A COSA SERVE IL FRAMEWORK NAZIONALE DI CYBER SECURITY

Il framework nazionale di cyber-security **nasce ufficialmente il 4 Febbraio 2016**. E' l'aula magna dell'università Sapienza di Roma a darne i natali con centinaia di partecipanti, nazionali ed internazionali, a celebrare l'evento. L'occasione è di quelle importanti, con **personalità da tutte le realtà del Paese**: governo, accademia, aziende, istituzioni, militari, stampa. E' una giornata speciale, di quelle che aprono un nuovo capitolo nello scenario economico ed informatico italiano.

SOLO PER ADDETTI AI LAVORI?

Sono oltre mille i nominativi registrati per la presentazione: si tratta principalmente di addetti ai lavori con molta esperienza nel settore (il documento è disponibile online http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf). Questo aspetto può far pensare che il tema sia difficile da portare al di fuori della cerchia degli esperti, qualcosa di cui **si riesce solo ad intuire la rilevanza** ma non si comprende bene a chi e a che cosa serva. Tuttavia un tentativo va fatto per cercare di capire di cosa parlano i cyber esperti italiani.

ECONOMIA È CYBERSPAZIO

Oggi **economia e cyberspazio** sono parole con significati diversi, la loro distanza varia a seconda della ragione del mondo in cui ci si trova, ma ogni giorno questi termini si avvicinano e fra qualche anno saranno sinonimi nel dizionario che declina la morfologia del futuro. Lo sanno bene in USA, dove da pochi giorni il presidente OBAMA ha annunciato (https://www.whitehouse.gov/blog/2016/01/30/computer-science-all) che l'informatica sarà insegnata nelle scuole elementari "*per fare in modo che la nuova generazione di studenti americani abbia le competenze per prosperare in un'economia digitale*". Sviluppare la cyber-security nel nostro paese significa anche **sviluppare l'economia nazionale**, è necessario dare una risposta come sistema paese alla protezione degli interessi nazionali, nel cyberspazio non c'è distinzione tra pubblico e privato, civile e militare, il dualismo è intrinseco.

A COSA SERVE?

Il framework definisce la metodologia (e non la tecnologia) che un'azienda (grande o piccola che sia) può seguire per rendere più sicura la sua infrastruttura informatica:

innanzitutto **permette di valutare la propria cyber-postura**, ovvero lo stato attuale dell'azienda, e la indirizza verso quello che dovrebbe essere l'obiettivo di sicurezza minima da raggiungere, indicando tutti i passaggi da compiere per mitigare il rischio di perdere parte del suo valore (reputazione, brevetti, interruzione, etc.). Il tutto contestualizzato all'interno del quadro normativo nazionale ed arricchito da preziose **linee guida che diventano fari che illuminano il percorso da seguire per migliorare la sicurezza nel cyberspazio**. La protezione del cyberspace è condizione necessaria per la prosperità economica, le nazioni che non avranno gli strumenti per intercettare questa rivoluzione saranno preda delle altre. E' importante evidenziare che nel framework viene suggerita un'idea in particolare: **la protezione cyber viene considerata uno standard di qualità per valutare la caratura dell'azienda**.

UN MANUALE PER LE AZIENDE

Per aiutare la comprensione, potremmo dire che si tratta di un insieme di regole da seguire (su base volontaria) per **migliorare in modo strutturato la sicurezza informatica aziendale**: una serie di indicazioni (non legate a standard tecnologici) che offrono gli strumenti e le procedure a disposizione per soggetti pubblici e privati che sono sempre più esposti al rischio di attacchi informatici. Da questo punto di vista il framework nazionale è uno strumento di auto-analisi di un'organizzazione.

NON SOLO PER AZIENDE ICT

Il framework è uno strumento dinamico, un documento vivo, che può e deve essere aggiornato nel tempo, perché il cyberspazio cambia a grande velocità. Si rivolge a **tutte quelle aziende che hanno da perdere nella guerra cyber**, non solo quelle ICT, anzi specialmente a quelle non ICT. In questo contesto le aziende italiane sono un ghiotto bersaglio perché il loro vantaggio competitivo è spesso l'idea originale, la proprietà intellettuale, il segreto industriale; proprio quelle risorse che facilmente si prestano ad essere rubate (emblematico il caso di un'azienda che, a distanza di pochi mesi da un incidente informatico, ha ricevuto in assistenza i suoi prodotti contraffatti http://formiche.net/2015/06/29/cybersecurity-attacco-hacker-costi-cina/).

ESEMPI PRATICI

Il Framework raccoglie decine di regole (attualmente 98) che devono essere poi contestualizzate all'interno di un determinato ambito. Ad esempio nel settore aerospaziale potrebbero bastarne solo un sottoinsieme (perché alcune potrebbero essere considerate

ridondanti), quelle rilevanti possono essere individuate (ad esempio dai regolatori di settore) nell'esperienza specifica del settore che le vuole utilizzare. A questo punto l'azienda che opera nel settore aerospaziale verifica ognuna di quelle regole e valuta se hanno una priorità alta, media o bassa. A questo punto l'azienda applica quelle regole (seguendone la priorità) **con il livello di maturità che ritiene più vicino alla sua realtà quotidiana** ed all'investimento che può realizzare: ad esempio potrebbe valutare che per la regola DE.CM4 (individuazione codice malevolo) intende a raggiungere una gestione dell'antivirus centralizzata e non localizzata su ogni postazione. Il framework diventa quindi una lingua comune e la diffusione di questa grammatica semplificherà le interazioni tra aziende, ad esempio sarà possibili traslare le regole da un settore ad un altro, da un'azienda ad un'altra, generando un'**accelerazione del sistema Paese**.

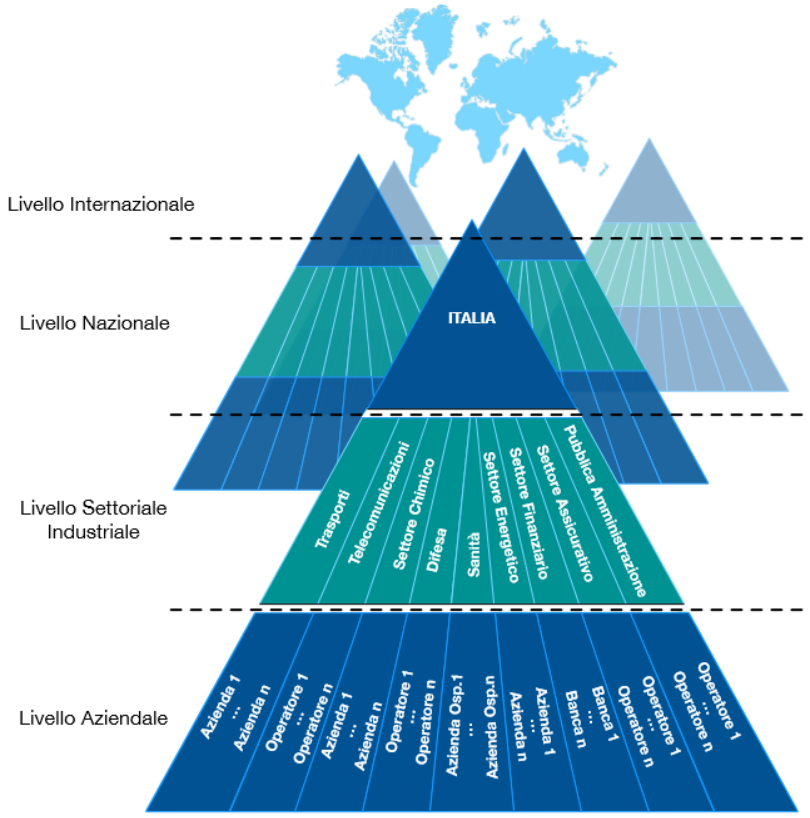

Figura 1: Contesto internazionale, nazionale, di settore e aziendale

LA GESTIONE DEL RISCHIO

La singola azienda decide il livello di sicurezza che vuole raggiungere, valutandone costi e benefici: la sicurezza assoluta è un asintoto, **ci si può avvicinare tantissimo**, ma non la si può toccare. Per questo motivo parte del rischio cyber (ovvero il rischio derivante dalle minacce cyber) potrà essere a carico di un'assicurazione: si trasferisce ad un soggetto terzo la quota di rischio non coperta dalle metodologie messe in campo. D'altra parte il

mercato assicurativo ha capito già da tempo che la parola chiave è cyber-risk come evidenziano alcuni recenti studi di settore (http://formiche.net/2015/09/20/cyber-assicurazione/). In questo modo la gestione del rischio informatico diventa parte stabile della gestione del rischio aziendale e rientra in un contesto già ben compreso dalla dirigenza di un'azienda. L'obiettivo è fare entrare la sicurezza informatica nel top management aziendale e farla uscire dai confini dei dipartimenti di IT.

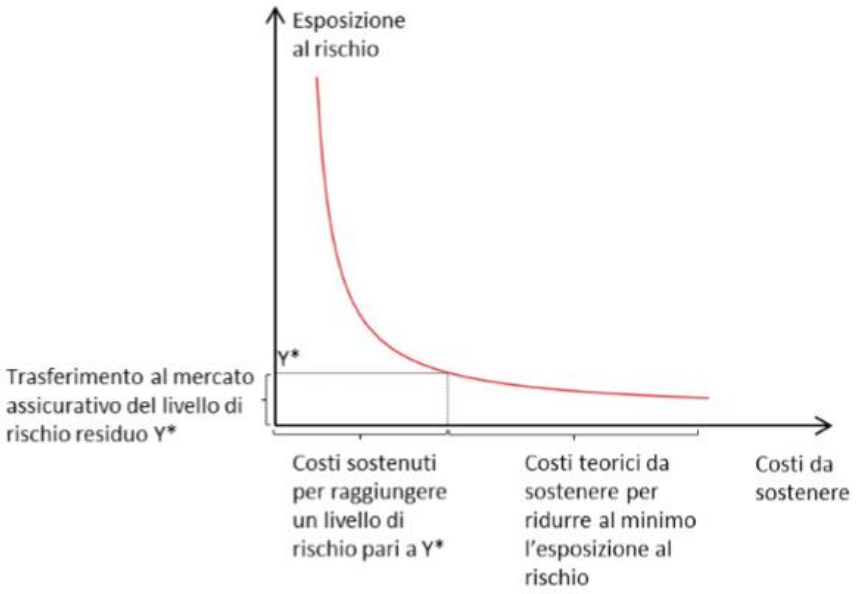

Figura 2: Trasferimento al mercato assicurativo del rischio residuo

ADOZIONE VOLONTARIA MA RACCOMANDATA

L'adesione al documento è volontaria ma i vantaggi per l'azienda sono tali da raccomandarne l'adozione. Il framework nazionale diventa un fattore importante che permette di valutare la qualità cyber di un'azienda, può diventare un elemento decisivo della catena di approvvigionamento: ad esempio una grande impresa, oppure un ente, potrebbe decidere che **un determinato profilo cyber sia un requisito minimo per l'acquisto di beni e servizi**. Un altro aspetto non trascurabile, legato al mondo del diritto, è il concetto del duty of care, il "dovere di attenzione", per semplificare: se un'azienda subisce una violazione informatica, la sua posizione assume una valutazione ben diversa se sono state messe in essere opportune misure di protezione informatica rispetto invece ad un'azienda negligente. In questo scenario adottare il framework nazionale è sicuramente indice di attenzione da parte dell'azienda, che dimostra di portare avanti un processo per minimizzare questo rischio.

COLLABORAZIONE VIRTUOSA

Le università italiane (in particolare CIS e CINI http://formiche.net/2016/01/23/cyber-security-cose-e-cosa-serve-il-framework-nazionale-di-cis-e-cini/), con il supporto attivo del governo, hanno riunito intorno al tavolo importanti aziende nazionali per produrre questo documento che nel suo percorso **si è arricchito anche di emendamenti raccolti con una consultazione aperta** che ha visto una tangibile partecipazione del pubblico. Il catalizzatore attorno al quale si è realizzato questo lavoro è il prof. BALDONI che ha così commentato: "*Il framework nazionale rappresenta di fatto un documento che dà un indirizzo a tutto un settore, chiaramente dall'implementazione di questo framework nazionale nasceranno competenze e posti di lavoro, nascerà un mercato che darà forza al sistema Paese dal punto di vista della protezione cyber e questo permetterà anche nuovi investimenti in Italia*".

VANTAGGI PER LA NAZIONE

Il framework si rivolge a più utilizzatori: innanzitutto le piccole e medie imprese che sono la spina dorsale del Paese, ma anche alle grandi imprese, alle infrastrutture critiche, ai regolatori di settore, alla pubblica amministrazione. Fornisce un **quadro comune a diverse autorità che disciplinano il settore in modo da regolamentare in modo coerente** (Garante Privacy, AGID, PCM, etc.). In questo modo è possibile incastonare le varie regolamentazioni dei diversi operatori nazionali, evitando sovrapposizioni ed operando in modo omogeneo.

LA CYBER-SECURITY UNA PRIORITÀ PER IL GOVERNO

Sul versante istituzionale è il Dipartimento delle Informazioni per la Sicurezza della Repubblica (Presidenza del Consiglio dei Ministri) l'organo istituzionale ha investito sul framework nazionale di cyber-security. Il Sottosegretario MINNITI è intervenuto alla presentazione ufficiale (in qualità di Autorità delegata per la Sicurezza della Repubblica) ed ha affermato che l'importanza della sicurezza informatica è cresciuta nella consapevolezza politica e istituzionale: dal dicembre del 2013 ad oggi si è sviluppato un **rapporto molto fecondo con l'accademia**, ad oggi il laboratorio nazionale che si muove in questo campo conta 33 facoltà e 500 ricercatori che formano una considerevole forza di elaborazione e conoscenza. Il messaggio trasmesso dall'Autorità di governo è chiaro: dal 2013 ad oggi una parte dei compiti a casa è stata fatta: è stato presentato il piano nazionale senza derogare sui tempi, sono state siglate le convenzioni con 13 grandi imprese nazionali considerate

infrastrutture critiche, ed oggi il commento icastico alla presentazione del documento è: "**Framework Nazionale adottato**".

L'ITALIA DEVE ACCELERARE

Il senatore MINNITI ha poi aggiunto che il framework è un progetto molto convincente che **diventa per l'Autorità un riferimento importante** e sottolinea tre obiettivi: semplificare la capacità di autovalutazione delle difese cibernetiche, aumentare la consapevolezza della sfida, ampliare la platea coinvolta. Ha poi aggiunto: "*L'Italia non è all'anno zero, non è un paese di archeologia cibernetica, può competere nel contesto internazionale ma deve produrre un'accelerazione"* perché la minaccia è cresciuta: nel cyber-spionaggio (sia per finalità distruttive sia per furto di conoscenza), nell'hacktivismo, e ancora di più nello scenario del terrorismo. Per comprendere quanto sia importante il fattore velocità "*l'obiettivo del sistema Paese è di utilizzare nel migliore dei modi gli investimenti previsti (150 milioni di euro* http://formiche.net/2016/01/18/cyber-sulla-sicurezza-il-governo-fa-sul-serio/ *) e già a partire dall'anno prossimo il paese deve essere cambiato nella capacità di usare la cyber-security perché la realtà corre velocissima*".

FABIO DE PAOLIS

Fabio De Paolis è esperto in sicurezza informatica con oltre 20 anni di attività nel settore. E' laureato in Sicurezza dei Sistemi e delle Reti Informatiche presso l'Università di Milano; è CERTIFIED ETHICAL HACKER presso EC COUNCIL di Londra; è CHIEF INFORMATION SECURITY OFFICER in un'azienda italiana che offre servizi di ingegneria del software e sicurezza informatica; è consulente di enti ed organizzazioni private per individuare ed esaminare minacce informatiche; si interessa di cyber-security e cyber-warfare con particolare attenzione al mondo dell'intelligence; è attivo sulla Rete da quando la posta elettronica si scambiava solo fra BBS tramite modem analogico.