Consiglio dell'Unione europea

Bruxelles, 18 dicembre 2020
(OR. en)

14150/20
ADD 3

Fascicolo interistituzionale: 2020/0359(COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	16 dicembre 2020
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	SWD(2020) 344 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO che accompagna il documento Proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148

Si trasmette in allegato, per le delegazioni, il documento SWD(2020) 344 final.

All: SWD(2020) 344 final

COMMISSIONE
EUROPEA

Bruxelles, 16.12.2020
SWD(2020) 344 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di direttiva del Parlamento europeo e del Consiglio

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Scheda di sintesi

Valutazione d'impatto sul *riesame della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (di seguito, "la direttiva NIS")*

A. Necessità di intervenire

Qual è il problema e perché si pone a livello dell'UE?

Nonostante i risultati considerevoli, la direttiva NIS, che ha spianato la strada a un significativo cambiamento di mentalità e dell'approccio istituzionale e normativo alla cibersicurezza in molti Stati membri, mostra ormai anche i suoi limiti. La trasformazione digitale della società (intensificata dalla crisi COVID-19) ha ampliato il panorama delle minacce e lancia nuove sfide, che richiedono risposte adeguate e innovative. Gli attacchi informatici sono in continuo aumento, molti dei quali, sempre più sofisticati, provengono da un'ampia gamma di fonti interne ed esterne all'UE.

Sulla base della valutazione del funzionamento della direttiva NIS, la valutazione d'impatto ha individuato i seguenti problemi: un basso livello di ciberresilienza delle imprese operanti nell'UE; un livello di resilienza differente tra Stati membri e tra settori, una carente consapevolezza situazionale comune e la mancanza di una risposta comune alle crisi. Ad esempio, per effetto di alcuni di questi problemi e fattori determinanti, vi sono situazioni in cui alcuni importanti ospedali di uno Stato membro non rientrano nell'ambito di applicazione della direttiva NIS e pertanto non sono tenuti ad attuare le risultanti misure di sicurezza, mentre in un altro Stato membro quasi tutti gli ospedali sono soggetti ai requisiti di sicurezza della direttiva NIS.

Quali sono gli obiettivi da conseguire?

Gli obiettivi generali del riesame della NIS sono tre:

1. **aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea in tutti i settori pertinenti,** adottando norme che assicurino che tutti i soggetti pubblici e privati del mercato interno, che svolgono funzioni importanti per l'economia e la società nel complesso, siano tenuti ad adottare adeguate misure di cibersicurezza;
2. **ridurre le incongruenze in termini di resilienza sul mercato interno nei settori già disciplinati dalla direttiva,** attraverso un ulteriore allineamento 1) dell'ambito di applicazione de facto, 2) dei requisiti di sicurezza e segnalazione degli incidenti, 3) delle disposizioni che disciplinano la vigilanza e l'attuazione nazionali e 4) delle capacità delle autorità competenti negli Stati membri;
3. **migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta,** adottando misure atte ad aumentare il livello di fiducia tra le autorità competenti, condividendo maggiori informazioni e definendo regole e procedure in caso di incidenti o crisi su vasta scala.

Qual è il valore aggiunto dell'intervento a livello dell'UE (sussidiarietà)?

La resilienza in termini di cibersicurezza all'interno dell'Unione non può essere efficace se affrontata in modo diverso nei vari silos nazionali o regionali. La direttiva NIS ha ovviato a questa carenza definendo un quadro per la sicurezza delle reti e dei sistemi informativi a livello nazionale e dell'Unione. Tuttavia il suo recepimento e la sua attuazione hanno portato alla luce anche difetti intrinseci di alcune disposizioni o approcci, come la poco chiara delimitazione del suo ambito di applicazione. Inoltre, con la crisi COVID-19, l'economia europea è diventata dipendente dai sistemi informatici e di rete come mai prima d'ora,

mentre settori e servizi sono sempre più interconnessi. Il primo riesame periodico della direttiva NIS ha creato pertanto l'opportunità di un'ulteriore azione dell'UE. L'intervento dell'UE che va oltre le attuali misure della direttiva NIS è giustificato principalmente dai seguenti fattori: i) la natura transfrontaliera del problema; ii) le potenzialità degli interventi dell'UE volti a migliorare e agevolare strategie nazionali efficaci; iii) il contributo degli interventi strategici concertati e collaborativi della NIS volti a un'efficace protezione dei dati e della vita privata.

B. Soluzioni

Quali sono le varie opzioni per conseguire gli obiettivi? Ne è stata prescelta una? In caso negativo, indicare i motivi.

La valutazione d'impatto ha esaminato quattro opzioni strategiche: 0) mantenimento dello status quo; 1) misure non legislative volte a uniformare il recepimento; 2) modifiche limitate alla direttiva NIS ai fini di una maggiore armonizzazione; 3) modifiche sistemiche e strutturali della direttiva NIS. L'opzione 1 è stata scartata nella fase iniziale in quanto non si discosta molto dallo status quo. La valutazione d'impatto conclude che **l'opzione prescelta** è l'opzione 3 (ossia **modifiche sistemiche e strutturali del quadro NIS**), in quanto prevedrebbe un cambio di approccio più profondo che interessa un segmento più ampio delle economie dell'Unione, seppure con una vigilanza più mirata rivolta in modo proporzionale a imprese chiave e di grandi dimensioni, determinando chiaramente al contempo l'ambito di applicazione. Semplificherebbe altresì e armonizzerebbe ulteriormente gli obblighi imposti alle imprese in termini di sicurezza, creerebbe una definizione più efficace degli aspetti operativi e stabilirebbe una chiara base per la responsabilizzazione (accountability) e le responsabilità condivise dei soggetti pertinenti e incentiverebbe la condivisione di informazioni.

Quali sono le opinioni dei diversi portatori di interessi? Chi sono i sostenitori delle varie opzioni?

La maggioranza delle autorità competenti e delle imprese si è mostrata favorevole a una revisione della direttiva NIS. Nelle varie consultazioni, hanno segnalato che una direttiva NIS rivista dovrebbe disciplinare ulteriori settori e sottosettori, uniformare o razionalizzare ulteriormente le misure di sicurezza e gli obblighi di segnalazione. Anche i portatori di interessi si sono espressi favorevolmente rispetto a nuovi concetti o misure strategiche che fanno parte solo dell'opzione preferita (ad esempio politiche in materia di sicurezza della catena di approvvigionamento, istituzionalizzazione di un quadro operativo UE di gestione delle crisi).

C. Impatto dell'opzione prescelta

Quali sono i vantaggi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione prescelta apporterebbe vantaggi significativi: le stime effettuate sulla base di un modello economico sviluppato da uno studio a sostegno del riesame della NIS indicano che l'opzione prescelta può portare a una riduzione pari a 11,3 miliardi di EUR dei costi degli incidenti di cibersicurezza.

L'ambito di applicazione settoriale sarebbe notevolmente ampliato nel quadro della NIS, ma oltre ai vantaggi di cui sopra, l'onere che potrebbe essere creato dai requisiti della NIS, in particolare dal punto di vista della vigilanza, sarebbe anche bilanciato sia per i nuovi soggetti da comprendere nell'ambito di applicazione sia per le autorità competenti. Infatti il nuovo quadro della NIS definirebbe un approccio a due livelli, incentrato su soggetti chiave e di grandi dimensioni e su una differenziazione del regime di vigilanza che consenta la vigilanza solo ex post (ossia reattiva e senza un obbligo generale di documentare sistematicamente la conformità) per un ampio numero di tali soggetti, in particolare quelli considerati

"importanti" ma non "essenziali".

Complessivamente, l'opzione strategica prescelta determinerebbe efficienti compromessi e sinergie, con le migliori potenzialità tra tutte le opzioni strategiche analizzate per garantire un livello di ciberresilienza superiore e coerente dei soggetti chiave all'interno dell'Unione, con conseguenti risparmi di costi sia per le imprese che per la società.

Quali sono i costi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?

L'opzione strategica prescelta comporterebbe inoltre alcuni costi di conformità e di esecuzione per le autorità competenti degli Stati membri (è stato stimato un aumento complessivo di risorse di circa il 20-30 %). Il nuovo quadro apporterebbe tuttavia anche benefici sostanziali attraverso una migliore panoramica delle imprese chiave e l'interazione con esse, una maggiore cooperazione operativa transfrontaliera e a meccanismi di assistenza reciproca e di revisione tra pari. Ciò comporterebbe un aumento generale delle capacità di cibersicurezza in tutti gli Stati membri.

Per le imprese che rientrerebbero nell'ambito di applicazione del quadro NIS, si stima che per i primi anni successivi all'introduzione del nuovo quadro NIS sarebbe necessario un aumento massimo del 22 % della spesa corrente per la sicurezza delle TIC (tale aumento sarebbe del 12 % per le imprese già rientranti nell'ambito di applicazione della direttiva NIS vigente). Tuttavia, questo aumento medio della spesa per la sicurezza delle TIC porterebbe ad un beneficio proporzionale di tali investimenti, dovuto in particolare a una considerevole riduzione dei costi degli incidenti di cibersicurezza (stimata a 11,3 miliardi di EUR in dieci anni).

Quale sarà l'incidenza sulle PMI e sulla competitività?

Secondo l'opzione prescelta, le piccole imprese e le microimprese non rientrerebbero nell'ambito di applicazione del quadro NIS. Per le medie imprese, è probabile che vi sia un aumento del livello di spesa per la sicurezza delle TIC nei primi anni successivi all'introduzione del nuovo quadro NIS. Allo stesso tempo, l'aumento del livello dei requisiti di sicurezza per tali soggetti incentiverebbe anche le loro capacità di cibersicurezza e contribuirebbe a migliorare la loro gestione del rischio relativo alle TIC.

L'impatto sui bilanci e sulle amministrazioni nazionali sarà significativo?

Vi sarebbe un impatto sui bilanci e sulle amministrazioni nazionali: si potrebbe trattare di un aumento stimato di circa il 20-30 % delle risorse a breve e medio termine.

Sono previsti altri impatti significativi?

Non sono previsti altri impatti negativi significativi. L'opzione strategica prescelta dovrebbe determinare capacità di cibersicurezza più solide e di conseguenza avrebbe un maggiore effetto attenuante sul numero e sulla gravità degli incidenti, comprese le violazioni di dati. È inoltre probabile che abbia un impatto positivo nel garantire parità di condizioni tra gli Stati membri di tutti i soggetti rientranti nell'ambito di applicazione della NIS e che riduca le asimmetrie inerenti alle informazioni sulla cibersicurezza.

Proporzionalità?

L'opzione prescelta non va oltre ciò che è necessario per raggiungere in modo soddisfacente gli obiettivi specifici. L'allineamento e la razionalizzazione delle misure di sicurezza e degli obblighi di comunicazione previsti sono relativi alle richieste degli Stati membri e delle imprese di migliorare il quadro attuale.

D. Tappe successive

Quando saranno riesaminate le misure proposte?
Il primo riesame avrà luogo 54 mesi dopo l'entrata in vigore dello strumento giuridico. La Commissione dovrebbe fornire al Parlamento europeo e al Consiglio una relazione sul riesame compiuto. Il riesame dovrebbe essere preparato con il sostegno dell'ENISA e del gruppo di cooperazione.