EDITORIALE

Reti mobili 4G e 5G: siamo proprio sicuri?

Il 26 marzo 2019 la Commissione Europea ha pubblicato la raccomandazione 2019/534[1] sulla cibersicurezza delle reti 5G e i rischi derivanti dall'utilizzo delle reti mobili di nuova generazione. L'obiettivo è di stimolare la discussione tra i Paesi Membri e all'interno di ciascuno di questi, ma senza imporre alcun obbligo giuridico. La Commissione Europea ha scelto di non farsi influenzare dalla vicenda USA-Huawei, quindi non imponendo una soluzione unica a livello europeo e lasciando ai singoli Stati l'opportunità di valutare il rischio rilevato per la propria sicurezza nazionale per poi agire di conseguenza. D'altra parte in Europa è in vigore la direttiva 2016/1148 (NIS) del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi, con la quale l'UE affronta la questione della cibersicurezza con un approccio organico e trasversale per rafforzare la resilienza e la cooperazione tra stati membri.

In Italia la questione USA-Huawei è approdata anche al nostro Parlamento mediante l'interrogazione parlamentare al ministro del Lavoro e dello Sviluppo economico del 21 febbraio 2019[2] per chiedergli "*se sia a conoscenza della situazione e se non ritenga opportuno adoperarsi per verificare l'operato di Infratel e soprattutto per promuovere una specifica strategia volta alla tutela degli apparati elettronici circolanti in Italia e del più ampio interesse alla sicurezza cibernetica*".

Si ricorda a tal proposito che "*il progetto WiFi.Italia.it, realizzato attraverso Infratel, società controllata dal Ministero dello sviluppo economico, ha come obiettivo principale quello di permettere a cittadini e turisti di connettersi gratuitamente e in modo semplice a una rete WiFi libera e diffusa su tutto il territorio nazionale; dopo un primo stanziamento di 8 milioni di euro, per il progetto WiFi.Italia.it è previsto un ulteriore finanziamento di* ***45 milioni di euro per l'assegnazione dei quali Infratel non deve ricorrere a una gara****, ma si avvale direttamente di una convenzione per la fornitura di prodotti e servizi per la realizzazione, manutenzione e gestione di reti locali per le pubbliche amministrazioni(la Consip Lan 6), nella quale Huawei risulta come principale fornitore di tutti i dispositivi coinvolti*".

Se da una parte il Parlamento verifica l'operato delle aziende pubbliche, sul versamento delle aziende di telecomunicazioni private "sembra" agire direttamente il governo USA mettendo in guardia sul rischio: secondo The Wall Street Journal[3] si è cercato di convincere una telco italiana ad interrompere l'utilizzo di apparecchiature realizzate da Huawei. Sull'altro piatto della bilancia c'è il rischio, più concreto, che un divieto potrebbe far ritardare all'Europa il lancio del 5G.

Indiscrezioni del WSJ a parte, la Commissione Europea ha stabilito alcune azioni su scala nazionale, in particolare "**entro il 30 giugno 2019** gli Stati membri dovrebbero effettuare una valutazione dei rischi dell'infrastruttura della rete 5G, anche identificando gli elementi più sensibili in relazione ai quali le violazioni della sicurezza avrebbero un impatto negativo significativo. Entro la stessa data gli Stati membri dovrebbero altresì rivedere i requisiti di sicurezza".

Per quanto riguarda le azioni coordinate a livello europeo, **entro il 30 aprile 2019** "gli Stati membri dovrebbero cominciare ad operare nell'ambito di un apposito flusso di lavoro nell'ambito del gruppo di cooperazione", poi **entro il 15 luglio 2019 "**gli Stati membri dovrebbero trasmettere le valutazioni nazionali dei rischi alla Commissione e all'Agenzia dell'Unione europea per la cibersicurezza (ENISA)". Infine, **entro il 1° ottobre 2019** gli Stati dovrebbero completare una revisione congiunta dell'esposizione al rischio, ed entro il **entro il 31 dicembre 2019** dovrebbe essere concordato un insieme di possibili misure di gestione dei rischi a livello nazionale e di Unione.

Come ricordato dalla raccomandazione 2019/534, le reti 5G si baseranno sull'attuale 4ª generazione (4G) delle tecnologie di rete. Recentemente la Korea Advanced Institute of Science and Technology (KAIST)[4], tramite il tool opensource LTEFuzz, ha identificato con successo 15 vulnerabilità precedentemente divulgate sulla rete 4g LTE **e 36 nuove vulnerabilità**, indipendentemente dall'implementazione dei diversi vettori e fornitori di dispositivi. I risultati sono stati classificati in cinque tipi di vulnerabilità. Tra questi sono stati testati anche attacchi che possono essere utilizzati per negare vari servizi LTE, inviare messaggi di phishing e intercettare / manipolare il traffico dei dati. Questa scoperta segue quella dello scorso anno dei ricercatori della Purdue University e della University of Iowa che dimostrarono[5], tramite il tool LTEInspector, che si può modificare il reale mittente degli SMS ed anche intercettarli. Non sappiamo quanto tempo ci vorrà prima di utilizzare le tecnologie in 5G, intanto sarebbe necessario intervenire su quelle attuali per evitare che qualcuno, con strumentazione tecnica anche non molto costosa, possa illegalmente intercettare le nostre comunicazioni.

Giovanni Nazzaro

1 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019H0534&qid=1554017487593&from=IT

2 https://documenti.camera.it/leg18/resoconti/assemblea/html/sed0131/leg.18.sed0131.allegato_b.pdf

3 https://www.wsj.com/articles/european-carriers-like-their-huawei-gear-despite-u-s-concerns-11550140200

4 https://syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf

5 http://homepage.divms.uiowa.edu/~comarhaider/publications/LTE_NDSS18_paper.pdf