Consiglio dell'Unione europea

Bruxelles, 16 settembre 2022
(OR. en)

12429/22
ADD 6

Fascicolo interistituzionale: 2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	15 settembre 2022
Destinatario:	Segretariato generale del Consiglio
n. doc. Comm.:	SWD(2022) 283 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO riguardante la legge sulla ciberresilienza che accompagna il documento proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

Si trasmette in allegato, per le delegazioni, il documento SWD(2022) 283 final.

All.: SWD(2022) 283 final

COMMISSIONE
EUROPEA

Bruxelles, 15.9.2022
SWD(2022) 283 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO

riguardante la legge sulla ciberresilienza

che accompagna il documento

proposta di regolamento del Parlamento europeo e del Consiglio

relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Scheda di sintesi (massimo 2 pagine)

Valutazione d'impatto relativa alla legge sulla ciberresilienza

A. Necessità di intervenire

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

I prodotti hardware e software sono spesso soggetti ad attacchi informatici andati a segno, e si stima che entro il 2021 il costo globale annuo della criminalità informatica ammonterà a 5 500 miliardi di EUR. Tali prodotti risentono di due problemi principali, che comportano ulteriori costi per gli utilizzatori e per la società: 1) un basso livello di cibersicurezza, testimoniato da vulnerabilità diffuse e dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per porvi rimedio e 2) un'insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori, che impediscono loro di scegliere prodotti con caratteristiche di cibersicurezza adeguate o di utilizzarli in modo sicuro.

La cibersicurezza dei prodotti con elementi digitali ha una forte dimensione transfrontaliera, poiché i prodotti fabbricati in un paese sono spesso utilizzati in tutto il mercato interno. Inoltre gli incidenti che inizialmente interessano un singolo soggetto o un singolo Stato membro spesso si diffondono in pochi minuti nell'intero mercato interno.

Sebbene la normativa vigente in materia di mercato interno si applichi ad alcuni prodotti con elementi digitali, la maggior parte dei prodotti hardware e software non è attualmente disciplinata da alcuna normativa dell'UE riguardante la loro cibersicurezza. In particolare l'attuale quadro giuridico dell'UE non affronta la questione della cibersicurezza del software non incorporato, anche se gli attacchi alla cibersicurezza prendono sempre più di mira le vulnerabilità di tali prodotti, causando costi sociali ed economici significativi. Esempi recenti sono lo spyware Pegasus, che ha sfruttato le vulnerabilità dei telefoni cellulari, o il worm ransomware WannaCry, che ha sfruttato una vulnerabilità di Windows, colpendo i computer di tutto il mondo.

Quali sono gli obiettivi da conseguire?

Sono stati individuati due obiettivi principali per garantire il corretto funzionamento del mercato interno: 1) creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità e che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto; e 2) creare le condizioni che consentano agli utilizzatori di tenere conto della cibersicurezza nella scelta e nell'utilizzo dei prodotti con elementi digitali. Sono stati definiti quattro obiettivi specifici: i) garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita; ii) garantire un quadro coerente in materia di cibersicurezza, facilitando la conformità per i fabbricanti di hardware e software; iii) migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e iv) consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

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

La forte natura transfrontaliera della cibersicurezza e i crescenti incidenti, con effetti di ricaduta a livello transfrontaliero e trasversalmente ai settori e ai prodotti, fanno sì che gli obiettivi non possano essere raggiunti efficacemente dai soli Stati membri. Data la natura globale dei mercati dei prodotti con elementi digitali, sul rispettivo territorio gli Stati membri si trovano ad affrontare gli stessi rischi per lo stesso prodotto con elementi digitali. Il formarsi di un quadro frammentario di norme nazionali potenzialmente

divergenti rischia inoltre di ostacolare la creazione di un mercato unico aperto e competitivo per i prodotti con elementi digitali. È quindi necessaria un'azione comune a livello dell'UE per aumentare il grado di fiducia degli utilizzatori e l'attrattiva dei prodotti con elementi digitali sul mercato dell'UE. Tale azione avrebbe anche benefici per il mercato interno, garantendo la certezza del diritto e creando condizioni di parità per i fabbricanti di prodotti con elementi digitali.

B. Soluzioni

Quali sono le varie opzioni per conseguire gli obiettivi? Ne è stata prescelta una? In caso contrario, perché?

Sono state analizzate quattro opzioni strategiche e le relative sotto-opzioni che vanno oltre lo status quo: 1) approccio non vincolante (*soft law*) e misure volontarie; 2) intervento normativo ad hoc specifico per prodotto per la cibersicurezza dei prodotti tangibili con elementi digitali e dei relativi software incorporati; 3) approccio misto comprendente norme obbligatorie orizzontali per la cibersicurezza dei prodotti tangibili con elementi digitali e dei relativi software incorporati e un approccio scaglionato per il software non incorporato con due sotto-opzioni per la valutazione della conformità; e 4) un intervento normativo orizzontale che introduce requisiti di cibersicurezza per un'ampia gamma di prodotti con elementi digitali, compreso il software non incorporato, con sotto-opzioni per l'ambito di applicazione e la valutazione della conformità.

Sulla base della valutazione dell'efficacia rispetto agli obiettivi specifici, dell'efficienza dei costi rispetto ai benefici e della coerenza, la valutazione d'impatto ha concluso che l'**opzione prescelta** è l'opzione 4, che riguarda tutti i prodotti con elementi digitali e prevede una valutazione obbligatoria da parte di terzi per i prodotti critici.

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

Alla richiesta di valutare l'efficacia degli interventi strategici, i partecipanti alla consultazione pubblica hanno concordato che l'opzione 4 sarebbe la misura più efficace (4,08 su una scala da 1 a 5). Tra questi figurano le organizzazioni di consumatori (5,00), i partecipanti che si identificano come utilizzatori (4,22), gli organismi notificati (4,17), le autorità di vigilanza del mercato (5,00) e i fabbricanti di prodotti con elementi digitali (3,85), compresi quelli di piccole e medie dimensioni (4,05).

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 benefici significativi ai vari portatori di interessi. Per le imprese, eviterebbe norme di sicurezza divergenti per i prodotti con elementi digitali, ridurrebbe i costi di conformità alla relativa normativa in materia di cibersicurezza e diminuirebbe il numero di incidenti informatici, i costi di gestione degli incidenti e i danni alla reputazione. Per l'intera UE si stima che l'iniziativa potrebbe comportare una riduzione dei costi degli incidenti che interessano le imprese di circa 180-290 miliardi di EUR all'anno. Inoltre l'iniziativa determinerebbe un aumento del fatturato grazie alla crescente diffusione dei prodotti con elementi digitali e migliorerebbe anche la reputazione delle imprese a livello mondiale, portando a un aumento della domanda da fuori l'UE. Per gli utilizzatori finali l'opzione prescelta aumenterebbe la trasparenza delle proprietà di sicurezza e faciliterebbe l'uso dei prodotti con elementi digitali. I consumatori e i cittadini beneficerebbero inoltre di una migliore tutela dei loro diritti fondamentali, come la protezione della vita privata e dei dati.

Quali sono i costi dell'opzione prescelta (o in mancanza di quest'ultima, delle opzioni principali)?
L'opzione prescelta genererebbe costi di conformità e di applicazione per le imprese, gli organismi notificati e le autorità pubbliche, comprese le autorità di notifica, di accreditamento e di vigilanza del mercato. Per gli sviluppatori di software e i fabbricanti di hardware aumenteranno i costi diretti di conformità per i nuovi requisiti di cibersicurezza, la valutazione della conformità, gli obblighi di documentazione e di segnalazione, che porteranno a costi aggregati di conformità pari a circa 29 miliardi di EUR per un valore di mercato stimato dei prodotti con elementi digitali fino a 1 485 miliardi di EUR di fatturato. Gli utilizzatori finali, compresi gli utilizzatori finali commerciali, i consumatori e i cittadini, possono incorrere in un aumento dei prezzi dei prodotti con elementi digitali. Tuttavia tale aumento dovrebbe essere considerato alla luce dei benefici significativi descritti in precedenza. Per gli organismi notificati i costi aggiuntivi dovrebbero essere compensati da un aumento del fatturato.
Quale sarà l'incidenza sulle PMI e sulla competitività?
Le PMI saranno interessate dai nuovi requisiti sia come fabbricanti sia come utilizzatori finali. In termini di costi di conformità le PMI sarebbero in linea di principio più colpite rispetto alle grandi imprese, che generalmente hanno migliori economie di scala e una maggiore consapevolezza in materia di cibersicurezza. Tuttavia le PMI trarrebbero grandi vantaggi dall'iniziativa, poiché la cibersicurezza incorporata nei prodotti con elementi digitali rappresenterebbe un significativo risparmio di costi per le PMI in quanto utilizzatori. Come fabbricanti le PMI beneficerebbero di una maggiore fiducia da parte degli utilizzatori finali e di nuovi clienti. Un accesso senza soluzioni di continuità al mercato interno e una riduzione della frammentazione del mercato possono essere ancora più vantaggiosi per le PMI, che sono meno attrezzate per gestire requisiti normativi differenti. Pur sottolineando la necessità di un approccio proporzionato e di misure di sostegno, le PMI si sono generalmente espresse a favore di condizioni di parità tra tutte le imprese e non hanno ritenuto di essere svantaggiate rispetto alle imprese più grandi in uno scenario di requisiti obbligatori orizzontali.
L'impatto sui bilanci e sulle amministrazioni nazionali sarà significativo?
L'iniziativa avrà un impatto sulle autorità nazionali, come le autorità di notifica, le autorità di accreditamento e le autorità di vigilanza del mercato, che hanno la responsabilità di monitorare e applicare le misure proposte. Tali autorità sosterranno costi aggiuntivi di adeguamento (ad esempio formazione e risorse umane) e di applicazione per tenere conto dei nuovi requisiti. Le risorse impiegate dagli organismi di accreditamento sono tuttavia compensate e sostenute in gran parte dagli organismi di valutazione della conformità mediante l'acquisto di servizi di accreditamento.
Sono previsti altri impatti significativi?
Non sono previsti altri impatti negativi significativi. L'opzione strategica prescelta contribuirebbe a ridurre il numero e la gravità degli incidenti, comprese le violazioni dei dati personali, e avrebbe un impatto sociale positivo, ad esempio in termini di riduzione della criminalità informatica. È probabile che aumenti la domanda di professionisti della sicurezza e si ridurrebbero 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'intervento garantirebbe che i prodotti con elementi digitali siano protetti durante l'intero ciclo di vita e in modo proporzionale ai rischi affrontati.

D. Tappe successive
Quando saranno riesaminate le misure proposte?
Entro [36 mesi] dalla data di applicazione dell'iniziativa e successivamente ogni quattro anni la Commissione trasmette al Parlamento europeo e al Consiglio una relazione sulla valutazione e sul riesame dell'iniziativa.