XVIII LEGISLATURA

Legge di conversione del 21 marzo 2022, n. 21
Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina (AS 2564)
Articolo 29 "Rafforzamento della disciplina cyber"

Trend Micro, azienda giapponese quotata alla Borsa di Tokyo, leader globale nella cybersecurity e nel campo della ricerca sulle minacce informatiche, ha molto apprezzato che il Governo e il Parlamento abbiano avviato una discussione sul ddl di conversione del Decreto Legge sul "*Contrasto degli effetti economici e umanitari della crisi ucraina*" con l'introduzione di **significative novità nel campo della cybersecurity** che, anche alla luce dell'evoluzione della situazione internazionale e del contesto geopolitico, hanno l'obiettivo di **rafforzare la sovranità tecnologica e digitale del nostro Paese.**

1. Premessa e valutazioni generali

Durante gli ultimi anni abbiamo assistito a un'**accelerazione dei processi di digitalizzazione della società**, con la tecnologia che è ormai diventata un elemento fondamentale per rispondere in modo rapido ed efficace ai bisogni della "nuova normalità" che tutti stiamo vivendo.

La *digital transformation* continuerà a ritmi ancora più sostenuti nei prossimi anni, grazie anche alle risorse messe a disposizione dal **Next Generation EU,** con lo sviluppo di **tecnologie emergenti** - come il 5G, l'intelligenza artificiale, il cloud e l'IoT - **che avranno impatti rilevanti in ogni settore della società**: dalla salute all'industria, dalla Pubblica Amministrazione ai trasporti, dall'energia al turismo, dall'istruzione alla cultura, dall'agrifood al commercio.

Progressivamente, quindi, prenderà forma un **ecosistema distribuito territorialmente e continuamente connesso**, composto da una moltitudine di device con diverse applicazioni

"verticali" che gestiranno una quantità sempre maggiore di dati. Secondo un recente studio (Frost & Sullivan, "Future of Connected Living", febbraio 2021), il numero di device connessi nel mondo salirà **da 30,4 miliardi nel 2020 a 200 miliardi nel 2030**, con un tasso di crescita composto del 20,7%.

Se da un lato, dunque, le nuove tecnologie consentiranno di raggiungere la piena e integrata digitalizzazione di imprese, PA e cittadini, dall'altro **renderanno inevitabilmente individui e organizzazioni sempre più vulnerabili a nuove forme di cyber attacchi**. Secondo i dati che emergono da "*Navigating New Frontiers*", il report di Trend Micro Research sulle minacce informatiche registrate lo scorso anno**, l'Italia è quarta al mondo e prima in Europa nella classifica dei Paesi più colpiti dai malware**, mentre nel 2020 occupava il settimo posto a livello mondiale. Un primato, quello guadagnato dal nostro Paese, che non solo conferma il 2021 come un anno record per numero di attacchi, ma che dimostra soprattutto come l'Italia **sia impreparata di fronte alle sfide della cybersicurezza**.

Nonostante negli ultimi mesi siano stati fatti notevoli passi in avanti riguardo alla regolamentazione sulla cybersecurity - a cominciare dall'istituzione dell'**Agenzia per la Cybersicurezza Nazionale** - è importante evidenziare che, sebbene si parli sempre di più di reti, innovazione e infrastrutture digitali, nel nostro Paese si riscontra ancora una **scarsa consapevolezza dell'importanza che ricopre oggi la sicurezza cibernetica**.

In questo contesto, obiettivo fondamentale deve quindi essere quello di mettere in campo, anche grazie alle risorse del **PNRR**, politiche mirate al **rafforzamento della protezione cibernetica** e al miglioramento della resilienza dell'infrastruttura IT del Paese, partendo dalle funzioni e dai servizi essenziali dello Stato e dalle loro **supply chain**, che spesso possono essere punti vulnerabili del sistema. Solo in questo modo si potrà consentire ai **cittadini, alle imprese e alla Pubblica Amministrazione di sfruttare a pieno le potenzialità della transizione digitale senza rischi, mantenendo alti standard di sicurezza e protezione dei dati**.

2. Osservazioni sull'articolo 29 “Rafforzamento della disciplina cyber”

L’articolo 29 concernente il “*Rafforzamento della disciplina cyber”* rappresenta indubbiamente una misura importante per potenziare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici della Pubblica Amministrazione nell’attuale contesto geopolitico. Appare tuttavia fondamentale **chiarire alcuni punti del provvedimento**, in modo da **sostenere e accompagnare correttamente le Pubbliche Amministrazioni nazionali e locali nel processo di transizione** finalizzato ad erogare i servizi pubblici garantendo i massimi standard di sicurezza, in particolare:

- **Valutazione del rischio**

Innanzitutto, è fondamentale includere il **Cybersecurity Risk Assessment** (Valutazione del rischio informatico) come principio fondamentale per guidare il processo di diversificazione delle categorie di prodotti e servizi, definiti dal Decreto, che hanno un alto livello di pervasività sulle reti e i sistemi delle Pubbliche Amministrazioni in cui operano.

Per ridurre il rischio di cyber attacchi è necessario essere previdenti e capaci di mitigare l’impatto di eventuali incidenti di sicurezza informatica: in questo contesto, la prima cosa da fare è **l'analisi di tutti gli asset di una Pubblica Amministrazione**, come di un’azienda, comprendendo, oltre a tutte le infrastrutture digitali in uso, anche la totalità dei processi in esse collegati, per poi **organizzare un percorso di gestione del rischio informatico**.

Con la diffusione delle nuove tecnologie, infatti, si è ampliata la superficie digitale, moltiplicando i rischi legati agli attacchi informatici e alla gestione di tutti i dati sensibili presenti sulla rete. In generale, e gli ultimi casi di attacchi a imprese strategiche e a PA lo dimostrano, appare ormai evidente come la sicurezza cibernetica debba diventare non solo il **presupposto necessario di un’architettura nazionale di rete agile, evoluta e flessibile**, ma anche uno dei pilastri dell’attività per le organizzazioni pubbliche e private.

A tal fine, a nostro avviso è necessario chiarire nel Decreto che le procedure di acquisto di nuovi servizi e prodotti sulla cyber sicurezza, da parte delle Pubbliche Amministrazioni, dovrà avvenire non esclusivamente sulla base della convenienza economica, ma della **necessità di dotarsi di soluzioni che garantiscano i massimi livelli di protezione dai rischi di**

attacchi informatici.

- **Diversificazione dei fornitori**

Il comma 1 dell'articolo 29 stabilisce che **le Pubbliche Amministrazioni provvedano alla diversificazione delle dotazioni informatiche in uso,** per ciascuna delle categorie che saranno individuate con circolare dell'Agenzia per la cybersicurezza nazionale, **al fine di prevenire i rischi per la sicurezza delle reti, dei sistemi e servizi informatici**.

La norma prevede quindi anche la possibilità per le PA di avere due fornitori, ciascuno con i rispettivi programmi, per la protezione da attacchi cyber. Si ritiene fondamentale che questa ipotesi venga definita con maggiore chiarezza nel provvedimento, indicando in maniera più specifica **le modalità con cui si potrà prevedere la presenza contemporanea di due fornitori**, in modo da assicurare che le Pubbliche Amministrazioni si dotino di **sistemi compatibili e in grado di comunicare tra loro per garantire performance adeguate**.

- **Linee Guida uniformi per la PA**

La norma in esame parte dal presupposto di garantire la sicurezza informatica a tutta la Pubblica Amministrazione in un contesto nel quale sempre più spesso questa è oggetto di cyber attacchi: secondo i dati del Documento di Sicurezza Nazionale, negli ultimi due anni si è registrato nel nostro Paese un incremento del 20% di cyber attacchi, orientati per **oltre l'80% contro i sistemi IT di soggetti pubblici ed in particolare contro le amministrazioni locali**.

A tal fine, si ritiene fondamentale dare maggiori indicazioni alle PA su come difendersi da tutte le possibili minacce di attacchi, prevedendo la definizione, anche attraverso la normativa secondaria, di **linee guida che comprendano indicazioni chiare ed efficaci su tutti i sistemi di prevenzione e di risposta**.

Negli ultimi mesi abbiamo infatti assistito ad un aumento della superficie di attacco dovuta all'incremento delle soluzioni digitali adottate nella PA: questa circostanza non può essere ignorata o sottovalutata e pertanto i soggetti pubblici **devono essere pronti** a rispondere impostando piani efficaci di **incident response**.

Per prevenire le minacce cyber **è prioritario che tutte le Pubbliche Amministrazioni, non solo quelle centrali ma anche quelle locali, si dotino di una struttura difensiva adeguata**, **in grado di garantire più moderne ed efficienti apparecchiature**, costantemente aggiornate, più **avanzati sistemi antihacker** e **personale istruito, addestrato e qualificato**, pronto ad usare i suddetti strumenti in modo corretto per bloccare sul nascere le iniziative dei cyber criminali.

3. Conclusioni

L'implementazione di presidi efficaci di cybersecurity rappresenta oggi una delle sfide più impegnative e importanti per accelerare sulla strada dell'innovazione del Paese, in quanto costituisce il substrato indispensabile abilitante l'utilizzo delle nuove tecnologie.

A tal fine è necessario che le Istituzioni sostengano una sempre più forte **collaborazione con il settore privato**, non solo per quanto riguarda i **sistemi di sicurezza,** ma anche per la **formazione e l'educazione al digitale**. Perché il processo di evoluzione della cybersecurity possa essere efficace, è necessario infatti puntare sul tema della *awareness* e dello **sviluppo delle competenze industriali, tecnologiche e scientifiche**, in modo da permettere alla PA di affrontare con strumenti adeguati le nuove sfide legate alla sicurezza cibernetica. È prioritario dunque **investire maggiormente**, anche grazie alle risorse del PNRR, **su programmi di formazione per tutti i dipendenti delle PA centrali e locali.**

Per concludere. È necessario oggi **mettere a sistema, in un disegno compiuto, organico e organizzato, una strategia di medio-lungo periodo che possa prevenire tutti i possibili rischi e le minacce legate alla trasformazione verso l'*e-government***, superando così le criticità che impediscono di creare nel nostro Paese una rete, uniforme su tutto il territorio, in grado di erogare i servizi essenziali per i cittadini mantenendo standard elevati di sicurezza.