Commissioni riunite I Affari Costituzionali e IX Trasporti

Disegno di legge AC 2100 – "Conversione in legge del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"

***

Audizione di Vodafone Italia – Romano Righetti – Direttore Affari Esterni

8 ottobre 2019

1. Premessa

- Ringraziamenti a Presidente e Commissari per convocazione su provvedimento molto rilevante per futuro del Paese.
- Comprendiamo e condividiamo esigenza di dotarsi di un unico framework normativo aggiornato ed efficace su sicurezza cibernetica.

2. Vodafone e la sicurezza

- Per VF sicurezza proprie reti + tutela dati clienti sono pilastri fondamentali di processi/procedure/attività.
- Reti 4G + 5G difese da affidabili e specifiche misure di garanzia e sicurezza messe per selezione fornitori e per utilizzazione e manutenzione infrastrutture.
- Informazioni su reti VF efficacemente protette tramite sistema di crittografia a due livelli (Canale criptato tra telefono e SRB + Rete di trasporto criptata tra SRB e rete Core).
- Numerose misure di protezione (policy, governance e metodologia) su ogni singolo elemento (in particolare della Rete Core).
- VF implementa test anti-intrusione per garantire protezione prodotti e i servizi.
- A migliori pratiche sicurezza + certificazioni nazionali utile affiancare standard di sicurezza europeo.

3. Contesto

- Su un ambito molto delicato si intrecciano le complessità dettata delle esigenze di privacy dei clienti e quelle di sicurezza generale delle reti.
- Complessità e delicatezza hanno generato una normativa estremamente articolata che si è sviluppata in pochissimo tempo
    - In Europa Raccomandazione (UE) 2019/534 della Commissione del 26 marzo 2019 con misure entro il 31/12/19
    - In Italia:
        - Decreto MiSE del 12 dicembre 2018 "Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi."
        - Golden Power 5G in decreto Brexit (25 marzo 2019, n. 22).
        - DL 11 luglio 2019, n. 64 Golden Power, non convertito.
        - DPCM 5 settembre 2019.
        - DL 21 settembre 2019, n. 105.

- Esigenza di raccordare la normativa esistente e riconciliare i vari iter burocratici in un processo semplice, dall'esito definito, che consenta di garantire la sicurezza e rispettare la legge senza non ostacolare l'implementazione delle reti (attirando capitali che altrimenti andrebbero altrove).
- Far sì che la normativa spinga verso il concetto di "security by design", una modalità di progettazione che considera sicurezza informatica come parte del servizio e non come requisito accessorio.

4. Vodafone

- La sicurezza di Vodafone è garantita da un framework di sicurezza articolato e integrato tra livello nazionale e di gruppo attraverso:
    - Organizzazione
        - Dipartimento di Corporate Security: sicurezza fisica di tutte le infrastrutture e prestazioni obbligatorie
        - Dipartimento di ICT Security: sicurezza logica delle reti e protezione dei dati personali.
        - Entrambe i dipartimenti hanno responsabilità trasversale su tutti i processi aziendali riportando alla Direzione External Affairs.
    - Policy
        - di network management
        - di cyber defence
        - sulle vendor solutions
    - Governace
        - Protocolli di gestione
        - Protocolli di audit
        - Segregation of cluster (la sicurezza di ogni ambito è gestita indipendentemente rendendo ridondanti i sistemi di sicurezza)
    - Centri di monitoraggio sia a livello di gruppo che a livello nazionale attivi 24 ore al giorno e 7 giorni su 7.
        - NOC (Network Operations Center)
        - SOC (Security Operations Center)

5. L'importanza del 5G

- Servizi 5G non solo evoluzione 4G o 4,5G, ma vero e proprio fattore abilitante Gigabit Society (nuove opportunità sviluppo per cittadini e imprese).
- Prestazioni 5G rivoluzionarie, ma l'architettura conferma comprovata sicurezza e affidabilità reti 4G e 4,5G.
- Per 5G VF utilizzerà molte infrastrutture di rete in uso per 4G, attraverso aggiornamenti e integrazioni.
- Vodafone ha acquistato frequenze 5G con investimento 2,4 mld a cui aggiungerà investimenti per svariati miliardi di euro nei prossimi anni per sviluppare rete;
- VA a Milano con più importante sperimentazione europea 5G (90 mln investimento e oltre 40 progetti);
- Vodafone ha lanciato, prima in Italia, il 5G su rete commerciale in 5 città (100 entro il 2021);

6. Il DL n.105/2019 – Proposte e criticità

- Vodafone si associa e si riconosce alle osservazioni e ai rilievi presentati dal Presidente Pietro Guindani, a nome di ASSTEL.
- Importante ribadire che **DL rivolto correttamente a produttori ICT** (=soggetti destinatari attività di certificazione). **Operatori devono poter comprare HW/SW già certificati**.
- **Proposte miglioramento** DL:
    A. Necessità di collaborazione tra soggetti obbligati e autorità di sicurezza in fase attuativa (definizione misure). Opportuno che **coinvolgimento sia strutturato, continuativo e preventivo per definizione misure** attraverso individuazione tavolo di lavoro con principali interessati sin da fase attuativa.
    B. Imprese già hanno sistemi, policy e processi di sicurezza e selezione dei vendor, testati (nel caso di VF da 20 anni) e possono mettere a disposizione proprie competenze per più efficace realizzazione sistema di sicurezza nazionale cibernetica.
    C. **Fondamentale che legislatore tenga in considerazione sostenibilità per aziende + periodo per eventuale adeguamento** (decisioni di programmazione economico-finanziaria, tempi di procurement e tempi/modi installazione/implementazione non istantanei).
    D. Ad esempio, **tempi e procedure per esercizio controlli** e valutazioni preliminari **non ulteriormente dilatabili**. Diversamente si genererebbe incertezza, a detrimento capacità di Paese e imprese di attrarre investimenti.
    E. Utile spingere per **semplificazione** processi, magari cogliendo spunti proposti da imprese con consultazione pubblica.
    F. DL introduce norma di **integrazione con disciplina Golden Power** (= criteri stabiliti con regolamento per valutazione rischi effettuata da CVCN si applicano anche ad attività propedeutiche a esercizio dei poteri speciali) letta con favore perché prevede definizione di criteri omogenei per valutazione rischi.
    G. **Non condivisibile** introduzione **possibilità di rivedere i provvedimenti già adottati**, ex Golden Power. **Grave elemento di incertezza** per operatori occupati in realizzazione nuove reti 5G con importantissimi investimenti + che già garantiscono massimo rispetto tutte leggi vigenti e piena e costante collaborazione con istituzioni.

Security Governance by Vodafone

Nota di approfondimento sulla governance a presidio della sicurezza implementata da Vodafone Italia S.p.A.

Premessa.

Il rispetto puntuale della normativa europea e nazionale, con particolare riferimento alla gestione e garanzia della sicurezza, è il cardine generale su cui Vodafone organizza il proprio business e la propria struttura organizzativa.

Il Sistema di Controllo Interno e Gestione dei Rischi è fondato su tre linee di difesa, all'interno delle quali le funzioni aziendali di controllo hanno una chiara collocazione e svolgono ruoli ben definiti:

- La prima linea di difesa: i responsabili delle aree operative (risk owner) hanno la responsabilità di assicurare la corretta gestione dei rischi di sicurezza correlati alle attività svolte e di porre in essere adeguati presidi di controllo, nel rispetto dell'assetto organizzativo e degli indirizzi impartiti dal Gruppo Vodafone e dal CEO. I ruoli e le responsabilità di ciascuna unità organizzativa sono definiti nell'ambito del sistema di deleghe e poteri.
- La seconda linea di difesa: le funzioni Risk management e Compliance rispondono all'esigenza di garantire il monitoraggio continuo dei rischi più significativi per l'attività aziendale. Tali funzioni sono prive di compiti operativi e dedicate in via esclusiva a garantire un efficace presidio dei rischi su base permanente ed attraverso un sistema di monitoraggio e reportistica che va al Comitato esecutivo e al Gruppo per ulteriore verifica.
- Con riferimento specifico ai rischi di sicurezza informatica e al loro monitoraggio continuo, un ruolo di seconda linea di difesa è svolto dalla funzione Cyber Security del Gruppo Vodafone, cui è attribuita la responsabilità di definire gli standard per la corretta gestione del rischio Cyber. A questa funzione si affianca la funzione ICT Security di Vodafone Italia, che definisce i requisiti per la gestione dei rischi informatici correlati a servizi/prodotti forniti da terze parti e garantisce il monitoraggio del rispetto degli standard di sicurezza di Vodafone.
- La terza linea di difesa: la funzione Group internal audit garantisce il monitoraggio e la valutazione dell'efficacia e dell'efficienza del Sistema di Controllo Interno e di Gestione dei Rischi. Questa funzione si caratterizza per una spiccata indipendenza dal business e per un elevato grado di autonomia.

Focus aspetti organizzativi interni.

Per presidiare al meglio gli ambiti maggiormente esposti a vari rischi, Vodafone Italia ha individuato tre diverse unità organizzative preposte alla sicurezza aziendale:

1) Corporate Security, guidata dal dott. Fabio Ortolani, che si occupa della sicurezza fisica degli stabilimenti e delle infrastrutture di rete e delle attività di *crisis management/disaster recovery* connesse alla disponibilità e integrità delle infrastrutture critiche del nostro Paese. Questa struttura si occupa, inoltre, di gestire le richieste provenienti dall'Autorità giudiziaria nell'ambito delle c.d. prestazioni obbligatorie, così come di interagire quotidianamente con tutti gli apparati di sicurezza e le forze di polizia giudiziaria;
2) ICT Security, guidata dal dott. Corradino Corradi, che si occupa della protezione dei sistemi informatici con particolare riferimento della tutela dei dati relativi alla privacy dei clienti. Tale struttura è sostanzialmente responsabile di tutta la cyber-sicurezza dell'azienda verso

l'esterno, definendo strategie e requisiti di sicurezza attraverso un approccio c.d. by design (preventiva);

3) Technology Security Officer, che gestisce gli eventi relativi alla sicurezza delle informazioni, presidiando l'analisi ed il contenimento degli attacchi, e mettendo in atto le opportune verifiche ed azioni preventive in base alle minacce riscontrate. Essa inoltre supervisiona la progettazione e l'implementazione sicura dei sistemi ed apparati informatici, qualificandosi come ulteriore presidio della cyber-sicurezza aziendale verso l'interno.

Le funzioni di Corporate Security e ICT Security, che coordinano tutte le attività legate al presidio degli asset aziendali, sono nella Direzione External Affairs, a diretto riporto dell'Amministratore Delegato; questo assetto organizzativo ha l'obiettivo di garantire la massima indipendenza delle funzioni di sicurezza dai processi operativi. Il direttore External Affairs, Dott. Romano Righetti, riferisce mensilmente al Comitato Esecutivo dell'azienda sulle tematiche della sicurezza e della protezione dei dati personali e riporta funzionalmente all'External Affairs Group Director per le stesse tematiche.

Sistemi implementati in azienda.

La struttura operativa a presidio della sicurezza in Vodafone si articola in:

1. un Security Operations Center (SOC), allocato presso la sede di Milano, preposto alla sicurezza degli uffici e di tutta la parte fisica delle infrastrutture tecniche. Il SOC è parte del circuito nazionale delle emergenze per poter fronteggiare crisi e calamità garantendo sempre le comunicazioni anche in condizioni di congestione dovuta ad eventi eccezionali. Il SOC è attivo e presidiato 7 giorni su 7 per 24 ore al giorno. Risponde alla funzione Corporate Security (External Affairs);
2. un Network Operations Center (NOC) per il monitoraggio delle infrastrutture di rete fissa e mobile. Collegato al SOC di sicurezza fisica, dispaccia in tempo reale gli allarmi di intrusione, fumo, alta temperatura ed incendio degli oltre 22.000 apparati tecnici dislocati su tutto il territorio nazionale. Risponde alla funzione di Network;
3. un Global Cyber-security Operations Center (GSOC), presso il Gruppo Vodafone, con compiti di monitoraggio, gestione ed escalation di eventuali allarmi di sicurezza logica relative a tutte le piattaforme tecnologiche di Vodafone Italia. Il CSOC è attivo e presidiato 7 giorni su 7 per 24 ore al giorno. È in collegamento costante con ICT Security e con il Technology Security Officer in Italia.

Inoltre, Vodafone ha in essere un protocollo di collaborazione sia con il Computer emergency responce team (CERT) Nazionale del MISE sia con il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) della Polizia di Stato.

In generale, Vodafone adotta un approccio a 360 gradi al fine di assicurare la sicurezza logica e fisica per la protezione dei dati e delle reti articolato su una fase preventiva e su una reattiva e declinato, oltre che sulla cyber-security, anche sulla sicurezza fisica.

La Cybersecurity preventiva, sotto la responsabilità delle funzioni Corporate Security e ICT Security di External Affairs, in sintesi, è operativamente eseguita attraverso i seguenti strumenti:

- Sicurezza fisica e logica, mediante Firewall, Intrusion Prevention System e Web Application Firewall (WAF) nei sistemi informatici aziendali e nei data center interni;

- Sicurezza applicativa, mediante Vulnerability Assessment, Penetration Test, antivirus/anti-malware ed anti-spam per la parte di servizio e-mail, sempre per i sistemi sia interni sia situati presso terze parti;
- Protezione dei database e degli account di Rete dei dipendenti Vodafone, mediante sistemi di strong authentication, biometria, tracciamento granulare delle operazioni (DB Audit);
- Protezione perimetrale e degli accessi delle sedi tecniche definite strategiche per il sistema Paese;
- Audit annuali su tecnologie, fornitori e processi critici;
- Programmi di formazione ed aggiornamento ai dipendenti e terze parti per una migliore consapevolezza dei rischi cybercrime.

Vodafone, inoltre, svolge una attenta analisi sui nuovi prodotti e sui nuovi servizi prima di una loro utilizzazione, al fine di garantire la "security by design" e la "privacy-by-design".

Quanto alla sicurezza fisica, tutti i data center IT e le centrali di Rete sono protetti da avanzati sistemi di sicurezza perimetrale, di anti-intrusione e di monitoraggio da remoto (CCTV); gli allarmi sono inviati in tempo reale al SOC che garantisce la pronta presa in carico dell'allarme e lo dirama, dopo averlo verificato, alle forze dell'ordine.

La Cybersecurity reattiva di Vodafone invece si concretizza attraverso l'attività di monitoraggio attivo dello stato di sicurezza delle reti e dei servizi erogati 24 ore su 24.