19 Luglio 2024

Camera dei Deputati
I Commissione Affari Costituzionali, e IX Commissione Trasporti

Memoria nell'ambito dell'esame dell' Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (cd. NIS2)

Prof. Mauro Conti

Ringrazio i Presidenti e gli Onorevoli membri della Commissione per il gradito invito a condividere la mia memoria in merito al recepimento della direttiva NIS2 “Direttiva sulle misure per un livello comune elevato di cybersicurezza in tutta l'Unione”.

Mi presento brevemente solo per evidenziare il punto di vista che posso portare a questa discussione. Sono Professore Ordinario di Informatica all’Università di Padova, dove sono Presidente della Laurea Magistrale in Cybersecurity (Classe di Laurea Ministeriale LM66). Mi occupo di ricerca, didattica e trasferimento tecnologico, in particolare nel settore della Cybersecurity, da circa 20 anni.

Ritengo estremamente importante tutto il percorso normativo fatto dal legislatore italiano ed europeo in materia di cybersecurity (che in Italia va dalla riforma delle Agenzie di Intelligence, all’istituzione dell’Agenzia per la Cybersicurezza Nazionale, alla definizione del Perimetro di Sicurezza Nazionale, e che in ambito europeo ha visto in particolare le due direttive NIS e NIS2, oltre al GDPR e in qualche maniera anche l’AI Act). Nello specifico ora ci troviamo nel momento in cui il nostro Paese recepisce la direttiva NIS2 tramite l’Atto del Governo n. 164, oggetto della presente memoria.

Vado subito ad elencare i miei commenti sullo schema di decreto legislativo oggetto della discussione e resto a disposizione degli Onorevoli per eventuali approfondimenti.

1. In merito all’art. 3 (Ambito di applicazione), ritengo opportuno includere esplicitamente anche le Università tra i soggetti destinatari della normativa (ad esempio nell’Allegato III, alla lettera d, punto 5). Le **Università** rappresentano senza dubbio un **asset fondamentale per il nostro Paese**, alla base della ricerca (che include creazione di conoscenza e proprietà intellettuale), della formazione e del trasferimento tecnologico, essenziale per lo sviluppo e la competitività del nostro sistema economico e sociale. Mentre un attacco alle Università potrebbe apparire in prima istanza meno critico di un attacco ad esempio all’infrastruttura energetica, se ignorato può portare nel medio/lungo termine ad un significativo impoverimento del Paese. Inoltre, molte delle Università Italiane, hanno “popolazioni” di studenti e personale, che supera quello delle amministrazioni di cui all’Allegato 3, lettera c, punto 2.
   La stessa direttiva NIS 2 (rispetto alla precedente NIS) va nella direzione di ampliare il campo di applicazione includendo anche le pubbliche amministrazioni centrali (lasciando discrezionalità agli Stati membri di inserire gli enti locali in base all’assetto istituzionale), senza fare tuttavia chiaro riferimento alle Università. Ritengo però che

queste possano e debbano essere incluse esplicitamente nella normativa nazionale, in quanto soggetti che operano in ambiti strategici e che pertanto dovrebbero rientrare nei soggetti critici se non essenziali per il corretto funzionamento del paese.

2. Art. 12 comma 3 (dell'Atto di Governo n.164) *prevede che possono essere "chiamati a partecipare alle riunioni: altri rappresentanti delle amministrazioni di riferimento delle autorità NIS in relazione alle materie oggetto di trattazione; rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca; operatori privati interessati dalle previsioni di cui al presente provvedimento."*
   A tale proposito, suggerirei che il "*Tavolo permanente per l'attuazione della disciplina NIS2 presso l'Agenzia per la cybersicurezza nazionale (ACN)"* come da comma 1 dell'art. 12 **comprendesse in maniera permanente Professori Universitari esperti nell'area della Cybersecurity**. Questi rappresentano infatti figure scientifico-tecniche e strategiche soprattutto in merito alle attività di cui al comma 5 punto b (*formulare proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo ai fini dell'efficace attuazione del presente decreto*), in quanto possono fornire un punto di vista particolarmente aggiornato sugli attacchi e le tecniche di difesa che il mondo della ricerca definisce e aggiorna quotidianamente.

3. Considerata la scarsità di persone esperte nella Cybersecurity e quindi l'esigenza di essere attrattivi verso queste professionalità, e considerata l'importanza della materia per il nostro Paese, si suggerisce di stimolare e valorizzare maggiormente la partecipazione al Tavolo di cui all'art. 12. Nella proposta attuale, come sottolineato dalla Relazione Tecnica allegata, *"il comma 6 stabilisce che la partecipazione al Tavolo in parola non dà luogo alla corresponsione di gettoni di presenza, compensi o rimborsi di spese o altri emolumenti, comunque denominati",* assicurando quindi che la disposizione non rechi nuovi o maggiori oneri.
   Ritengo invece che una **giusta valorizzazione delle professionalità**, in generale, chiamate ad implementare questa direttiva, **sia un segnale dell'importanza che il nostro Paese dà a questa materia**, soprattutto nei confronti delle numerose organizzazioni che dovranno sottostare (anche con impianto sanzionatorio) alla normativa stessa.

4. La **formazione** è essenziale per garantire la sicurezza delle organizzazioni. E' quindi importante che questa sia **ben supportata, gestita e monitorata**.
   La Cybersecurity interessa tutte le persone e non solo i tecnici/esperti preposti all'implementazione e gestione delle misure di sicurezza. A dimostrarlo sono i numeri in tema di *social engineering* e *phishing,* che sempre più spesso sfruttano l'anello debole del sistema: gli utenti e i dipendenti delle organizzazioni coinvolte. Pertanto vorrei porre l'attenzione sulla formazione del personale e sulla necessità che questa formazione venga monitorata e gestita da enti preposti. Per l'adozione delle misure minime di sicurezza da implementare per essere conformi al già citato articolo 21, la Direttiva NIS2 impone ai membri degli organi di gestione delle entità "essenziali" e "importanti" di seguire una formazione specifica, verticalizzata sui dipendenti in base anche al ruolo ricoperto in azienda. L'ACN deve garantire che i compiti pianificati dalle aziende siano effettivamente realizzati e che vi sia un reale processo di monitoraggio e valutazione dei risultati ottenuti, affiancando gli enti nell'implementazione di strategie operative e soprattutto assicurandone il costante

aggiornamento. A tal fine, si suggerisce di essere **più incisivi e specifici su questi aspetti**, ad esempio nell'art. 23, comma 2.a ("*sono tenuti a seguire **una formazione** in materia di sicurezza informatica*") o in regolamentazione successiva, indicando quantità di ore di formazione o argomenti e modalità di verifica dell'apprendimento.

5. Per facilitare il miglioramento della postura di sicurezza (e non solo il mero adempimento normativo motivato dall'apparato sanzionatorio) delle organizzazioni e dunque dell'apparato nazionale si dovrà specificare alcune modalità pratiche relative alla vigilanza: il quadro di riferimento delle misure di Cybersecurity utilizzate per valutare gli enti, le modalità ispettive degli enti, le condizioni per l'accreditamento degli organismi di controllo, ecc. In questa direzione, altri stati membri che hanno già adottato la direttiva NIS2, possono fungere riferimento al fine di **limitare l'aggravio economico/organizzativo sulle imprese**. Ad esempio, il Belgio ha delimitato in maniera chiara quelle che potrebbero essere le misure da adottare per essere conforme a quanto richiesto dalla direttiva, indicando il rispetto del CyberFundamentals Framework (CyFun) fornito dalla CCB (l'ACN belga), nonché la certificazione ISO 27001. Il framework belga CyFun riunisce infatti una serie di misure ispirate a diversi standard di sicurezza informatica: la già citata ISO 27001/27002, NIST CSF, CIS Controls e IEC 62443 per la protezione degli apparati OT. La Germania, si è mossa verso la definizione chiara dei soggetti interessati e dall'utilizzo degli stessi di standard già esistenti quali ad esempio il BSI Act, l'IT Security Act 2.0 e l'ordinanza KRITIS. Allo stesso modo la Francia, tramite l'ANSSI, ha previsto di implementare diversi **strumenti di assistenza online**. Per facilitare l'adeguamento dei soggetti interessati ha messo a disposizione uno strumento per valutare l'idoneità di un'organizzazione a NIS2, un servizio di supporto per l'implementazione e uno **strumento per monitorare le misure di sicurezza informatica**.

6. Il **budget previsto** all'art. 13 comma 6, di 1 milione di euro, **non sembra essere sufficiente al raggiungimento degli obiettivi**, in particolare tenuto conto dell'enorme numero di soggetti che ci si aspetta essere destinatari della direttiva NIS2 e del crescente numero di attacchi e del loro impatto. Nella relazione tecnica allegata viene specificato (a grandi linee) la destinazione di questo budget annuale, destinato al 50% ad ACN e per il restante 50% al Ministero della Difesa. A titolo di esempio, ACN avrebbe a disposizione solo 200 mila euro annui per costi *"derivanti dalle specifiche funzioni, anche attraverso l'implementazione di strutture tecnologiche utili al coordinamento delle attività di gestione delle crisi cibernetiche su vasta scala e allo scambio informativo in condizioni di sicurezza".* Sembra che una dotazione di soli 200 mila euro (soprattutto nei primi anni) per la gestione di crisi su vasta scala, sia piuttosto limitato. Fermo restando che la **mancanza di disponibilità di personale esperto** (non solo con profilo giuridico, ma anche e soprattutto tecnico, per la gestione delle crisi) **potrebbe essere la criticità principale.**

7. Per quanto riguarda l'art 25, comma 4, lettera a, ritengo opportuno specificare un importo minimo per le "perdite finanziarie", per **non aggravare l'ACN e tutta la procedura di gestione delle notifiche** (che avrebbe conseguenze sull'efficacia generale, anche nella gestione di attacchi più importanti), **in merito ad incidenti effettivamente minori**. Inserendo un importo minimo alle perdite, si potrebbero

evitare notifiche in casi non troppo rilevanti. Ad esempio, si immagini un computer che non gestisce transazioni o informazioni rilevanti e non produce perdite economiche restando offline qualche ora. Se questo venisse colpito da un virus tradizionale (non un ransomware e non un attacco mirato) aprendo semplicemente un allegato email malevolo, e l'unico costo conseguente fosse il corrispettivo di qualche ora di lavoro per ripristinare il sistema, si potrebbe valutare di evitare la notifica (e i suoi conseguenti costi di gestione).

8. Per evitare che i soggetti interessati sottostimino l'importanza di adeguarsi alle indicazioni della direttiva, non limiterei i poteri ispettivi di cui Art. 36 comma 2, al possesso di "*indicazioni o informazioni che suggeriscano possibili violazioni*".

9. Al fine di migliorare la postura di sicurezza del nostro Paese e facilitare l'adeguamento alla direttiva NIS, specificherei nel decreto che gli **introiti delle sanzioni amministrative pecuniarie** di cui all'art. 34 comma 1.d, **siano completamente destinati ad iniziative di miglioramento della postura di sicurezza e di supporto all'adeguamento alla direttiva**. Sarebbe auspicabile dedicare almeno 20% di questi fondi alla formazione in area Cybersecurity rivolta a persone che vogliano specializzarsi nel settore o personale di organizzazioni a cui si applica la direttiva NIS2, e almeno il 30% di questi fondi ad incoraggiare e finanziare attività di sviluppo e commercializzazione di tecnologie di Cybersecurity nel nostro Paese. Questo ultimo suggerimento, può aiutare a far si che la Cybersecurity non sia solo un costo, ma un'**opportunità di sviluppo e crescita per il Paese**.