è stato individuato dalla NATO come attore chiave per portare all’interno del cyberspazio innovazioni tecnologiche e competenze utili a tutti gli alleati in termini di Cyber Defence. Con quest’obiettivo, attraverso la **NATO Industry**

Cyber Partnership (NICP), sono state rafforzate le relazioni con l'industria privata agevolando le attività di formazione, information sharing, esercitazioni, ecc.

Anche l'UE ha capito che ha bisogno di strutture più solide e più efficaci per garantire una forte resilienza alle minacce cyber, promuovere la cyber security e rispondere agli attacchi cyber rivolti agli Stati membri, istituzioni, agenzie e agli organismi dell'UE. Pertanto, il 20 dicembre 2017, le istituzioni dell'UE hanno compiuto un passo importante per rafforzare la cooperazione contro gli attacchi cyber, attraverso la "**Riforma della Cyber Security**". Questa mira a creare misure atte a sviluppare una strategia di cyber security sulla base della direttiva Europea **NIS -Network and Information Security**. Inoltre, grazie ad un accordo inter-istituzionale, è stato istituito il **CERT-UE – Computer Emergency Response Team**, con il compito di difendere le istituzioni, gli organi e le agenzie dell'UE, cooperando con i CERT nazionali di ogni stato membro e con la controparte NATO, **NATO Computer Incident Response Capability (NCIRC)**.

Jean-Claude Juncker, presidente della Commissione europea, ha dichiarato: "Gli attacchi informatici possono essere molto pericolosi per la stabilità delle democrazie e delle economie rispetto alle armi convenzionali. Gli attacchi informatici non conoscono confini e nessuno è immune. Per questo motivo, la Commissione propone nuovi strumenti, tra cui un'Agenzia europea per la sicurezza informatica, per difenderci da tali attacchi".

La Commissione Europea ha pertanto deciso di rafforzare la resilienza, la deterrenza e la risposta agli attacchi cyber attraverso:

- La creazione della "**European Union Cybersecurity Agency**", parte dell'**ENISA – The European Union Agency for Network and Information Security**, centro di competenza che supporta gli Stati membri nel

rafforzamento della sicurezza informatica[6];

- La realizzazione dello "**EU-wide cybersecurity certification scheme**", schema di certificazione della sicurezza informatica a livello UE, che aumenti la cybersecurity di prodotti e servizi nel mondo digitale;
- La creazione di una **Blueprint**, piano per rispondere rapidamente e operativamente in caso di attacco cyber su larga scala;
- Una rete di "**European Cybersecurity Research and Competence Centre**", che contribuirà a sviluppare gli strumenti e la tecnologia necessari a costruire una difesa più forte possibile contro delle nuove minacce;
- Una nuova direttiva per la lotta contro le frodi tramite i mezzi di pagamento elettronici;
- Un **Framework** per una risposta diplomatica comune dell'UE alle attività informatiche dannose e per un consolidamento della cooperazione internazionale sulla cybersecurity, compreso l'approfondimento della cooperazione tra l'UE e la NATO;
- Lo sviluppo di competenze di alto livello per i professionisti civili e militari.

Anche l'Italia si è mossa in tal senso sviluppando un piano di sicurezza nazionale[7] suddiviso in 3 parti.

La prima parte, definita "**QUADRO STRATEGICO NAZIONALE (QSN)**", mira a sviluppare gli indirizzi strategici, tra i quali:

- Il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese;
- Il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
- L'incentivazione della cooperazione tra istituzioni ed imprese nazionali;
- La promozione e la diffusione della cultura della sicurezza cibernetica,
- Il rafforzamento della cooperazione internazionale in

materia di sicurezza cibernetica, e infine, il rafforzamento delle capacità di contrasto alle attività e ai contenuti illegali on-line.

La seconda parte, definita "**PIANO NAZIONALE (PN)**" mira a sviluppare gli indirizzi operativi, tra i quali:

- Potenziamento della capacità di intelligence, di polizia e di difesa civile e militare;
- Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;
- Promozione e diffusione della cultura della sicurezza informatica;
- Cooperazione internazionale, formazione ed esercitazioni;
- Operatività delle strutture nazionali di incident prevention, response e remediation;
- Interventi legislativi e compliance con obblighi internazionali;
- Compliance a standard e protocolli di sicurezza;
- Supporto allo sviluppo industriale e tecnologico;
- Comunicazione strategica e operativa;
- Implementazione di un sistema di cyber risk management nazionale.

La terza parte, definita "**PIANO D'AZIONE**" mira a:

- Revisionare il Nucleo per la Sicurezza Cibernetica;
- Accorciare la catena di comando per la gestione delle crisi cibernetiche;
- Ridurre la complessità dell'architettura nazionale;
- Unificare i CERT-N e CERT-PA per costituire il CSIRT[8];
- Istituire un centro di valutazione e certificazione nazionale ICT;
- Creare una fondazione o fondo di venture capital;
- Istituire un Centro nazionale di ricerca e sviluppo sulla cybersecurity;

- Costituire un Centro nazionale di crittografia;



Sono anche previste iniziative volte a realizzare il “**Centro nazionale di Ricerca e Sviluppo in Cybersecurity**” e il “**Centro nazionale di crittografia**”.

Il settore privato è stato visto come un attore chiave e necessario in materia di cyber security per poter organizzare un robusto e funzionale piano di sicurezza nazionale. Pertanto l’alleanza tra pubblico e privato è stata ampliata e nuovi operatori critici e strategici hanno sottoscritto convenzioni con il **Dipartimento delle informazioni per la sicurezza della Repubblica – DIS**[9].

NOTE

- [1] FIRST – confederazione internazionale di team di risposta agli incidenti informatici che gestiscono in modo cooperativo gli incidenti di sicurezza informatica e promuovono programmi di prevenzione.
- [2] https://www.first.org/tlp/
- [3] https://ccdcoe.org/multimedia/national-cyber-security-framework-manual.html
- [4] http://www.consilium.europa.eu/en/policies/cyber-security/
- [5] https://www.nato.int/cps/en/natohq/topics_78170.htm
- [6] http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity-EU%20agency%20and%20certification%20framework.en.pdf
- [7] https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pubblicato-il-nuovo-piano-nazionale-cyber.html
- [8] CSIRT – Computer Security Incident Response Team

- [9] https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html

A cura di: **Giuseppe Brando**

L’articolo La Cyber Intelligence a protezione del sistema Paese proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/la-cyber-intelligence-a-protezione-del-sistema-paese/