Audizione

dell’Istituto Superiore delle Comunicazioni e delle Tecnologie dell’Informazione – MISE

presso

IX COMMISSIONE PERMANENTE

(Trasporti, poste e telecomunicazioni)

Indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G ed alla gestione dei big data

7 maggio 2019

1. **PREMESSA**

Le tecnologie dell'informazione e della comunicazione costituiscono l’elemento portante della crescita economica: finanza, sanità, energia e trasporti, oltre naturalmente alle telecomunicazioni, dipendono dal corretto funzionamento delle reti e dei sistemi informatici. L’utilizzo di queste tecnologie, inoltre, si va estendendo anche al settore manifatturiero, modificando radicalmente i processi produttivi. In costante sviluppo, grazie alle nuove tecnologie, sono anche i servizi di “e-government”, che permettono di aumentare l’efficienza della Pubblica Amministrazione nel rapporto con i cittadini.

Parallelamente allo sviluppo di nuove tecnologie ed al loro uso estensivo si registra un incremento degli attacchi cyber che diventano sempre più sofisticati e possono colpire il funzionamento dell’apparato statale o la fornitura di servizi essenziali per i cittadini con conseguenti danni economici e pregiudizio per la qualità della vita.

In particolare, il prossimo dispiegamento delle tecnologie di rete di 5^ generazione costituirà un fattore abilitante per lo sviluppo dei servizi digitali. Le reti 5G, infatti, sarà l’infrastruttura portante non solo di nuovi servizi di comunicazione elettronica ma anche di una vasta gamma di servizi essenziali, quali l'energia, i trasporti, i servizi bancari e sanitari e i sistemi di controllo industriale.

Considerato pertanto che molti servizi essenziali dipenderanno dalle reti 5G, le conseguenze di eventuali attacchi ed incidenti informatici potrebbero avere un impatto rilevante su Cittadini e Imprese.

Sarà quindi necessario garantire il massimo della sicurezza delle reti 5G anche in considerazione dell’interconnessione delle infrastrutture e della natura transfrontaliera della minaccia informatica.

E’ proprio su tali aspetti che, nel corso di questa audizione, fornirò un mio contributo, soffermandomi nella parte iniziale sui recenti sviluppi della cyber security relativamente al settore delle comunicazioni elettroniche ed in particolare alla tecnologia 5G.

Innanzitutto, tengo a sottolineare che l’Unione Europea si confronta con la problematica della sicurezza informatica da almeno 15 anni.

Già dal 2004, infatti, l'Unione Europea si è dotata di un'Agenzia per la sicurezza delle reti e dell'informazione, l’ENISA - European Union Agency for Network and Information Security - con l’obiettivo di favorire l’incremento del livello di sicurezza delle reti e dell'informazione nell’UE nonché lo sviluppo di una cultura in materia a vantaggio di cittadini e imprese.

In particolare l’ENISA agisce come centro di competenza per lo scambio di informazioni e buone pratiche tra settore pubblico e privato, analizzando i rischi attuali ed emergenti.

Il noto attacco che, nella primavera del 2007, ha colpito l'Estonia ha fatto crescere ulteriormente in Europa la consapevolezza dei potenziali rischi e della conseguente necessità di rafforzare le capacità nazionali e il coordinamento a livello europeo.

1. **Sicurezza e integrità delle reti di comunicazione elettronica**

Gli articoli 16bis e 16ter del decreto legislativo n. 259 del 2003 recante il Codice delle comunicazioni elettroniche, introdotti a seguito dell’approvazione del decreto legislativo n.70 del 2012 di attuazione della Direttiva 2009/140/CE, prevedono per la prima volta nel panorama nazionale disposizioni in materia di sicurezza e integrità delle reti di comunicazione elettronica: i fornitori di reti e servizi di comunicazione elettronica hanno l’obbligo di adottare misure di sicurezza nell’ottica di ridurre al massimo i rischi di interruzione dei servizi forniti agli utenti e l’obbligo di segnalare al Ministero dello Sviluppo Economico gli incidenti con significativo impatto sui servizi forniti.

Ai sensi dei medesimi articoli le misure di sicurezza ed integrità delle reti ed i casi in cui gli incidenti sono da ritenersi significativi sono definiti con decreto del Ministro dello sviluppo economico.

Il 12 dicembre 2018 il Ministro dello sviluppo economico ha emanato un decreto (GU n.17 del 21-1-2019) con il quale è stata data attuazione ai suddetti articoli 16 bis e 16 ter.

In virtù di questo provvedimento, sono individuate le misure di sicurezza e integrità che gli operatori devono adottare e i casi in cui gli incidenti informatici devono essere comunicati al CSIRT - *Computer Security Incident Response Team* - di cui si parlerà più avanti, e al Ministero dello Sviluppo Economico – Istituto Superiore delle comunicazioni e delle tecnologie dell’informazione (ISCTI).

1. **Sicurezza delle reti 5G**

Nella prospettiva di un uso pervasivo delle reti 5G nel prossimo futuro, appare utile una analisi dei possibili rischi in tema di sicurezza nazionale.

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.

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, in uno scenario in cui l’ampliamento della superficie di attacco porterà verosimilmente ad un incremento nel numero degli attacchi con un livello di sofisticazione sempre crescente.

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 i fornitori di reti e servizi e dirette verso i fornitori degli apparati.

Secondo la raccomandazione della Commissione Europea, 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 la realizzazione di schemi di certificazione della cibersicurezza.

**Panoramica sulla cyber security delle reti e dei sistemi informativi**

Ritengo utile a questo punto fare una panoramica sulla cyber security, soffermandomi su una serie di iniziative in ambito europeo che hanno consentito, anche a livello nazionale, di assistere ad una forte crescita della consapevolezza sia nel settore pubblico che in quello privato e al conseguente avvio di azioni finalizzate al rafforzamento della sicurezza della Pubblica Amministrazione e del Sistema delle Imprese.

* Sicurezza delle reti e dei sistemi informativi

In particolare, con la direttiva dell’Unione europea (UE) 2016/1148, nota come Direttiva NIS, recepita in Italia con il decreto legislativo n. 65 del 2018, sono state introdotte disposizioni volte a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi nell’Unione Europea.

Il Decreto n. 65 ha previsto il rafforzamento della sicurezza informatica nazionale secondo le seguenti linee di azione:

• l’individuazione delle Autorità competenti nei settori strategici identificati a livello europeo, vale a dire energia, infrastrutture e servizi digitali, comparti per i quali è competente il Mise, nonché trasporti, settore bancario e infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile;

• l’individuazione dei cosiddetti operatori di servizi essenziali (OSE) nei settori individuati e la previsione delle misure tecnico-organizzative che questi operatori devono adottare per ridurre il rischio e limitare l’impatto di incidenti informatici, unitamente all’obbligo di notifica di eventi che presentino un rilevante impatto sulla continuità dei servizi e che, quindi, si riflettano sulla collettività;

• la designazione di un “punto di contatto unico” di interfaccia verso l’Unione europea, individuato nel DIS;

• la costituzione presso la Presidenza del Consiglio dei Ministri di un unico CSIRT italiano, che opera in cooperazione con gli omologhi organismi europei.

Con decreto del Ministro dello sviluppo economico del 26 ottobre 2018 all’Istituto superiore delle comunicazioni e tecnologie dell’informazione (ISCTI) è stata attribuita la funzione di Autorità NIS per i settori energia, infrastrutture e servizi digitali.

Il 9 novembre 2018, entro la scadenza prevista dalla norma, sono stati poi individuati con decreto direttoriale gli operatori dei servizi essenziali (OSE) nei settori di nostra competenza e contestualmente, sempre presso l’Istituto, è stato istituito l’elenco nazionale degli OSE individuati dalle Autorità competenti in tutti i settori indicati.

È attualmente in corso l’iter per l’adozione di un DPCM, su proposta del Mise di concerto con il Ministero della pubblica amministrazione, relativo alla costituzione del Comitato tecnico di raccordo delle Autorità NIS nazionali, che sarà istituito presso la Presidenza del Consiglio dei Ministri e avrà la funzione di assicurare la collaborazione tra le medesime Autorità competenti NIS, il CSIRT italiano ed il punto di contatto unico verso l’Europa, vale a dire il DIS.

Allo stato, le Autorità NIS stanno già collaborando per la stesura delle linee guida che dovranno essere emanate a breve.

* CERT Nazionale

Passerò ora a fornire una sintetica descrizione sul CERT (Computer Emergency Response Team) Nazionale di cui l’Italia si è dotato, ai sensi dell’art. 16 bis del D.Lgs 259/2003, a partire dalla data ufficiale di avvio dei servizi che risale al 5 giugno 2014, dopo un periodo di progettazione e sperimentazione.

La mission del CERT Nazionale, che opera presso il Ministero dello sviluppo economico – ISCTI, è quella supportare cittadini e imprese attraverso azioni di sensibilizzazione per la crescita della cultura della sicurezza, e azioni di prevenzione assicurando il coordinamento della risposta ad eventi cibernetici su vasta scala.

I suoi principali obiettivi sono:

• fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini

• cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica, promuovendone l’interazione

• facilitare la risposta ad incidenti informatici su larga scala

• fornire supporto nel processo di soluzione di crisi cibernetica

In tale contesto, il CERT Nazionale rappresenta il punto di riferimento nazionale per la prevenzione, il monitoraggio, l’analisi e il coordinamento della risposta a incidenti informatici verso i CERT europei ed extra-europei.

Per un funzionamento efficace del CERT Nazionale le interazioni con il settore pubblico e con le Imprese sono determinanti:

* COLLABORAZIONI CON IL SETTORE PUBBLICO: Per quanto riguarda il settore pubblico Il CERT nazionale si rapporta costantemente in ambito nazionale con il CERT PA, con il Comando Interforze Operazioni Cibernetiche (CIOC) del Ministero della Difesa e con il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) del Ministero dell’Interno, attraverso un proficuo scambio di informazioni e nell’ambito dei tavoli di coordinamento della Presidenza del Consiglio.
* COLLABORAZIONI CON IL SETTORE PRIVATO: Gli accordi sottoscritti con il settore privato hanno attivato una fattiva collaborazione tra il CERT Nazionale e le strutture di sicurezza informatica di numerose Imprese operanti nei settori delle telecomunicazioni, energia, “e-government”, finanziario/assicurativo, manifatturiero nonché, su un piano diverso, della sicurezza informatica.

Tali imprese e associazioni hanno sottoscritto con l’Istituto Superiore il reciproco impegno a scambiare informazioni relative a minacce, vulnerabilità e incidenti informatici, ma anche a realizzare iniziative di formazione tecnica, ad organizzare eventi e incontri in tema di sicurezza informatica.

In particolare molte delle Imprese che gestiscono o utilizzano reti e sistemi informatici a supporto della fornitura di servizi essenziali siedono ad un Tavolo Tecnico Permanente - creato ad hoc presso il CERT Nazionale - per un confronto diretto sulle tematiche di interesse comune ed un efficiente scambio delle informazioni.

Con il D.Lgs 65 del 2018, come si è già detto il CSIRT è costituito presso la Presidenza del Consiglio dei Ministri.

In attesa dell’approvazione del Decreto della Presidenza del Consiglio dei Ministri che definirà l’organizzazione ed il funzionamento del CSIRT Italiano, il CERT Nazionale sta procedendo con le azioni di progressiva integrazione delle procedure con il CERT-PA (il CERT della Pubblica Amministrazione, gestito da AGID).

A tal proposito, si precisa che il Ministero dello sviluppo economico, attraverso la Direzione Generale Istituto superiore delle comunicazioni e tecnologie dell’informazione (ISCTI), continua ad assicurare l’operatività del CERT (Computer Emergency Response Team) Nazionale, nelle more della piena entrata a regime del neo costituito CSIRT.

1. **Sicurezza dei prodotti e dei sistemi**

Dopo questa rapida carrellata sullo stato dell’arte della “cyber security” delle reti di comunicazione elettronica e sulle reti e sistemi informativi a supporto dei servizi essenziali è opportuno focalizzare l’attenzione anche sulla sicurezza dei prodotti che su tali reti sono installati.

* Centro di valutazione e certificazione nazionale

In questa prospettiva va letta, infatti, la recente istituzione del Centro di valutazione e certificazione nazionale (CVCN) presso il Ministero dello Sviluppo Economico, che si aggiunge ai già attivi OCSI (Organismo di certificazione della sicurezza informatica) per prodotti e sistemi ICT commerciali – attivato nel 2004 - e CE.VA. (Centro di Valutazione) della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione), anch’essi operativi presso l’ISCTI del Ministero dello Sviluppo Economico.

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. La fase di progettazione del Centro è stata ultimata ed è in corso di completamento anche la definizione delle procedure per il suo funzionamento, perseguendo l’obiettivo generale di contemperare gli aspetti di sicurezza e le esigenze di mercato delle imprese coinvolte.

Il 19 aprile 2019 il Direttore dell’ISCTI ha firmato il Decreto che descrive il modello di funzionamento, l’organizzazione ed il piano di sviluppo del CVCN.

La sua operatività si svilupperà secondo un approccio graduale sulla base delle risorse umane e finanziarie disponibili.

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 Governo - 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 in un regolamento di prossima pubblicazione nell’Unione Europea, comunemente denominato “Cyber Act”.

Tale regolamento, che fra l’altro prevede il rafforzamento del mandato dell’ENISA, istituisce un perimetro normativo comune per la certificazione della sicurezza informatica. Il nuovo quadro di certificazione mira a rafforzare 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.