AUDIZIONE COMMISSIONE FINANZE DEL SENATO

RETI 5G: PROBLEMATICHE DI CYBER SICUREZZA ED INIZIATIVE IN CORSO

Inquadramento della problematica

Nella prospettiva di un uso pervasivo delle reti 5G nel prossimo futuro, appare utile una analisi dei possibili rischi in tema di sicurezza nazionale legati al sempre maggiore ricorso a tecnologie provenienti da aziende non europee.

Sulla base della diffusione del parco apparati oggi installato, relativo alle reti per telecomunicazioni, infatti, va preso atto che alcuni fornitori extraeuropei risultano già massicciamente presenti nelle reti dei grandi operatori nazionali, al punto da essere i costruttori di riferimento.

Il progressivo inserimento nel mercato italiano di tali apparati, mediante politiche di mercato talora anche aggressive, ci mette di fronte una realtà che vede le reti fisse e mobili prevalentemente poggiate su tecnologie extra-UE; ciò è vero in Italia così come in gran parte del mercato globale.

Inoltre, vanno considerati i mutamenti tecnici introdotti dalle reti 5G.

Tradizionalmente, le apparecchiature di rete utilizzate dagli operatori di telecomunicazioni sono classificate come parte della rete "*core*" o della rete "*edge*".

Nella parte "*core"* hanno luogo le funzioni più sensibili, tra cui il controllo degli accessi, l'autenticazione, il routing di voce e dati e la fatturazione.

La parte di rete "*edge"*, invece, è costituita dagli elementi radio utilizzati per collegare i dispositivi d'utente (come telefoni, laptop e tablet) alla rete principale.

Mentre le precedenti reti mobili presentavano chiare divisioni funzionali tra *core* e *edge*, la tecnologia 5G è progettata in modo che le funzioni sensibili attualmente eseguite nella rete *core*, isolata fisicamente e logicamente, si avvicinino gradualmente alla periferia della rete.

In altri termini, la distinzione tra rete *core* e *edge* nel 5G tende a sfumare.

Questo cambiamento introduce nuove sfide per gli operatori chiamati a garantire la sicurezza dei propri clienti, poiché alcune funzioni sensibili si realizzano al di fuori dell'ambiente *core*, che è quello tipicamente caratterizzato da più elevata protezione.

In buona sostanza, la flessibilità architetturale delle reti 5G rende la sicurezza un tema veramente complesso da gestire, in quanto le relative architetture saranno composte da una pluralità di segmenti che vanno dalla parte di accesso radio fino alla rete core, e con una vastità di terminali che svolgono funzioni sempre più complesse; quindi avremo un insieme molto ampio di elementi che presenteranno diversi aspetti di vulnerabilità.

Inoltre, la stessa gestione delle risorse, pensata per essere attuata in maniera virtuale e dinamica, con procedure sia centralizzate che distribuite, potrebbe essere sede di attacchi mai affrontati finora nelle attuali reti cellulari.

Pertanto, si presenta la necessità di conoscere le caratteristiche tecnologiche delle reti e dove risiedono le criticità delle applicazioni su di esse veicolate.

Ai fini della protezione delle infrastrutture critiche e strategiche nazionali si profilano diversi nuovi scenari tra i quali i due seguenti possibili scenari, anche sovrapponibili:

1) investire massicciamente sulla certificazione degli apparati, ai fini della mitigazione dei rischi di sicurezza nazionale
2) definire per quali applicazioni potrebbe essere necessario valutare con attenzione la criticità dell'installazione, sulle reti di rilevanza nazionale, di apparati prodotti da soggetti extra-UE, anche attraverso le procedure per l'esercizio dei poteri speciali.

Iniziative in corso in ambito europeo e nazionale

Ai fini del contenimento degli effetti di attacchi malevoli alle reti 5G, si riportano di seguito le principali iniziative **in ambito europeo**.

- ✓ **CYBERSECURITY ACT**

  In ambito EU, a dicembre scorso la Commissione, il Consiglio e il Parlamento hanno raggiunto, a livello di "Trilogo", l'accordo sul regolamento UE comunemente definito "Cybersecurity Act" (o "Cyber Act"), che rafforzerà il mandato di ENISA (European Union Agency for Network and Information Security), l'Agenzia dell'Unione europea per la cybersicurezza, istituendo anche un perimetro normativo comune per la certificazione della sicurezza informatica.

  Il 12 marzo scorso il testo è stato adottato da parte del Parlamento europeo e, per quanto noto, è prevista a breve la sua approvazione da parte del Consiglio UE.

  Il nuovo quadro di certificazione della sicurezza informatica rafforzerà il mercato unico digitale dell'Unione, accrescendo l'affidabilità dei prodotti e la consapevolezza degli utenti.

  In questo nuovo contesto, che prevede la costituzione di sistemi europei di certificazione di prodotti e servizi ICT, il nostro Paese, per il tramite del Ministero dello sviluppo economico, si trova assolutamente in linea con l'azione europea.

- ✓ **CENTRO EUROPEO DI COMPETENZA**

  Sempre in ambito europeo il Ministero, congiuntamente alla Presidenza del Consiglio dei Ministri, segue i lavori relativi al nuovo regolamento che prevede l'istituzione del "Centro europeo di competenza" sulla cybersecurity e la rete dei centri nazionali di coordinamento.

L'obiettivo di questo nuovo regolamento è quello di creare una rete di Centri di competenza nazionali sulla sicurezza cibernetica (Network of national coordination centres) per indirizzare e coordinare al meglio i finanziamenti per la ricerca e l'innovazione in materia di sicurezza industriale e tecnologica.

Il lavoro di questa rete di Centri sarà coordinato da un Centro europeo di competenza, che avrà anche il compito di facilitare gli investimenti congiunti dell'Unione, degli Stati membri e dell'industria nei progetti di ricerca e innovazione, nelle infrastrutture di sperimentazione, nello sviluppo delle competenze, nonché nella diffusione di prodotti e soluzioni di sicurezza cibernetica in tutto l'ecosistema economico comune.

- ✓ **RACCOMANDAZIONE DELLA COMMISSIONE EUROPEA SUL 5 G**

Al riguardo si coglie l'occasione per citare una recentissima iniziativa europea: il 26 marzo scorso la Commissione europea ha raccomandato una serie di azioni e misure operative volte a rivedere e rafforzare le vigenti norme di sicurezza in questo settore per assicurare che riflettano l'importanza strategica delle reti 5G, nonché l'evoluzione delle minacce, tra le quali l'aumento degli attacchi informatici e il loro crescente livello di sofisticazione.

In tale contesto, entro la fine di giugno 2019, ogni Stato Membro dovrà completare la valutazione nazionale dei rischi ed aggiornare i requisiti di sicurezza vigenti a carico dei fornitori di rete includendo condizioni per garantire la sicurezza delle reti pubbliche.

La raccomandazione, inoltre, prevede azioni da condurre a livello nazionale e a livello UE e consente di avviare una distinzione, per quanto tecnologicamente possibile, tra azioni prescrittive dirette verso gli operatori e azioni (di validazione e certificazione) dirette verso i fornitori degli apparati.

Secondo la raccomandazione, gli Stati membri dovrebbero elaborare requisiti di sicurezza specifici che potrebbero essere applicati nel contesto degli appalti pubblici relativi alle reti 5G, tra cui requisiti obbligatori per l'attuazione di sistemi di certificazione della cibersicurezza. Questi requisiti potrebbero trovare una declinazione nell'attuare le recenti disposizioni Golden Power in tema di tecnologia 5G.

In ambito nazionale molte sono le azioni avviate a protezione delle reti e dei apparati su di esse installati. Di seguito si riportano le principali iniziative.

- ✓ **MISURE DI SICUREZZA E INTEGRITÀ DELLE RETI DI COMUNICAZIONE ELETTRONICA**

A livello nazionale, il 12 dicembre 2018 il Ministro dello sviluppo economico ha emanato un decreto, con il quale sono state previste adeguate misure di natura tecnico-organizzativa per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica e sono stati definiti i casi in cui le violazioni della rete o la perdita di integrità siano da considerarsi "significative".

In virtù di questo provvedimento, i fornitori di reti e servizi di comunicazione elettronica (cosiddetti "operatori TELCO") sono ora tenuti ad osservare specifiche misure di sicurezza e integrità e a comunicare eventuali incidenti informatici "significativi".

Gli operatori TELCO devono assicurare misure atte a garantire, tra l'altro:

- la sicurezza fisica dei locali e delle aree dove sono collocati i *server* e le componenti strategiche delle infrastrutture;
- il rispetto di adeguati *standard* tecnologici delle commesse per l'adeguamento o l'implementazionedell'infrastruttura di rete;
- -la sottoposizione a *test* preventivi di reti, sistemi informativi e nuove versioni del *software* prima del loro utilizzo o del loro collegamento alla rete ed il costante monitoraggio dei sistemi critici;
- la definizione di specifici processi interni diretti a garantire la sicurezza delle reti;
- la gestione e la notifica al CSIRT (Computer Security Incident Response Team) degli incidenti informatici.

In particolare, gli operatori sono tenuti a definire i requisiti dei servizi e prodotti forniti da terze parti e a verificare il rispetto di tali requisiti fissati nei contratti.

- ✓ **CENTRO DI VALUTAZIONE E DI CERTIFICAZIONE NAZIONALE**

Nella medesima prospettiva va letta anche la recente istituzione del Centro di valutazione e certificazione nazionale (CVCN), che si aggiunge ai già attivi OCSI (Organismo di certificazione della sicurezza informatica) e CEVA (Centro di valutazione della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione), operativi presso l'ISCTI del Dicastero.

Sul piano normativo, il DPCM 17 febbraio 2017 aveva definito l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica.

In questo contesto, è stato all'epoca previsto che il Ministero dello sviluppo economico promuovesse "l'istituzione di un centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale".

Successivamente, il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica, varato dalla Presidenza del Consiglio dei Ministri nel marzo 2017, ha precisato che tale Centro sarebbe stato realizzato presso il Ministero dello sviluppo economico.

In tale contesto, il Centro di valutazione e certificazione nazionale, istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019, costituisce, soprattutto in prospettiva, un importante tassello ai fini della sicurezza cibernetica del Paese.

Il Centro è stato istituito presso l'Istituto Superiore delle Comunicazioni e Tecnologie dell'Informazione (ISCTI) del Mise per la competenza acquisita negli anni nel settore della certificazione informatica. Il Ministero ha completato la fase di progettazione del Centro e sta ultimando le procedure per il suo funzionamento, con l'obiettivo di contemperare gli aspetti di sicurezza e le esigenze di mercato delle imprese coinvolte.

In considerazione della complessità della realizzazione del CVCN, il Centro si svilupperà con la necessaria gradualità sulla base delle risorse umane e finanziarie disponibili, avvalendosi

soprattutto nella fase iniziale di collaborazioni con Università e Centri di Ricerca nell'ottica di porre solide basi ad una iniziativa così strategica.

Al di là degli aspetti tecnici di realizzazione del Centro l'impatto delle sue attività dipenderà da una serie di fattori, in particolare la definizione di un quadro normativo che individui le infrastrutture critiche e strategiche - problematica comunque già all'attenzione del DIS - e stabilisca specifici obblighi per l'acquisizione di prodotti e sistemi destinati alle predette infrastrutture. Tale quadro dovrà tenere anche conto delle disposizioni sulla realizzazione del "framework" di certificazione europea, contenute del cosiddetto "Cyber Act", come già detto di prossima adozione nell'Unione Europea.