Dott. Massimo Ravenna, *Responsabile Cyber Security ACEA*
Audizione alla IX Commissione della Camera
1 luglio 2021

Conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" (AC 3161)

1. Contesto generale

La digitalizzazione nel contesto dei servizi essenziali, in particolare l'esperienza nel settore energetico ed idrico, ha comportato il ridisegnare infrastrutture e servizi, secondo principi di interoperabilità, decentralizzazione, capacità di agire in tempo reale e modularità.
Abbiamo quindi delle infrastrutture profondamente interconnesse, più efficienti, più veloci nei cambiamenti.

Questo scenario tuttavia mette gravemente a repentaglio la sicurezza, poiché offre ad attori ostili maggiori possibilità di interferire con i servizi pubblici: letteralmente ogni giorno, infatti, si rilevano tentativi di attacco, ad esempio per fini estorsivi.

2. Principi di sicurezza e Acea

Per affrontare questi scenari risulta essenziale il coinvolgimento diretto degli operatori privati, possessori e gestori delle infrastrutture critiche, puntando sulla loro responsabilizzazione, su incentivi positivi e meccanismi di fiducia reciproca.

Nel caso di Acea, ad esempio - il primo operatore idrico con oltre il 20% della quota di mercato nazionale ed uno dei primi del settore energetico, gestendo tutta la distribuzione elettrica di Roma, in primis di organi costituzionali, Stato del Vaticano, ambasciate, comparto sicurezza ed intelligence – questa responsabilità si è tradotta in un piano strategico pluriennale per lo sviluppo di capacità di cyber security.

Nel corso del 2020, in piena emergenza pandemica, Acea ha sviluppato una struttura dedicata, con una massiccia campagna di assunzioni, intercettando talenti dalle università e dal mercato e puntando sulla diversità di competenze, formazione, età ed esperienze.

L'impegno poi è stato volto a bilanciare da un lato le capacità operative di risposta ad incidenti – realizzate con l'unità CSIRT, resa operativa ed accreditata in meno di 6 mesi - dall'altro la capacità di visione strategica, per guidare quei processi di trasformazione che ho citato all'inizio, arricchiti questa volta dal principio di *security by design* e *by default*.

In questo percorso l'adozione delle tecnologie risulta secondario rispetto alla valorizzazione di capacità e competenze umane.

3. Partnership pubblico privato

Proprio in riferimento alla valorizzazione e allo sviluppo di capacità, si accoglie con grande favore l'importanza che il testo riserva alla *partnership* pubblico-privato.

Il mercato italiano della sicurezza vede la grande spinta propulsiva di PMI, tuttavia poco valorizzate sia dal sistema istituzionale e pubblico, che dai grandi *player* nazionali.

Si consideri, che anche nel settore delle infrastrutture critiche, vi è una presenza preponderante, ove non monopolista, di servizi di sicurezza e tecnologie estere.

Lo sviluppo di capacità nazionali, anche in ottica di mercato eurounitario, può essere il fattore chiave per il rafforzamento del sistema di sicurezza collettiva.

Tuttavia dal mondo pubblico, oltre a responsabilità di coordinamento e indirizzo, così come indicate nel testo in esame, occorrono azioni concrete e strutturate, con strumenti operativi definiti.

La proposta della costituzione di un Registro nazionale delle *startup* di *cyber security*, ad esempio, rappresenta un'iniziativa abbandonata forse troppo presto nel 2017, ma che, se attuata, potrebbe contribuire a definire requisiti di competenze da sviluppare, a mappare capacità su scala nazionale e di conseguenza a supportarne la crescita.

Crescita che in questo settore si basa anche molto sulla eterogeneità delle esperienze professionali, su percorsi di carriere arricchiti da diversi punti di vista.

Purtroppo ad oggi non c'è ancora un contesto normativo tale da invogliare e supportare i professionisti nel diversificare il proprio percorso: si è bloccati in silos verticali, dove la pubblica amministrazione ed il privato interpretano la *partnership* troppo spesso solo vincolata a singoli progetti e non come visione strutturata, incentrata sulle opportunità da offrire ai professionisti di oggi e soprattutto di domani.
Pertanto, la creazione di strumenti giuslavoristici applicabili dal pubblico e dal privato, specifici per i professionisti della *cyber security*, sarebbe quel chiaro passo in avanti che consentirebbe di incentivare questa osmosi di competenze, senza la quale si rischierebbe di persistere in un percorso che negli ultimi anni ha visto il pubblico – anche titolare della materia – procedere con andatura non sincronizzata alle evoluzioni dello scenario guidato dal privato.

4. Proposta modifica art.15

Infine, proprio per rispondere alle esigenze di allineamento tra i due mondi – pubblico e privato – ci si permette di richiamare l'attenzione sulle nuove competenze identificate all'art.15 del testo, che reca le modificazioni al decreto legislativo NIS.

Con tale decreto si recepiva la direttiva comunitaria sulla sicurezza delle reti e dei sistemi informativi, si definiva l'attuale assetto istituzionale in materia di *cyber security* – con le autorità NIS presso le Amministrazioni centrali dello Stato, le Regioni e Province autonome

– e si individuavano le responsabilità a carico degli Operatori di Servizi Essenziali (OSE) e dei Fornitori di Servizi Digitali (FSD).

In tale assetto sono individuati una molteplicità di attori pubblici e privati che devono rispondere ai numerosi obblighi previsti dalle norme in materia di comunicazioni, gestione di incidenti ed adozione di presidi di sicurezza.

L'esperienza di questi anni restituisce una sostanziale insoddisfazione degli operatori nazionali circa l'eccessiva eterogeneità di azione da parte delle Amministrazioni competenti: in particolare sul tema dell'individuazione e designazione proprio degli OSE e FSD, con conseguenti effetti negativi ricadenti direttamente su tutti i soggetti coinvolti.

Pertanto, al fine di favorire un assetto che assicuri l'unicità di azione, si suggerisce l'inserimento, a favore della neonata Agenzia Nazionale per la Cybersicurezza, del potere di modifica ed integrazione delle segnalazioni e designazioni degli OSE e FSD provenienti dalle Amministrazioni centrali e locali competenti.

La proposta nasce dalla necessità di meglio inquadrare quei soggetti societari – quali le società finanziarie, *holding* – che, pur non risultando titolari di infrastrutture designate quali OSE o FSD a cura dell'istituzione competente di settore (es. MITE nel caso energia), attraverso i propri *asset* detengono il controllo decisionale sugli Operatori stessi.

Ad oggi, quindi, le *holding* rischiano di essere in una zona grigia dal perimetro *cyber* e potrebbero rimanere escluse anche da eventuali partenariati pubblico-privato, indebolendo così la portata di qualsiasi azione normativa.

Il mantenimento dell'attuale schema di responsabilità quindi rischia da un lato di danneggiare i suddetti Operatori, dall'altro aprire a potenziali falle informative, con conseguenti rischi per la sicurezza collettiva.

5. Conclusioni

In conclusione, il testo in esame nella sua attuale configurazione, al netto delle eventuali proposte di modifiche, rappresenta quella significativa evoluzione nella *governance* della *cyber security* nazionale da tempo attesa, di cui si auspica una piena e completa attuazione, con particolare attenzione alle sue componenti operative.

Massimo Ravenna
Per oltre 10 anni come Ufficiale dell'Esercito specializzato in telecomunicazioni e *cyber security* militare, successivamente alla Presidenza del Consiglio dei Ministri, con il consigliere militare del Presidente, sui temi di *cyber security* ed infrastrutture critiche e da poco più di un anno responsabile della *cyber security* del Gruppo Acea.