Roma, martedì 8 ottobre 2019

Alla c.a. IX Commissione (Trasporti, poste e telecomunicazioni)

I Commissione (Affari costituzionali)

Documento lasciato agli atti delle Commissioni

Oggetto: audizione informale Ericsson Telecomunicazioni S.p.A. in relazione all'esame del Disegno di Legge C. 2100 Governo recante conversione in legge del decreto-legge n. 105 del 2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

Premessa

Vista la sintesi necessaria per la presente l'audizione, Ericsson Telecomunicazioni S.p.A. assicura sin da ora la sua disponibilità ad approfondire le tematiche qui esposte, in eventi ed iniziative successive, mettendo a completa disposizione competenze ed esperienze tecniche volte ad accrescere ulteriormente la resilienza delle infrastrutture digitali.

Con riferimento all'oggetto di questa audizione, Ericsson concorda nel merito con quanto espresso dal Disegno di Legge. Il Disegno di Legge adotta un approccio metodologico, con la definizione puntuale della governance di sicurezza, del perimetro di applicazione, del ruolo dei soggetti obbligati e dei criteri di valutazione.

Le reti di telecomunicazione sono assi portanti dello sviluppo e della gestione del Paese. La realizzazione del 5G e dei suoi impieghi, oggi, pone ancor più chiaramente l'accento su aspetti di sicurezza che riguardano le reti in generale, su cui è richiesto di porre in essere strumenti di immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza in ambito cibernetico.

Si riportano quindi di seguito, alcune osservazioni che riteniamo possano essere utili a rafforzare l'efficacia del provvedimento, soprattutto nella sua applicazione, fondamentale per una corretta attuazione dei requisiti di sicurezza.

Ericsson nel mondo - Ericsson è una società europea, fondata nel 1876 a Stoccolma, tra i leader globali nella fornitura di tecnologie e servizi per la comunicazione elettronica. È presente in 180 paesi con oltre 94.500 professionisti. Ogni giorno oltre il 40% del traffico mobile mondiale passa attraverso reti fornite da Ericsson. Nel 2018 ha registrato un fatturato di 210,8 miliardi di SEK. È quotata alla Borsa di Stoccolma e alla Borsa di New York.

Le attività di R&S rappresentano un ambito al quale la società ha da sempre dedicato importanti risorse e investimenti - nel 2018 ha investito in R&S il 18,4% del fatturato globale - registrando risultati di eccellenza a livello mondiale che le permettono oggi di possedere oltre 49.000 brevetti essenziali nel campo delle comunicazioni mobili e di essere il principale contributore alla standardizzazione di tutte le generazioni di reti mobili, 5G compreso.

Ericsson in Europa - Ericsson è presente in 43 Paesi europei, dove impiega circa 35.000 professionisti, tra cui 14.000 ricercatori. L'azienda ha 22 centri R&D europei, dislocati su 15 diversi Paesi, e collabora con oltre 100 università e accademie.

Un modello di investimento locale e non centralizzato, il contatto diretto dei vari siti di R&S nel mondo con clienti ha sempre rappresentato un elemento distintivo del modo di lavorare di Ericsson rispetto ad altri competitor.

Ericsson in Italia – E' presente dal 1918, l'azienda conta tra le sue fila oltre 3.000 professionisti, il 25% dei quali ha un profilo da ricercatore.

Ericsson ha all'attivo 41 anni di Ricerca & Sviluppo in Italia, oggi svolta all'interno dei tre centri di eccellenza mondiale di Genova, Pisa e Pagani (Salerno). Dall'anno 2000 sono oltre 600 i brevetti registrati dai ricercatori italiani, protagonisti anche di diversi record mondiali e responsabili dello sviluppo di soluzioni tecnologiche che stanno contribuendo al lancio delle prime reti 5G nel mondo. Il Centro di R&S di Genova è specializzato sugli apparati dei sistemi ottici e cloud, il Centro di R&S di Pagani sulla sicurezza e intercettazione legale, il Centro di R&S di Pisa sulla fotonica integrata.

Oggi sono decine i progetti EU che vedono coinvolti i ricercatori di Ericsson in Italia.

Con riferimento al 5G - Ericsson è in prima linea nello sviluppo del 5G anche in Italia, come già avvenuto per tutte le precedenti tecnologie mobili. Lo dimostra la presenza globale come primo fornitore con reti 5G commerciali operative nei quattro continenti, nonché i vari primati raggiunti, i più recenti sulla call 5G "Stand Alone end2end" e sui test di Spectrum Sharing 4G/5G.

Il grande contributo alle installazioni massive in USA, Korea ed altri paesi (oltre 210.000 stazioni radio base) dimostrano la capacità di Ericsson di essere un punto di riferimento europeo anche in Italia con prodotti e soluzioni "best in class".

Decreto di Legge n. 105 del 2019 - Con riferimento alle misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, si riportano le seguenti osservazioni:

Politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio

Nei sistemi di telecomunicazione moderni, gli aggiornamenti del software sono molto frequenti e lo saranno ancor più in modelli sempre più programmabili via software. Questi aggiornamenti continui, anche con frequenza quotidiana, sono funzionali al miglioramento delle prestazioni di servizio offerte all'utente, nonché all'aggiornamento e all'incremento dell'efficacia di protezione e sicurezza dei sistemi verso nuovi tipi di attacchi.

Eventuali test di integrità e sicurezza effettuati dopo lo sviluppo dei prodotti e prima di essere rilasciati nelle reti commerciali, siano essi prodotti software o hardware, oltre a non tener conto di questi continui aggiornamenti, sarebbero condizionati dalle innumerevoli configurazioni in rete che ne variano il comportamento reale in campo per esigenze di ogni provider.

Per assicurare l'integrità e la sicurezza delle reti 5G non ci si può dunque affidare alla certificazione del software e/o dell'hardware, perché questa creerebbe una falsa mitigazione del rischio, mentre sarebbe più opportuno adottare dei criteri di conformità alla sicurezza in ogni fase dello sviluppo del Software e dell'Hardware in modo misurabile. Attraverso il "Security by Design" la sicurezza viene inserita nel processo di sviluppo come ogni altra parte che concorre nella definizione della soluzione sin dalla fase di realizzazione, permettendone in ogni momento misurabilità e valutazione dei criteri di aderenza (compliance tecnica e di implementazione).

Ericsson ha definito degli strumenti efficienti atti a ridurre le vulnerabilità ed incrementare la sicurezza durante la fase di sviluppo (vedasi https://www.ericsson.com/en/security)

Anche la struttura organizzativa e la gestione del rischio dovrebbero trasparentemente risultare in ogni contratto e tipologia di servizio, pratica già adoperata da Ericsson con riferimento alle certificazioni ISO 27001 e collegati.

Mitigazione e gestione degli incidenti e alla loro prevenzione

Come correttamente riferito dal Disegno di Legge, è opportuno riferirsi a standard e procedure globali per evitare caratterizzazioni e specificità locali onerose e non armonizzate per tutta la filiera.

Utilizzando una metodologia di garanzia della sicurezza in ogni fase dello sviluppo del prodotto, i fornitori possono dimostrare, in maniera continuativa, che l'implementazione dei protocolli di sicurezza nei loro prodotti è conforme alle linee guida concordate. Ciò permette di sviluppare il prodotto "abbracciando" i requisiti degli standard di telecomunicazione 3GPP.

A tal proposito, si suggerisce di favorire il disegno e l'implementazione di un'architettura di security avente delle solide fondamenta, basate sullo sviluppo dei prodotti mediante un modello assimilabile al framework Ericsson, denominato SRM (Security Reliability Model), nonché aderire al framework "Security Assurance Methodology" (SECAM) e alle certificazioni ISO 27001 in ambito telecomunicazioni, sia in Italia che in eventuali altri centri mondiali di supporto nonché per l'insieme delle società e dei fornitori di tutta la filiera che collaborano allo sviluppo dei prodotti.

Per la mitigazione e gestione degli incidenti e la prevenzione dei casi altamente critici, andrebbero aggiunte opportune misure di assessment, volte a determinare i tempi di reazione del personale di supporto alla sicurezza. Attraverso test ricorrenti andrebbe valutata la propensione alla reattività di persone e sistemi nel riportare gli apparati e servizi in uno stato "verificato", sulla base di diverse possibili configurazioni che l'operatore potrebbe adottare in "campo".

Protezione fisica e logica e dei dati e Integrità delle reti e dei sistemi informativi

Come noto, le reti di telecomunicazioni mobili, ivi comprese le reti 5G, sono generalmente separate in differenti parti logiche: la Rete Radio (sia in modalità Non Stand-Alone che Stand-Alone), la Rete Core (sia in modalità Non Stand-Alone che Stand-Alone), la Rete di Trasporto ed anche i sistemi di supporto alle Operazioni (OSS) ed i sistemi di supporto al Business (BSS).

Tutte queste parti logiche della rete sono esposte a rischi di sicurezza e vulnerabilità.

Infatti, le reti di telecomunicazioni mobili gestiscono differenti tipi di traffico e ciascuna parte logica della rete è coinvolta in maniera differente nella gestione di questi:

- "traffico di segnalazione", per stabilire l'accesso ad un sito web o per stabilire una chiamata voce;

- "traffico utente" che corrisponde al traffico vero e proprio;

- "traffico di controllo" della rete, e cioè comandi e dati scambiati tra i sistemi di controllo (OSS) e reti radio, core e trasporto; tale traffico include la supervisione di rete, le configurazioni di rete e la risoluzione dei problemi;

- il "traffico con i sistemi di gestione (BSS)" che include informazioni quali durata delle connessioni e delle chiamate, orari delle chiamate o connessioni, e tutte le informazioni utili per la fatturazione del traffico e la sottoscrizione degli utenti.

In particolare, meriterebbero di essere attenzionate tutte le componenti "attive" delle reti di telecomunicazione, cioè quelle che gestiscono i differenti tipi di traffico descritti in precedenza, ad eccezione delle componenti "passive" e cioè delle componenti, quali sistemi di condizionamento, alimentazione elettrica etc. che non gestiscono nessun traffico dati.

Monitoraggio, test e controllo

A dimostrazione della solidità della misura di conformità, il monitoraggio della sicurezza deve tradursi nella generazione di report descriventi lo stato di conformità, lungo l'asse temporale del servizio e del progetto. Report generati in modo automatico, renderebbero semplici e trasparenti le verifiche dei soggetti preposti.

Formazione e consapevolezza

È quanto mai opportuno collaborare metodicamente per la sicurezza a tutela di reti, sistemi e servizi informatici da cui dipende l'esercizio delle funzioni essenziali del Paese, mettere a disposizione persone e laboratori di ricerca e sviluppo per un confronto continuo e strutturato.

La sicurezza delle reti è un tema complessivo (end2end), che va oltre lo standard 5G in quanto tale, che rimane comunque il più sicuro mai sviluppato fino ad oggi. La sicurezza complessiva di una rete è dunque qualcosa su cui è coinvolta tutta la filiera dei servizi tecnici, dal dispositivo all'applicazione.

La formazione e la consapevolezza va costruita attraverso l'istituzionalizzazione di momenti di confronto dedicati tra soggetti pubblico/privato lungo tutta la filiera. Fare leva su risorse e competenze locali, permetterebbe tempestività, reattività e uno scambio strutturato di informazioni anche in considerazione della rapidità di evoluzione dei sistemi e delle tecnologie.

Affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale

La sicurezza tecnica resta condizione necessaria ma non sufficiente nella garanzia di sicurezza di un Paese. Nella conformità delle reti e infrastrutture critiche è infatti necessario dimostrare e garantire la sicurezza anche nelle "interdipendenze" tra le infrastrutture, che evidentemente non possono essere solo una prerogativa nazionale. Ciò ha stimolato da tempo il Consiglio dell'UE che ha adottato un programma per la protezione delle infrastrutture critiche, stabilendo un nuovo approccio mirato a costruire una maggiore protezione e resilienza delle infrastrutture critiche interdipendenti.