Consiglio dell'Unione europea

Bruxelles, 14 settembre 2017
(OR. en)

12183/17
ADD 2

Fascicolo interistituzionale: 2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	SWD(2017) 501 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE SINTESI DELLA VALUTAZIONE D'IMPATTO che accompagna il documento Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")

Si trasmette in allegato, per le delegazioni, il documento SWD(2017) 501 final.

All.: SWD(2017) 501 final

COMMISSIONE
EUROPEA

Bruxelles, 13.9.2017
SWD(2017) 501 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 502 final}

A. NECESSITÀ DI AZIONE

In cosa consiste il problema e perché è considerato tale?

Le tecnologie digitali e internet sono i pilastri dell'economia e della società dell'UE. Settori economici cruciali come i trasporti, l'energia, la sanità e la finanza dipendono sempre più dalle reti e dai sistemi informativi per lo svolgimento delle loro attività principali. L'internet degli oggetti connette oggetti e persone attraverso le reti di comunicazione. Questa nuova realtà crea opportunità senza precedenti, ma genera anche vulnerabilità. Gli incidenti informatici sono infatti in forte aumento. La loro complessità, la frequenza con cui si verificano e l'entità del loro impatto - dall'accesso ai servizi essenziali ai processi democratici - sono destinati ad aumentare ulteriormente.

In tale contesto sono stati individuati i seguenti problemi, tra loro correlati:

- frammentazione delle politiche e degli approcci alla cibersicurezza negli Stati membri,
- dispersione delle risorse e degli approcci alla cibersicurezza delle istituzioni, delle agenzie e degli organismi dell'UE,
- insufficiente consapevolezza da parte di cittadini e imprese delle minacce informatiche e insufficiente informazione sulle caratteristiche relative alla sicurezza dei prodotti e servizi TIC che acquistano, associate alla crescente diffusione di molteplici sistemi di certificazione nazionali e settoriali.

Questi problemi incidono sulla ciberresilienza globale dell'UE e sul funzionamento efficace del mercato interno.

Quali sono gli obiettivi da conseguire?

Gli obiettivi strategici specifici che l'iniziativa intende conseguire sono i seguenti:

1. Rafforzare le capacità e la preparazione degli Stati membri e delle imprese, in particolare per quanto riguarda le infrastrutture critiche.
2. Migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE.
3. Potenziare le capacità a livello di UE per integrare l'azione degli Stati membri, in particolare in caso di crisi informatiche transfrontaliere.
4. Aumentare la consapevolezza di cittadini e imprese sulle questioni riguardanti la cibersicurezza.
5. Aumentare la trasparenza complessiva dell'affidabilità dei prodotti e servizi TIC in termini di cibersicurezza, al fine di rafforzare la fiducia nel mercato unico digitale e nell'innovazione digitale.
6. Evitare la frammentazione dei sistemi di certificazione nell'UE e dei relativi requisiti di sicurezza e criteri di valutazione nei vari Stati membri e settori.

Qual è il valore aggiunto di un'iniziativa a livello dell'UE?

Tenuto conto della portata globale della digitalizzazione e dell'interconnessione dell'economia e della società, i problemi hanno una dimensione transfrontaliera. Per questo motivo è necessario un intervento a livello di Unione. Osservando il contesto attuale e guardando al futuro, sembra che le singole azioni degli Stati membri e un approccio frammentario alla cibersicurezza, in particolare in considerazione della sua forte dimensione transfrontaliera, non consentano di aumentare la ciberresilienza collettiva dell'Unione.

B. SOLUZIONI

Quali sono le varie opzioni per conseguire gli obiettivi? È stata preferita un'opzione?

La presente valutazione d'impatto analizza una serie di opzioni strategiche che riguardano il riesame dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e la certificazione della sicurezza delle TIC.

Riesame dell'ENISA

Opzione 0 - Scenario di base - Questa opzione prevede il mantenimento della situazione attuale. Il mandato dell'ENISA sarebbe prorogato e gli obiettivi e i compiti dell'Agenzia resterebbero per lo più invariati, tenendo conto allo stesso tempo dei compiti affidati all'ENISA dalla legislazione successiva dell'UE (ad esempio la direttiva NIS).

Opzione 1 - Scadenza del mandato dell'ENISA (chiusura dell'ENISA). Questa opzione comporterebbe la chiusura dell'ENISA e la fine del suo mandato (nel giugno 2020) ed eventualmente una ridistribuzione delle competenze/attività a livello UE e/o nazionale.

Opzione 2 - "ENISA riformata". Questa opzione si baserebbe sull'attuale mandato dell'ENISA ma prevede l'adozione di modifiche puntuali che tengano conto dell'evoluzione del panorama della cibersicurezza. All'Agenzia sarebbe conferito un mandato permanente, basato sui seguenti elementi chiave: sostegno allo sviluppo e all'attuazione delle politiche dell'UE; rafforzamento delle capacità; conoscenze e informazioni; compiti connessi al mercato; ricerca e innovazione; cooperazione operativa e gestione delle crisi.

Opzione 3 - Agenzia dell'UE per la cibersicurezza dotata di piena capacità operativa. Questa opzione comporta la necessità di riformare l'ENISA attraverso il raggruppamento di tre funzioni principali: 1. funzione politica/consultiva; 2. centro di informazione e competenze; 3. squadra di pronto intervento informatico (CERT). In larga misura, questa opzione comporterebbe lo stesso cambiamento dell'opzione 2 per quanto riguarda il campo di applicazione del mandato. Tuttavia, l'Agenzia avrebbe compiti supplementari nell'ambito della risposta agli incidenti e della gestione delle crisi, coprendo così l'intero ciclo di vita della cibersicurezza e gestendo la prevenzione e l'individuazione degli incidenti informatici e la risposta agli stessi.

Certificazione

Opzione 0 - Scenario di base - Nessun provvedimento. Questa opzione prevede il mantenimento dello status quo e nessuna azione politica o legislativa.

Opzione 1 - **Misure non legislative**. Questa opzione prevede il ricorso a strumenti non vincolanti (ad esempio comunicazioni interpretative, sostegno a iniziative di autoregolamentazione a livello dell'UE e attività di normazione) al fine di migliorare la trasparenza e ridurre la frammentazione.

Opzione 2 - Un atto legislativo dell'UE per estendere l'accordo SOG-IS a tutti gli Stati membri. Questa opzione prevede la proposta da parte della Commissione di un atto legislativo per estendere l'accordo a tutti gli Stati membri.

Opzione 3 - Un quadro generale dell'UE per la certificazione della sicurezza delle TIC. Questa opzione prevede di istituire un quadro europeo per la certificazione della sicurezza delle TIC (compreso un gruppo di esperti composto da autorità nazionali) basandosi il più possibile sui sistemi esistenti di certificazione della sicurezza delle TIC. In sostanza, il quadro consentirebbe la creazione di sistemi di certificazione dell'UE accettati in tutti gli Stati membri.

L'opzione prescelta è una combinazione dell'opzione 2 per l'ENISA e dell'opzione 3 per la certificazione.

Quali sono le varie parti in causa? Chi sono i sostenitori delle varie opzioni?

La grande maggioranza dei portatori di interessi di tutte le categorie (Stati membri, industria, istituzioni dell'UE, comunità di ricerca) che hanno partecipato alla consultazione sembra essere favorevole all'opzione prescelta, in quanto appoggia il rafforzamento dell'ENISA e la creazione di un quadro europeo di certificazione della sicurezza delle TIC.

In particolare, vi è consenso sulla necessità di avere (come minimo) un'agenzia dell'UE ben funzionante con un mandato permanente, che sia dotata di risorse adeguate e incaricata di affrontare le attuali e future sfide in materia di cibersicurezza. Vi è inoltre un ampio consenso tra i portatori di interessi sulla creazione di un quadro europeo scalabile su base volontaria.

Per quanto riguarda il settore industriale, questa soluzione per la certificazione è appoggiata dalle imprese che sono già soggette a requisiti di certificazione e che trarrebbero vantaggio da un sistema a livello di UE basato sul riconoscimento reciproco dei certificati. Sono a favore di questa soluzione anche le PMI, che sarebbero i soggetti più colpiti se già devono o dovessero avviare processi di certificazione diversi nei vari Stati membri. Alcuni Stati membri, in particolare quelli che dispongono di minori risorse, e alcuni rappresentanti dell'industria e delle istituzioni dell'UE hanno espresso pareri positivi anche per quanto riguarda l'opzione 3 per l'ENISA.

C. IMPATTO DELL'OPZIONE PRESCELTA

Quali sono i vantaggi dell'opzione prescelta (se ne esiste una, altrimenti delle opzioni principali)?

L'opzione prescelta prevede che l'UE abbia un'agenzia, prevalentemente destinata a fornire sostegno agli Stati membri, alle istituzioni dell'UE e alle imprese negli ambiti in cui apporterebbe il valore aggiunto maggiore. Tali ambiti riguardano: sostegno all'attuazione della direttiva NIS; sviluppo e attuazione delle politiche, informazioni, conoscenze e sensibilizzazione; ricerca; cooperazione operativa e crisi; mercato. In particolare, l'ENISA dovrebbe sostenere la politica dell'UE in materia di certificazione della sicurezza delle TIC, garantendo la gestione amministrativa e tecnica di un quadro europeo di certificazione della sicurezza delle TIC. Un tale quadro darebbe effettiva attuazione a una serie di norme sulla governance della certificazione della sicurezza delle TIC nell'UE, il che consentirebbe di promuovere un sistema di reciproco riconoscimento dei certificati rilasciati in tutti gli Stati membri. La combinazione di queste opzioni è ritenuta la più efficace per l'UE ai fini del conseguimento degli obiettivi individuati: rafforzare le capacità di cibersicurezza; preparazione: cooperazione; sensibilizzazione; trasparenza; evitare la frammentazione del mercato. Questa opzione è anche la più coerente con le priorità politiche, in quanto si iscrive nella strategia per la cibersicurezza e le politiche correlate (ad esempio la direttiva NIS) e nella strategia per il mercato unico digitale. Inoltre, permetterebbe di conseguire gli obiettivi attraverso un impiego adeguato delle risorse.

Quali sono i costi dell'opzione prescelta (se ne esiste una, altrimenti delle opzioni principali)?

Nonostante l'assunzione di nuovi compiti, un'ENISA riformata continuerebbe ad essere un'organizzazione flessibile. Il contributo finanziario richiesto dal bilancio dell'UE sarebbe maggiore rispetto a quello attuale, ma ancora di molto inferiore a quello delle altre agenzie che operano in settori cruciali.

La creazione di un quadro europeo di certificazione della sicurezza delle TIC non comporterebbe ulteriori costi iniziali per il settore (comprese le PMI). Potrebbe generare al contrario notevoli risparmi per le imprese che già certificano i loro prodotti o sono disposte a effettuare la certificazione della sicurezza, con ricadute positive sulla loro competitività a livello mondiale. Dall'altro lato, comporterebbe alcuni impegni di bilancio per garantire il mantenimento del quadro, cui provvederebbe soprattutto il modello dell'ENISA riformata, per quanto riguarda l'assistenza tecnica e i compiti di segreteria.

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

No, i costi destinati al potenziamento dell'ENISA sarebbero in gran parte sostenuti dal bilancio dell'UE, mentre gli Stati membri potrebbero comunque fornire contributi finanziari volontari. Per quanto riguarda la certificazione, l'impatto principale sui bilanci e sulle amministrazioni nazionali deriverebbe dall'eventuale creazione di un'autorità di certificazione.

Sono previsti altri effetti significativi?

No.

Proporzionalità

L'opzione prescelta prevede misure equilibrate, tutte ritenute necessarie per conseguire gli obiettivi previsti senza imporre oneri eccessivi ai portatori d'interessi coinvolti. In quest'ottica, l'iniziativa è ritenuta conforme al principio di proporzionalità.

D. SEGUITO

Quando saranno riesaminate le misure proposte?

Si propone di effettuare la prima valutazione cinque anni dopo l'entrata in vigore del regolamento. Successivamente la Commissione riferirà al Parlamento europeo e al Consiglio in merito ai risultati della valutazione, corredata se del caso di una proposta di riesame. Le successive valutazioni avranno una periodicità di cinque anni.