IL QUADRO STRATEGICO NAZIONALE PER LA *CYBERSECURITY*

di Roberto Setola

Presidenza del Consiglio dei Ministri - Dipartimento per la Sicurezza (DIS) - Comunicato del 7 febbraio 2014

Con decreti del Presidente del Consiglio dei ministri in data 27 gennaio 2014 sono stati adottati il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" ed il "Piano nazionale per la protezione cibernetica e la sicurezza informatica", in attuazione dell'articolo 3, comma 1, del decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013. I documenti sono resi disponibili sul sito istituzionale del Governo (www.governo.it) e su quello del Sistema di informazione per la sicurezza della Repubblica (http://www.sicurezzanazionale.gov.it/).

Lo scorso 7 febbraio, un po' in sordina, è stato pubblicato sulla Gazzetta Ufficiale il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", con annesso il "Piano nazionale per la protezione cibernetica e la sicurezza informatica", dando attuazione al DPCM 24/01/2013 per quel che riguarda il contrasto alla minaccia cibernetica per il nostro Paese.
Il documento, con pregevole acume, evidenzia come la principale minaccia che proviene dal *cyberspace* è rivolta alla sicurezza delle nostro tessuto industriale in quanto soggetti terzi possono utilizzare lo strumento cyber per sottrarre, a volte senza che ve ne sia neanche la cognizione, il *know-how* scientifico, tecnologico e aziendale che è alla base del nostro made in Italy e, quindi, del benessere economico e sociale della Nazione. In questo contesto il documento evidenzia quale elemento fondamentale la definizione di strategie co-partecipate tra il settore pubblico e quello privato che, con una strategia olistica sia in grado da un lato di migliorare la capacità di prevenzione, ma anche quella di reazione, contrasto e contenimento. Tale approccio deve prendere le mosse dalla costatazione che la minaccia *cyber* si è andata evolvendo sia sul piano tecnologico, che su quello delle possibili conseguenze ma anche, e soprattutto, per quel che riguarda gli attori in campo. Infatti, a fronte di una ridotta minaccia legata al terrorismo (indicata nel documento come "per ora solo ipotetica"), è ritenuta molto più attuale e presente quella di spionaggio/sabotaggio perpetrata anche da soggetti "para-statali".

Interessante a questo riguardo l'evidenziazione che "*diversi Governi si sono dotati delle necessarie capabilities per penetrare nelle reti nazionali di altri Stati*" e ciò non solo tramite l'attacco *cyber*, ma anche mediante una più subdola strategia che passa per una "mobilitazione delle loro industrie nazionali "al fine di alterare componenti *hardware* da esse prodotte acquisendo così la capacità di superare in maniera pressoché irrivelabile ogni difesa". Espressione, quest'ultima, che sottende sia la difficoltà di una difesa rispetto ad eventuali falle/*back-door* presenti nei diversi componenti *hardware*, che un chiaro richiamo a porre maggiore attenzione rispetto ad alcune pratiche commerciali che, sfruttando una politica dei prezzi molto aggressiva, sono riusciti ad acquisire in brevissimo tempo ampie fette di mercato assumendo di fatto un ruolo cruciale rispetto a importanti porzioni di infrastrutture telematiche di rilevanza nazionale (richiamo, non proprio velato, agli *allert* portati avanti dagli USA e non solo verso gruppi industriali "*made in China*").
In questo quadro l'altra potenziale minaccia, oltre che strumento per la veicolazione di materiale illegale, è la minaccia alla capacità di funzionamento delle nostre infrastrutture critiche. E qui, occorre dire con piacevole sorpresa, gli estensori hanno colto l'importanza di declinare la parola "sicurezza" nella sua totale eccezione del vocabolo italiano, andando a riconoscere che il *cyberspace*, come ogni dominio creato dall'uomo, è potenzialmente fallibile. Da qui la necessità di "sviluppare la capacità per anticipare e prevenire eventi rari e inattesi, assicurando la continuità delle reti e dei sistemi", ovvero abbracciando quella filosofia di pensiero "All-Hazard" che pone l'attenzione principale sul contenimento delle conseguenze rispetto a qualunque tipologia di eventi.
Il tutto è perseguibile solo attraverso "*un'adeguata formazione, sensibilizzazione e responsabilizzazione del personale*" e mediante adozioni di misure di sicurezza fisiche, logiche e procedurali.

Per raggiungere tali obiettivi, il Quadro Strategico individua 6 indirizzi strategici ed 11 indirizzi operativi. Nello specifico gli obiettivi strategici riguardano:

1) il miglioramento delle capacità operative e tecnologiche dei diversi attori istituzionali impegnati nel contrasto alla minaccia *cyber*;
2) il potenziamento della capacità di difesa delle Infrastrutture Critiche nazionali;
3) incentivazione della *partnership* pubblico-privato (**PPP**) per migliorare la capacità di tutela delle proprietà intellettuali e la capacità di innovazione del Paese;
4) la promozione della cultura della sicurezza con un crescente coinvolgimento del mondo delle università e della ricerca;
5) rafforzamento della capacità di contrasto alla diffusione di attività e contenuti illegali *online*;
6) rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica.

Questo elenco di obiettivi ribadisce che il *target,* a cui il quadro fa riferimento, è una dimensione residente nella sicurezza nazionale, che mira a salvaguardare in primo luogo le capacità di

crescita del Paese nel suo intero. **Questa impostazione spiega la mancanza di specifici obiettivi per quel che riguarda la tutela del singolo**. Apprezzabile è certamente l'idea, che ricalca quanto già realizzato da altre nazioni a partire dagli USA, di individuare nel mondo delle università e della ricerca un interlocutore privilegiato per quel che riguarda la diffusione della cultura della sicurezza, con l'auspicio (forse per lungo tempo resterà ancora inatteso), che tali argomenti inizino ad entrare in modo più consistente nel bagaglio formativo dei nuovi laureati.

Concentrandoci sul punto 2), nella sintetica declinazione presente nel testo, gli obiettivi di potenziamento della capacità di protezione delle infrastrutture critiche è tradotta in termini di "*assicurando la business continuity e, al contempo, la compliance con standard e protocolli di sicurezza internazionali*", che posto in questo esclusivo contesto potrebbe suggerire agli operatori approcci troppo conservativi a discapito di soluzioni di cooperazione e pro-attività che, in talune circostanze, sarebbe da preferire rispetto alla mere riproduzione di formalismi.

Per l'attuazione di questi obiettivi strategici, il Quadro strategico individua 11 obiettivi operativi, che sono poi maggiormente delineati e dettagliati nel "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica" pubblicato contestualmente al Quadro Strategico e reperibile sempre su sito web del DIS:

1) Sviluppo della capacità della autorità competenti ai fini di una efficace prevenzione, identificazione, repressione, contrasto, neutralizzazione e mitigazione degli eventi che accadono nel *cyberspace* e delle conseguenze che essi hanno sui sistemi IT, sulle Infrastrutture Critiche e sul sistema Paese nel suo insieme.
2) Identificazione di una Autorità nazionale NIS (*Network and Information Security*) che cooperi con le altre autorità omologhe a livello internazionale per lo scambio di informazioni. Favorire la PPP mediante creazione di tavoli di raccordo, l'esecuzione periodiche di esercitazioni, l'introduzione dell'obbligo della segnalazione di incidenti informatici alle Autorità competenti e la definizione di procedure operative per lo scambio di informazioni.
3) Definizione di strumenti per la valutazione del livello di competenza e consapevolezza, realizzazione di campagne di formazione ed introduzione di moduli formativi nelle scuole di ogni grado per promuovere la cultura della sicurezza e sviluppo di ambienti sintetici/simulativi per favorire la capacità di formazione ed addestramento.
4) Rafforzamento della cooperazione internazionale.
5) Dare piena attuazione al CERT Nazionale (da attuare nell'ambito del Ministero dello Sviluppo Economico ai sensi dell'art. 16 bis del Dlgs n. 259/2003, risalente ormai a 11 anni fa) unitamente al CERT-PA.
6) Adeguamento normativo e organizzativo adattando la legislazione all'evoluzione della tecnologia.
7) Elaborazione ed adozioni di norme tecniche per migliorare la sicurezza IT incluso l'individuazione di standard di sicurezza di prodotti e sistemi.
8) Cooperazione con il "comparto" industriale e le PMI includendo anche "previsioni di incentivi volti a stimolare la competitività industriale e tecnologica" ed il potenziamento delle attività di R&S.
9) Mantenimento di una stretta coerenza tra le comunicazioni strategiche istituzionali e le attività condotte nel *cyberspace* al fine di dissuadere i potenziali avversari.
10) Attribuzione ai settori strategici della PA di risorse umane, finanziarie, tecnologiche e logistiche per il perseguimento degli obiettivi programmatici.
11) Implementazione di un sistema integrato di *Information Risk Management* nazionale.

Non potendoci dilungare sui singoli punti, ci limiteremo a soffermarci su alcuni aspetti partendo dal punto 2) che, seppur in modo asettico, prende atto delle numerose critiche avanzate al DPCM 24/01/2013 circa la farraginosità dello strumento dovuto alla presenza di una pluralità di soggetti coinvolti, con l'idea di individuare un interlocutore unitario in grado di semplificare la comunicazione e la cooperazione soprattutto verso i soggetti privati che oggi evidenziano la presenza di una inutile frammentazione e duplicazione di attività. In questo quadro complessivo, **un suggerimento potrebbe essere quello di aumentare il perimetro del NIS per far ricadere al suo interno anche la tematica della Protezione delle Infrastrutture Critiche**, in quell'ottica di approccio "All-Hazard" richiamato pure a pagina 16 del Quadro Strategico.
Rimanendo sempre su questo punto, l'esperienza portata avanti in questi anni dal CNAIPIC, con la realizzazione di convenzioni bilaterali, appare uno strumento efficace per quel che riguarda gli aspetti di definizione delle modalità di interscambio di informazione perché sufficientemente flessibile rispetto, al contrario, ad uno schema rigido ed unitario.

Inoltre, in questo quadro generale, appare mancante un esplicito richiamo alla opportunità di una maggiore capacità di cooperazione fra i soggetti privati che dovrebbe essere favorita, ma non necessariamente mediata, dal soggetto pubblico. Infine l'ultimo cenno riguarda il discorso dell'obbligo di segnalazione degli incidenti informatici sancito anche dal DPCM 24/01/2013. Tema questo di ampio dibattito che vede contrapposte esigenze che andrà necessariamente risolto per via normativa, introducendo meccanismi sia di premialità/tutela a fronte di una denuncia che di penalizzazione in presenza di una mancata segnalazione.

Nel complesso il Quadro di Strategico rappresenta un importante passo in avanti che, ci si augura, possa aiutare a colmare un gap molto ampio con gli altri Paesi. Il piano può essere sicuramente migliorato, ma rappresenta indubbiamente un'ottima sintesi delle diverse necessità e delinea una valida road-map. L'unica pecca è che esso non fornisce alcuna dimensione quantitativa né temporale: Entro quando devono essere raggiunti i vari obiettivi ? Quali sono le "adeguate risorse" necessarie per la loro implementazione?
In definitiva, non si può esimersi da evidenziare come il documento soffra di quelle ambiguità gia descritte (vedi "Sicurezza e Giustizia" n. II/MMXII, "istituito il nucleo per la sicurezza cibernetica" a firma dello scrivente) che riguardano il problema di definire quelle che sono le Infrastrutture Critiche Nazionali, ma questo è una argomento esorbitante rispetto al Quadro Strategico la cui soluzione, si auspica, possa essere a breve trovata. ©