Pubblicato sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 il nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica che completa il quadro di riordino iniziato con Il DPCM 17 febbraio 2017 (fonte: https://www.sicurezzanazionale.gov.it/)

di Roberto Setola

IL PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

Roberto SETOLA è professore associato (settore ING-INF/04 Automatica) presso l'Università Campus BioMedico di Roma dove ricopre anche il ruolo di Direttore del Laboratori Sistemi Complessi e Sicurezza. È il Direttore Scientifico del Master universitario di II livello in "Homeland Security: Sistemi, Metodi e Strumenti per la Security ed in Crisis Management".

Il ***Piano Nazionale per la protezione cibernetica e la sicurezza informatica*** è la "roadmap" che definisce le modalità per l'attuazione, nell'ambito degli indirizzi individuati con il DPCM 17 febbraio 2017 (***Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali***), del ***Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*** (QSN - documento quest'ultimo rimasto l'unico della triade non aggiornato rispetto alla sua formulazione del 2013). In un tentativo di estrema semplificazione il Piano Nazionale rappresenta il **come** attuare le strategie previste dal Quadro Strategico Nazionale. Sicuramente apprezzabile è lo sforzo da parte dell'Amministrazione di definire in brevissimo tempo dall'adozione del nuovo DPCM anche la nuova versione del PN. Occorre però rilevare che le indicazioni previste nel Piano appaiono di non semplice lettura per almeno due ordini di fattori: In primo luogo il documento risente di una struttura istituzionale "complessa", che si articola nella presenza di una pluralità di soggetti, atti e documenti la cui semplificazione è uno degli obiettivi individuati dal Piano stesso; poi le modalità con cui sono riportati gli indirizzi operativi presenti. Infatti gli 11 obiettivi operativi sono decomposti in 34 sotto-obiettivi a loro volta espansi in 93 classi di attività: risulta così un elenco di 127 punti, senza che però sia articolata una strutturazione per priorità, soggetto competente e tempistica degli stessi.

Per altro l'assenza nel piano di qualunque riferimento temporale per l'adozione delle iniziative per il conseguimento dei diversi obiettivi operativi nonché la mancanza di indicatori atti a qualificare il conseguimento degli stessi, unitamente alla sostanziale assenza di indicazioni sulle risorse finanziarie da utilizzare (infatti l'obiettivo operativo 10 seppur titolato "Risorse" si concentra sull'analisi dei costi senza fornire elementi sulle risorse a disposizione), rappresentano gli elementi di maggior debolezza del Piano. In questo senso si evidenzia che il Piano, sebbene rappresenti un aggiornamento al mutato contesto di quello adottato nel 2013, non si sofferma in alcun modo nell'analizzare lo stato di attuazione dei diversi obiettivi strategici al fine di evidenziare la "strada già percorsa" ma si limita nell'introduzione a sottolineare che le principali direttrici dell'intervento di revisione hanno riguardato l'indirizzo operativo 5 (Operatività delle strutture nazionali di incident prevention, response e remediation) e l'indirizzo operativo 1 (Potenziamento capacità di intelligence, di polizia e di difesa civile e militare).

A rendere più complessa l'analisi del documento è l'introduzione di un "***Piano di Azione***" che "*raccoglie le iniziative individuate per garantire il necessario ed effettivo cambio di passo in termini di innalzamento dei livelli di sicurezza dei sistemi e delle reti del nostro Paese, cui la recente approvazione del citato DPCM 17 febbraio 2017 intende fornire un deciso impulso.*" Tale piano di azione individua otto obiettivi:

1. Revisione del Nucleo per la Sicurezza Cibernetica
2. Contrazione della catena di comando per la gestione delle crisi cibernetiche
3. Riduzione della complessità dell'architettura nazionale, mediante soppressione/accorpamento di organi
4. Progressiva unificazione dei CERT
5. Istituzione di un centro di valutazione e certificazione nazionale ICT
6. Fondazione o Fondo di venture capital
7. Istituzione di un Centro nazionale di ricerca e sviluppo in cybersecurity
8. Costituzione di un Centro nazionale di crittografia

Come evidenziato, questi obiettivi emergono dall'esigenza di consentire un rapido ed efficace salto di qualità dell'architettura individuando "*un nucleo essenziale di iniziative, cui attribuire carattere di priorità ed urgenza*". Questi obiettivi, che sono di forte interesse ed impatto, non coincidono però in modo puntuale con gli 11 obiettivi operativi (né con i loro sotto-obiettivi) andando così a porsi in parte come obiettivi aggiuntivi. L'impressione che emerge dalla lettura del capitolo "Piano di Azione" sembra suggerire che il legislatore abbia individuato negli otto punti elencati nel Piano di Azione le priorità per il sistema Paese sebbene le stesse vadano articolate in un quadro di riferimento che limita le capacità operative ed attuative delle singole iniziative, da qui la necessità di ricondurre (operazione che appare più formale che sostanziale) il piano di azione all'interno degli 11 obiettivi operativi.

Un ultimo aspetto di carattere generale è il costante riferimento che il documento fa alla direttiva NIS, o meglio al suo recepimento nell'ordinamento nazionale. È chiaro infatti a tutti coloro che operano nel settore che l'attuale cornice legislativa non è completa e presenta una serie di elementi di inefficienza e inefficacia (l'assenza ad esempio di una adeguata normativa sulle infrastrutture critiche da un lato e la presenza di leggi che istituiscono una pluralità di CERT solo per fare due esempi). In questo quadro l'iter legislativo per il recepimento della direttiva NIS rappresenta l'elemento, ovvero il mezzo, mediante il quale dare compimento ad un diverso assetto legislativo. Non per altro il punto operativo 6.4.c ha quale obiettivo "*Recepire la Direttiva nell'ordinamento nazionale e definire i relativi provvedimenti attuativi, armonizzando le nuove disposizioni con quelle relative alle infrastrutture critiche e strategiche (Direttiva 2008/114/CE e D.Lgs. n. 61/2011)*"

Nel seguito si illustreranno gli 11 obiettivi del piano fornendo per ciascuno di essi un sintetico commento.

IO1 – Potenziamento della capacità di intelligence, di polizia e di difesa civile e militare

L'obiettivo mira a creare un'approfondita conoscenza delle vulnerabilità – non solo del fattore tecnologico ma anche di quello umano – e delle minacce cibernetiche che le sfruttano mediante una valutazione in continuo delle stesse che includa sia i soggetti istituzionale, che i soggetti privati ed il mondo delle università e della ricerca creando a tal fine apposite piattaforme istituzionali. Pertanto è necessario sviluppare capacità di raccolta, elaborazione e disseminazione delle informazioni (cyber intelligence), nonché della gestione della conoscenza che ne deriva (knowledge management). La fase di analisi va completata con lo sviluppo delle capacità di contrasto alla minaccia cibernetica sia in termini di miglioramento delle capacità di attribuzione di un attacco cyber che le capacità di risposta integrata, secondo protocolli e regole d'ingaggio prestabiliti, adeguando il quadro normativo per creare pool d'intervento tecnici in supporto, in caso di gravi eventi cibernetici, alle amministrazioni centrali e ai gestori di servizi essenziali e di infrastrutture critiche

IO2 – Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati

Tale indirizzo si pone l'obiettivo di potenziare il coordinamento e la cooperazione non solo tra i diversi soggetti pubblici, ma anche tra questi e i soggetti privati, considerato che questi ultimi gestiscono le infrastrutture critiche nazionali. Da qui l'esigenza di favorire l'operatività dei già esistenti sistemi di collaborazione e di relazioni fiduciarie tra settore pubblico e privato nonché favorire l'attività di tavoli istituzionali, tavoli tecnici ed organismi competenti che prevedono la partecipazione di gestori di servizi essenziali, di operatori di infrastrutture critiche informatizzate nazionali (sebbene su questo aspetto nell'ottica della richiamata necessità di riduzione della complessità architetturale, sarebbe auspicabile una riduzione e una maggiore sinergia fra i diversi tavoli).
Sul piano operativo va potenziato il sistema di info-sharing, anche attraverso l'adozione di linguaggi strutturati e comuni mediante definizione di specifici standard di valutazione e format di comunicazione.
Vanno, inoltre, consolidati i canali di dialogo e consultazione tra le istituzioni ed il settore privato, nell'ottica dell'approccio "Sistema Paese", nonché favorita la partecipazione del settore privato ad esercitazioni internazionali sulle tematiche della protezione delle infrastrutture critiche informatizzate.

IO3 – Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento

Il fattore umano rappresenta un elemento essenziale per qualunque strategia efficace di sicurezza. In quest'ottica è fondamentale poter disporre sia di figure professionali qualificate che di una cultura della sicurezza a tutti i livelli. Questo si traduce in iniziative di sensibilizzazione e acculturamento mediate percorsi differenziati per cittadini, studenti, imprese e personale della Pubblica Amministrazione. D'altro canto è fondamentale formare e addestrare il personale con un focus specifico sulla tematica della cyber security sviluppando sinergie con enti universitari e di ricerca nella definizione di percorsi formativi ad hoc nonché mappando i centri di competenza nazionale al fine di creare poli di eccellenza.
In questo contesto sarebbe stato auspicabile una riflessione sui requisiti professionali da richiedere a coloro che operano su sistemi critici e sulla necessità di una loro formazione continua.

IO4 – Cooperazione internazionale ed esercitazioni

Il carattere transnazionale del cyberspace e la sua pervasività richiedono un approccio internazionale alla tematica, posto che i singoli Stati devono necessariamente agire sinergicamente per far fronte alla minaccia cyber. Il che impone il rafforzamento della cooperazione bilaterale e multilaterale instaurando rapporti strutturati di cooperazione con i Paesi membri della NATO, della UE

e con le nazioni partner anche mediante la promozione della partecipazione dei soggetti nazionali, pubblici e privati, ai Progetti ed ai finanziamenti dell'Unione Europea e di altre organizzazioni internazionali.
Organizzare, su base periodica, esercitazioni nazionali di sicurezza informatica (es. Cyber Italy), stimolando la partecipazione dei principali operatori di servizi essenziali e dei gestori di infrastrutture critiche e/o i settori strategici nazionali; nonché coordinare la partecipazione nazionale, nella componente pubblica e privata, alle esercitazioni pan-europee (Cyber Europe), con gli Stati Uniti (Cyber Atlantic) ed in ambito NATO (Cyber Coalition).

IO5 – Operatività delle strutture nazionali di incident prevention, response e remediation
L'approntamento di capacità di prevenzione e reazione ad eventi cibernetici richiede lo sviluppo di Computer Emergency Response Team (CERT) ovvero la sua evoluzione, come richiesto dalla NIS, di Computer Security Incident Response Team (CSIRT) mediante adeguamento del ruolo delle attuali strutture tecnico-operative nazionali di sicurezza cibernetica.
L'obiettivo prevede anche la definire di modalità ordinarie di acquisizione di beni e servizi da parte delle P.A.

IO6 – Interventi legislativi e compliance con obblighi internazionali
La rapida evoluzione tecnologico-informatica comporta un altrettanto veloce obsolescenza delle norme che disciplinano materie correlate alle tecnologie dell'informazione e della comunicazione. Pertanto, esse necessitano di periodiche revisioni e aggiornamenti anche alla luce della necessità di finalizzare il quadro normativo relativo alle infrastrutture critiche nazionali informatizzate nonché di semplificare e armonizzare gli adempimenti e gli obblighi gravanti su amministrazioni e imprese in materia.
Il tema riguarda anche l'introdurre nuove disposizioni per disciplinare l'impiego di strumenti di rilevazione e contrasto alle minacce cyber nonché per identificare gli strumenti tecnici, inclusi quelli relativi all'indirizzamento, necessari all'attribuzione di responsabilità in caso di violazioni di sicurezza (e delle relative sanzioni) da parte di amministratori ed utenti delle reti di interesse.
Uno specifico sottopunto, il 6.4, è dedicato agli aspetti relativi al recepimento della Direttiva NIS.

IO7 – Compliance a standard e protocolli di sicurezza
La compliance a standard e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune livello qualitativo della protezione informatica dei sistemi e delle reti. Occorre però provvedere all'identificazione, adozione, aggiornamento e verifica degli standard di riferimento, delle best practices e delle misure e requisiti minimi per la sicurezza delle reti e dei sistemi utilizzati dalla P.A. e dagli operatori di infrastrutture critiche.
Un altro aspetto è quello della certificazione degli apparati, strumenti e processi adottati sia per la gestione delle informazioni classificate che dagli operatori di servizi essenziali. Si evidenzia che il punto 7.4 non fa alcun riferimento a quanto previsto dall'art. 11 comma 2 DPCM del febbraio 2017 in merito all'istituzione di un "centro di valutazione e certificazione nazionale".

IO8 – Supporto allo sviluppo industriale e tecnologico
La garanzia dell'affidabilità e della sicurezza di componenti hardware e software impiegate da infrastrutture critiche e da soggetti che svolgono attività di rilevanza strategica per il Paese richiede la realizzazione di una catena di approvvigionamento di componenti sicure e resilienti dal punto di vista della sicurezza cibernetica, supportata da un processo flessibile e veloce di validazione, verifica e certificazione. Questo si potrà perseguire anche grazie alla costituzione di un laboratorio governativo di verifica che sottoponga ad analisi comparativa i sistemi ICT di interesse delle Amministrazioni e delle infrastrutture critiche di interesse nazionale.

IO9 – Comunicazione strategica
Per gestire correttamente un evento cyber con un impatto significativo sulla popolazione è necessario predisporre un coordinamento sulla Situation Awareness dei contenuti e delle informazioni, allo scopo di rendere efficaci i flussi comunicativi al fine di essere in grado di fornire, ove necessario o opportuno, un'informazione completa, corretta, veritiera e trasparente, senza con ciò creare inutili allarmismi che verrebbero ad amplificare l'impatto economico e sociale dell'evento stesso.

IO10 – Risorse
Punto di partenza per un'oculata pianificazione finanziaria e per la ripartizione delle risorse è l'analisi dei costi di eventi cibernetici occorsi o potenziali per poter definire coerentemente le priorità e le risorse/costi associati alle diverse misure di cyber-security e di cyber-defence per la protezione delle infrastrutture critiche e per lo sviluppo delle capacità operative fondamentali, sia per le componenti materiali e strumentali che per quelle relative al personale. Prerequisito per tale attività è lo sviluppo di una capacità di misurazione dell'impatto di eventi cyber. I punti 10.3 e 10.4 mirano all'efficientamento della spesa sfruttando economia di scala derivanti dalla condivisione di risorse materiale di personale. Non risultano previsioni su specifici finanzianti destinati al miglioramento della protezione cyber.

IO11 – Implementazione di un sistema di cyber risk management nazionale
Comprendere il rischio del sistema Paese connesso con la minaccia cyber è n elemento fondamentale per una corretta identificazione delle azioni da adottare. Questo si declina mediante l'individuazione di una metodologia di cyber risk management univoca e condivisa a livello strategico e l'adozione di il piano di valutazione dei rischi (come previsto anche dalla Direttiva NIS).©

REFERENZE

- DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" (GU n.87 del 13-4-2017).
- Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionale (G.U. n. 125 del 31 maggio 2017).
- Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico (QSN) (G.U. n. 41 del 19 febbraio 2014).
- Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS).