PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4781 di Venerdì 25 settembre 2020

UE: valutazione del rischio della sicurezza informatica delle reti 5G

Quali sono i problemi messi in evidenza dall'analisi di rischio sul 5G fatta dall'Unione Europea e quali sono gli strumenti che sono a disposizione per la riiduzione del rischio nel EU Toolbox?

Ormai tutto il mondo ha fame di reti di comunicazione ad altissima velocità, che potranno permettere di scaricare interi film in pochi secondi. Inoltre la proliferazione di apparati IoT certamente porterà ad un carico di traffico non indifferente sulle reti esistenti ed ecco la ragione perché tutti stanno cercando di migrare, seppur gradualmente, verso le reti di nuova generazione, chiamate 5G. Tuttavia sono numerose le perplessità, fra gli esperti di sicurezza informatica, circa il fatto che queste reti, che hanno prestazioni indubbiamente eccezionali, non possano avere delle back door, attraverso le quali organi di sicurezza di vari Stati potrebbero accedere ai contenuti delle comunicazioni.

Come i lettori sanno, gli Stati Uniti sono tra le nazioni più preoccupante di questa possibilità, tant'è vero che hanno posto limiti significativi all'utilizzo di apparati per reti 5G, soprattutto di provenienza cinese. Anche l'Europa si è preoccupata in questo senso ed ecco il motivo per cui è stato affidato a un comitato specializzato l'incarico di sviluppare un documento dal titolo:

EU coordinated risk assessment of the cybersecurity of 5G networks - Report 9 October 2019.

In parallelo, lo stesso comitato specializzato ha sviluppato un documento, che illustra quali strumenti possono essere utilizzati per mitigare i rischi, messi in evidenza nel documento precedente. Questo nuovo documento ha il titolo:

Cybersecurity of 5G networks EU Toolbox of risk mitigating measures - CG Publication 01/2020

Entrambi i documenti sono disponibili per i lettori in allegato.

Vediamo di illustrare rapidamente quali sono i problemi messi in evidenza dall'analisi di rischio e quali sono gli strumenti che sono a disposizione nello EU Toolbox.

Tanto per cominciare, questo documento mette in evidenza come l'utilizzo probabilmente sempre più allargato delle reti 5G potrebbe giocare un ruolo determinante nell'economia digitale e nello sviluppo della società civile, negli anni a venire. Applicazioni nella medicina personalizzata, nella intelligenza artificiale applicata all'agricoltura ed alle reti elettriche, fino a un aumento della mobilità interconnessa, la rete 5G potrebbe coinvolgere le attività sociali e industriali di cittadini, aziende e nazioni. Ecco il motivo per cui i problemi di sicurezza nazionale di tutela dei dati personali devono essere affrontati in modo organico e coordinato, almeno a livello europeo.

L'obiettivo di questo strumento, messo a disposizione dalla commissione NIS cybersecurity su 5G è proprio quello di offrire una serie di strumenti, da utilizzare in modo armonizzato in tutti paesi europei, che possono mettere sotto controllo i rischi che sono stati già messi in evidenza nel documento principale.

Questo documento raccomanda una serie di interventi, da parte degli Stati membri della commissione, che permettano di garantire ai cittadini ed alle imprese, nonché alle nazioni tutte, un utilizzo efficiente ed efficace di questa rete, portando al minimo i rischi afferenti alla sicurezza informatica.

Ecco perché questo documento mette in evidenza la necessità di stabilire regole stringenti di controllo dell'accesso, l'adozione di strumenti di monitoraggio del traffico e limitazioni nel consentire a soggetti terzi di intervenire sulla rete stessa. Inoltre è indispensabile che ogni operatore di telecomunicazione adotti una strategia, che gli permetta di rifornirsi da vari fornitori, in maniera che, ove un fornitore presenti problemi non tanto di consegna, ma di qualità e affidabilità del prodotto, sia possibile trovare una soluzione alternativa.

Inoltre, per rimanere a cavallo della tigre, il documento raccomanda all'unione europea di investire in ricerca e sviluppo avanzati, che possono permettere di tenere sotto controllo la sicurezza di questa rete e pensare già da adesso a futuri schemi, meglio ancora se validati da processi di certificazione.

Inoltre il documento, anche se approvato da rappresentanti di tutte le nazioni europee, dalla commissione e dall'agenzia per la cybersecurity dell'unione europea, al momento rappresenta uno strumento, che è solo raccomandato e non è ancora imposto come obbligatorio. Non vi è però da stupirsi se, anche a breve, l'adozione delle misure raccomandate in questo documento possa diventare obbligatoria per tutte le nazioni. Anche in questo caso, purtroppo, bisognerà che capiti qualche grosso inconveniente, perché si passi dalla raccomandazione all'obbligo.

Un'attenzione particolare, in questo documento, è posta alla possibilità di interferenze sulla rete, che siano causate dall'azione ostile di un paese terzo. Ecco il motivo per cui si raccomanda di avere sempre a disposizione soluzioni alternative, nella scelta dei fornitori.

È bene ricordare, a proposito, che già oggi, a livello unione europea, sono disponibili dei documenti di riferimento che permettono di migliorare il livello sicurezza della rete 5G.

Ad esempio lo **EU telecommunication framework** impone degli obblighi agli operatori di telecomunicazioni e gli Stati membri devono monitorare attentamente il comportamento di questi operatori.

Lo **European electronic communication code**, che al 21 dicembre 2020 sostituirà l'attuale quadro di riferimento, introduce misure ancora più restrittive e indicazioni su come gestire incidenti afferenti alla sicurezza ed alla continuità operativa.

Anche la **direttiva NIS - Network and Information Security** richiede agli operatori attivi in settori essenziali, come l'energia, la finanza, la salute, il trasporto, eccetera, di prendere appropriate misure di sicurezza e segnalare subito, a livello europeo, eventuali incidenti afferenti alla sicurezza. Sarà così possibile adottare misure correttive che siano efficaci a livello europeo. Questa direttiva dovrebbe essere riesaminata ed aggiornata prima della fine del 2020.

Infine, occorre ricordare il **cybersecurity act**, che è entrato in vigore a giugno 2019, che stabilisce un quadro di riferimento per gli schemi di certificazione per prodotti, processi e servizi afferenti alle telecomunicazioni.

Una volta attuate queste indicazioni, gli schemi di certificazione potranno garantire che l'operatore ed il fornitore dei prodotti abbiano messo in essere specifiche misure di sicurezza, a garanzia dei cittadini, delle aziende e dell'intera nazione.

Raccomando ai lettori di tenere sotto attento controllo la successiva evoluzione di questi documenti, perché la conoscenza del rischio è il primo passo per metterlo sotto controllo. Il responsabile della sicurezza informatica di grandi e piccole aziende nazionali dovrà tenersi sempre aggiornato su questo tema, in maniera da scegliere sin da adesso le soluzioni più garantistiche, tra quelli disponibili sul mercato.

EU coordinated risk assessment of the cybersecurity of 5G networks_-_Report_9 October 2019 (PDF)

Cybersecurity of 5G networks_EU Toolbox of risk mitigating measures - CG Publication_01/2020 (PDF)

Adalberto Biasiotti

---

www.puntosicuro.it