RISPOSTE DELLA COMMISSIONE EUROPEA ALLA RELAZIONE SPECIALE DELLA CORTE DEI CONTI EUROPEA:

"L'INTRODUZIONE DEL 5G NELL'UE: VI SONO RITARDI NEL DISPIEGAMENTO DELLE RETI E LE QUESTIONI DI SICUREZZA RIMANGONO IRRISOLTE"

SINTESI

Osservazioni introduttive della Commissione

I. Il dispiegamento rapido e sicuro delle reti 5G è una delle principali priorità della Commissione europea. Proteggere le reti 5G dalle minacce informatiche significa valutare e mitigare le minacce e i rischi. Tali minacce e rischi sono stati individuati e valutati congiuntamente dagli Stati membri, con il sostegno della Commissione e dell'ENISA, e su tale base è stata individuata una serie di misure complete per mitigare detti rischi. Sebbene alcuni Stati membri si stiano ancora adoperando al riguardo, la stragrande maggioranza di essi ha già rafforzato o sta rafforzando i requisiti di sicurezza per le reti 5G sulla base del pacchetto di strumenti dell'UE.

Il pacchetto di strumenti dell'UE è stato riconosciuto come un quadro di riferimento completo per affrontare i rischi per la sicurezza del 5G.

L'azione coordinata per la cibersicurezza del 5G a livello dell'UE e il pacchetto di strumenti dell'UE si inseriscono in un quadro europeo più ampio per la protezione delle reti di comunicazione elettronica e di altre infrastrutture essenziali, integrando misure esistenti quali il codice europeo per le comunicazioni elettroniche, il quadro per le telecomunicazioni, la legge sulla cibersicurezza e la direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) e, se del caso, le norme sulla libera circolazione stabilite nel trattato e nella Carta dei diritti fondamentali dell'UE.

III. Il 5G svolgerà un ruolo essenziale nella digitalizzazione della nostra economia e della nostra società negli anni a venire. Dobbiamo garantire che le reti 5G siano sicure dal punto di vista della cibersicurezza e resilienti contro il crescente numero di incidenti e minacce informatici. Per tale motivo e per affrontare efficacemente i principali rischi per le reti 5G, come gli attacchi informatici criminali, lo spionaggio e il sabotaggio, in modo coordinato, la Commissione e gli Stati membri hanno messo in atto un processo di coordinamento volto a definire e attuare un quadro completo di sicurezza per il 5G, sotto forma di un pacchetto di misure, concordato nel gennaio 2020, per la mitigazione del rischio. Sebbene alcuni Stati membri si stiano ancora adoperando al riguardo, la stragrande maggioranza di essi ha già rafforzato o sta rafforzando i requisiti di sicurezza per le reti 5G sulla base del pacchetto di strumenti dell'UE.

VII. Il pacchetto di strumenti dell'UE fornisce un quadro di riferimento per promuovere la coerenza nel mercato interno, rispettando nel contempo le competenze nazionali in materia di sicurezza in questo settore.

Per quanto riguarda l'approccio degli Stati membri nei confronti dei fornitori ad alto rischio, la Commissione ritiene che sarà possibile eseguire una valutazione definitiva solo quando saranno disponibili maggiori informazioni.

Ora che l'attuazione è in corso, la Commissione sta collaborando con gli Stati membri in seno al gruppo di cooperazione NIS per promuovere l'allineamento e la convergenza degli approcci nazionali.

IX. Primo trattino - La Commissione accoglie la raccomandazione.

Secondo trattino - La Commissione accoglie la raccomandazione.

Terzo trattino - La Commissione accoglie la raccomandazione.

La Commissione effettuerà la valutazione tenendo conto delle competenze nazionali.

INTRODUZIONE

04. La Commissione riconosce l'esistenza di rischi per la sicurezza del 5G, tuttavia sottolinea che la tecnologia e gli standard delle reti 5G possono comunque portare miglioramenti sotto il profilo della sicurezza rispetto alle generazioni di reti precedenti.

OSSERVAZIONI

30. Sebbene il 4G sia già in grado di supportare un'ampia gamma di servizi, il 5G dovrebbe rappresentare un notevole "balzo in avanti", un cambiamento radicale rispetto al 4G, pertanto la sfida principale è costituita dalla transizione dal 4G al 5G con il dispiegamento del 5G in tutta l'UE. Il rischio di un divario digitale esiste comunque, ma si prevede di affrontarlo tra le priorità strategiche del programma "Percorso per il decennio digitale" in relazione ai percorsi verso il conseguimento dell'obiettivo del 100 % di copertura 5G in tutte le zone abitate entro il 2030, sostenendo quindi gli Stati membri affinché intervengano in questo settore, soprattutto per quanto riguarda l'accesso nelle zone rurali.

32. L'Osservatorio 5G è stato una risorsa affidabile per monitorare il dispiegamento del 5G nell'UE e all'esterno dell'UE, anche se si sono riscontrate alcune carenze. I servizi della Commissione si aspettano di avere a disposizione informazioni più aggiornate con il nuovo contraente.

Risposta comune della Commissione ai paragrafi 48 e 49

La Commissione ritiene che la scelta dello strumento (raccomandazione) e l'approccio collaborativo con gli Stati membri per individuare i rischi e le misure di mitigazione rappresentino la linea d'azione più appropriata per affrontare i rischi per la sicurezza del 5G in modo rapido, efficace e concertato.

La Commissione ha optato per una raccomandazione e ha scelto di lavorare in collaborazione con gli Stati membri per individuare i rischi e le misure di mitigazione, in considerazione della complessità e della natura trasversale della materia, che spazia da competenze nazionali a competenze dell'UE e interessa l'importante dimensione della sicurezza nazionale. Inoltre la Commissione ha tenuto conto del fatto che gli Stati membri presentano contesti nazionali molto diversi (struttura del mercato, capacità in materia di cibersicurezza, informazioni sulle minacce, ecc.).

Il pacchetto di strumenti dell'UE rappresenta uno strumento agile basato sul rischio per affrontare le problematiche di sicurezza, il che ha permesso di gestire gli aspetti della cibersicurezza del 5G in modo tempestivo ed efficiente.

Nella sua comunicazione "Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE" del gennaio 2020, la Commissione ha annunciato che avrebbe fornito sostegno all'attuazione delle misure del pacchetto di strumenti relative ai requisiti di sicurezza, in particolare per quanto riguarda le pertinenti disposizioni della normativa europea sulle comunicazioni elettroniche, e preso in esame il valore aggiunto di eventuali atti di esecuzione che specifichino misure di sicurezza tecniche e organizzative al fine di integrare le norme nazionali e rafforzare l'efficacia e la coerenza delle misure di sicurezza imposte agli operatori.

Risposta comune della Commissione ai paragrafi 51 e 52

Nel contesto del riesame della raccomandazione della Commissione, che ha avuto luogo nel dicembre 2020, la Commissione ha interpellato le autorità competenti di tutti gli Stati membri, le quali hanno definito l'azione coordinata dell'Europa in materia di cibersicurezza del 5G tempestiva, efficace e proporzionata. L'approccio collaborativo tra le autorità nazionali, la Commissione, l'ENISA e altri portatori di interessi pertinenti è stato considerato adatto ad affrontare questa complessa questione. Ha

permesso di definire in modo tempestivo obiettivi e metodologie comuni, consentendo al contempo agli Stati membri di adattare le misure alle loro circostanze nazionali.

Il pacchetto di strumenti dell'UE e la relazione sullo stato dei lavori pubblicata dal gruppo di cooperazione NIS nel luglio 2020 raccomandano di definire piani di attuazione e/o periodi di transizione per gli operatori che attualmente utilizzano apparecchiature di fornitori ad alto rischio o che avevano già stipulato contratti con fornitori ad alto rischio prima dell'adozione del pacchetto di strumenti dell'UE (ad esempio tenendo conto dei cicli di aggiornamento delle apparecchiature, in particolare della migrazione da reti 5G *non-standalone* a reti 5G *standalone*, cioè da "non autonome" ad "autonome").

55. La Commissione prende nota delle osservazioni comunicate dalla Corte dei conti europea.

Per sostenere ulteriormente la loro attuazione, sin dall'approvazione del pacchetto di strumenti dell'UE i relativi criteri per valutare i fornitori ad alto rischio sono stati oggetto di numerosi scambi tra le autorità nazionali competenti in seno al gruppo di cooperazione NIS.

56. Il pacchetto di strumenti dell'UE raccomanda di prendere in considerazione i fattori di rischio presentati nella valutazione dei rischi coordinata a livello dell'UE e le informazioni specifiche per paese (ad esempio la valutazione delle minacce fornita dai servizi di sicurezza nazionali, ecc.) per valutare il profilo di rischio dei fornitori.

61. La capacità del fornitore di assicurare la fornitura è uno dei criteri raccomandati dal pacchetto di strumenti dell'UE per valutare il profilo di rischio dei fornitori. La capacità di assicurare la fornitura potrebbe anche essere influenzata da possibili sanzioni commerciali irrogate a un particolare fornitore, come indicato nello scenario di rischio sulla dipendenza di cui alla valutazione dei rischi coordinata a livello dell'UE.

Risposta comune della Commissione ai paragrafi 70 e 73

La Commissione e gli Stati membri stanno condividendo informazioni dettagliate sull'attuazione del pacchetto di strumenti a livello nazionale in seno al gruppo di cooperazione NIS. Per quanto riguarda la divulgazione di informazioni non pubbliche, la responsabilità spetta agli Stati membri.

Risposta comune della Commissione ai paragrafi da 74 a 76 e al riquadro 5

Il pacchetto di strumenti dell'UE fornisce un quadro di riferimento per promuovere la coerenza nel mercato interno, rispettando nel contempo le competenze nazionali in materia di sicurezza in questo settore.

Per quanto riguarda l'approccio degli Stati membri nei confronti dei fornitori ad alto rischio, la Commissione ritiene che sarà possibile eseguire una valutazione definitiva solo quando saranno disponibili maggiori informazioni.

Ora che l'attuazione è in corso, la Commissione sta collaborando con gli Stati membri in seno al gruppo di cooperazione NIS per promuovere l'allineamento e la convergenza degli approcci nazionali.

CONCLUSIONI E RACCOMANDAZIONI

81. Il dispiegamento rapido e sicuro delle reti 5G è una delle principali priorità della Commissione. Proteggere le reti 5G dalle minacce informatiche significa valutare e mitigare le minacce e i rischi. Tali minacce e rischi sono stati individuati e valutati congiuntamente dagli Stati membri, con il sostegno della Commissione e dell'ENISA, e su tale base è stata individuata una serie di misure complete per mitigare detti rischi. Sebbene alcuni Stati membri si stiano ancora adoperando al riguardo, la stragrande maggioranza di essi ha già rafforzato o sta rafforzando i requisiti di sicurezza per le reti 5G sulla base del pacchetto di strumenti dell'UE.

Il pacchetto di strumenti dell'UE fornisce un quadro di riferimento completo per affrontare i rischi per la sicurezza del 5G.

83. Il 5G rappresenta un notevole "balzo in avanti", un cambiamento radicale rispetto al 4G, pertanto la sfida principale per evitare il divario digitale è costituita dalla transizione dal 4G al 5G in tutta l'UE.

Le specifiche del 5G coprono un'intera gamma di indicatori di performance, legati in particolare a casi d'uso verticali, che possono includere, tra l'altro, requisiti di affidabilità, velocità di istanza del servizio, flessibilità di attuazione e livelli di sicurezza.

Raccomandazione 1 – Promuovere un dispiegamento bilanciato e tempestivo delle reti 5G nell'UE

a) La Commissione accoglie la raccomandazione.

La Commissione collabora con gli Stati membri per elaborare una definizione comune della qualità del servizio attesa per le reti 5G. Nel contesto del decennio digitale e della proposta di decisione sul programma di politica digitale per il 2030, la Commissione intende collaborare con gli Stati membri per un approccio comune alla qualità del servizio 5G nell'UE, anche in termini di comparabilità delle misure e dei dati di monitoraggio.

La qualità del servizio non riguarda solo la velocità e la latenza, ma copre un'intera gamma di indicatori di performance legati in particolare a casi d'uso verticali.

La Commissione intende collaborare con gli Stati membri per definire tali misurazioni, nonché per effettuare controlli annuali e raccomandare politiche, misure e azioni per raggiungere la piena copertura 5G entro il 2030.

Il programma di politica digitale istituirà una solida governance attraverso un meccanismo di monitoraggio e cooperazione per garantire che siano compiuti progressi verso la realizzazione degli obiettivi del programma strategico, compreso il dispiegamento del 5G, e raccomandare azioni correttive degli Stati membri a tale proposito.

b) La Commissione accoglie la raccomandazione.

c) La Commissione accoglie la raccomandazione.

Raccomandazione 2 – Promuovere tra gli Stati membri un approccio concordato alla sicurezza del 5G

a) La Commissione accoglie la raccomandazione.

La Commissione valuterà, insieme agli Stati membri, la necessità di ulteriori azioni o sostegno, ad esempio sotto forma di orientamenti relativi a determinati aspetti del pacchetto di strumenti dell'UE.

b) La Commissione accoglie la raccomandazione.

La Commissione monitorerà e riferirà sulla questione in piena collaborazione con gli Stati membri e l'ENISA.

c) La Commissione accoglie la raccomandazione.

Raccomandazione 3 – Affrontare l'impatto che gli approcci divergenti degli Stati membri alla sicurezza del 5G esercitano sull'efficace funzionamento del mercato unico

a) La Commissione accoglie la raccomandazione.

b) La Commissione accoglie la raccomandazione.

La Commissione effettuerà la valutazione tenendo conto delle competenze nazionali.

Nell'ambito del pacchetto di strumenti dell'UE, spetta agli Stati membri decidere la portata esatta delle restrizioni adeguate e/o delle esclusioni necessarie per elementi essenziali definiti critici e sensibili

nella valutazione dei rischi coordinata a livello dell'UE (ad esempio funzioni della rete centrale, funzioni di gestione e orchestrazione della rete e funzioni di accesso alla rete), allo scopo di mitigare efficacemente i rischi individuati, tenendo conto anche della valutazione delle minacce da parte dei servizi nazionali di intelligence. Gli Stati membri hanno il diritto di adottare misure relative alla sicurezza nazionale, comprese potenziali restrizioni o esclusioni per i fornitori ad alto rischio.