COMMISSIONE
EUROPEA

Bruxelles, 7.2.2013
SWD(2013) 31 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di direttiva del Parlamento europeo e del Consiglio

recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione

{COM(2013) 48 final}
{SWD(2013) 32 final}

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di direttiva del Parlamento europeo e del Consiglio

recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione

1. CAMPO DI APPLICAZIONE

La presente valutazione dell'impatto analizza le opzioni strategiche che permettono di migliorare la sicurezza di internet e di altre reti e sistemi informativi su cui si basano servizi fondamentali per il funzionamento della nostra società (come amministrazioni pubbliche, finanza e banche, energia, trasporti, sanità e alcuni servizi internet che rendono possibili processi economici e societali fondamentali come le piattaforme del commercio elettronico e le reti sociali). Tutto questo va sotto il nome di Sicurezza delle reti e dell'informazione (SRI).

2. CONTESTO POLITICO

La Commissione ha riconosciuto la crescente importanza della sicurezza delle reti e dell'informazione per le nostre società e le nostre economie per la prima volta nel 2001. Nel 2004 la Comunità europea ha deciso di istituire l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) allo scopo garantire un livello elevato ed efficace di sicurezza delle reti e dell'informazione nell'Unione. L'approccio finora seguito dall'Unione europea in questo settore è consistito soprattutto nell'adozione di una serie di piani di azione e di strategie per indurre gli Stati membri a dotarsi di mezzi più adeguati per far fronte alla sicurezza delle reti e dell'informazione e a collaborare per contrastare i problemi transnazionali in questo campo.

I soggetti interessati sono stati consultati sui vari aspetti dell'iniziativa (definizione del problema e possibilità di ovviare alle lacune esistenti) attraverso:

- una **consultazione pubblica online** sul tema "Migliorare la sicurezza delle reti e dell'informazione nell'UE" svoltasi dal 23 luglio al 15 ottobre 2012. La Commissione ha ricevuto 169 risposte via internet e 10 risposte per iscritto;
- discussioni con gli **Stati membri** nell'ambito del forum europeo degli Stati membri (EFMS), in riunioni bilaterali e in occasione della conferenza dell'UE sulla cibersicurezza organizzata il 6 luglio 2012 dalla Commissione e dal Servizio europeo per l'azione esterna;
- discussioni con imprese e associazioni del **settore privato** nell'ambito del partenariato europeo pubblico-privato per la resilienza (EP3R) e nel corso di riunioni bilaterali;
- discussioni con **l'ENISA e la squadra di pronto intervento informatico CERT-UE**;
- discussioni nell'ambito dell'**Assemblea dell'Agenda digitale del 2012.**

3. DESCRIZIONE DEL PROBLEMA

3.1. Definizione del problema

Il problema può essere descritto come un ***livello insufficiente di protezione contro gli incidenti, i rischi e le minacce per la sicurezza delle reti e dell'informazione nell'UE che compromettono il corretto funzionamento del mercato interno.***

Poiché le reti e i sistemi informativi sono interconnessi e data la dimensione planetaria di internet, molti incidenti SRI travalicano i confini nazionali e minano il funzionamento del mercato interno.

Le violazioni di sicurezza, come nel caso di attacchi contro eBay e PayPal, possono rendere indisponibili, sospendere o interrompere servizi transnazionali. La necessità di agire rapidamente per rimediare ai problemi e trasmettersi le informazioni in caso di incidente significativo è stata evidenziata in occasione degli attacchi contro la compagnia olandese di certificazione internet Diginotar. In seguito agli incidenti verificatisi in passato gli Stati membri cominciano a adottare regolamentazione proprie, ma il mancato coordinamento degli interventi regolamentari può dar luogo a frammentazione e a barriere nel mercato interno e creare costi di messa in conformità per le imprese che operano in più di uno Stato membro.

Questo problema colpisce tutti i settori della società e dell'economia (amministrazioni, imprese e consumatori). Vi sono in particolare settori che svolgono un ruolo essenziale nel fornire servizi fondamentali di supporto per la nostra economia e la nostra società e la sicurezza dei loro sistemi riveste un'importanza particolare ai fini del funzionamento del mercato interno. Si tratta di settori come le banche, le borse, la generazione la trasmissione e la distribuzione di energia, i trasporti (aerei, ferroviari e marittimi), la sanità, i facilitatori di servizi internet e le amministrazioni pubbliche. La consultazione pubblica ha evidenziato che le parti interessate sono risolutamente a favore del progetto di affrontare i problemi di sicurezza delle reti e dell'informazione in questi settori e di un'azione a livello europeo al riguardo.

In mancanza di ulteriori misure per contrastare il numero crescente di incidenti, la fiducia dei consumatori nei servizi online rischia di risentirne il che può compromettere il conseguimento degli obiettivi dell'Agenda digitale.

3.2. Fattori determinanti del problema

Il problema definito deriva da una serie di fattori.

Innanzitutto gli **Stati membri dell'UE dispongono di capacità disuguali**, il che ostacola la creazione di quel clima di fiducia tra pari indispensabile per la collaborazione e lo scambio di informazioni.

In secondo luogo, lo **scambio di informazioni sugli incidenti, i rischi e le minacce è insufficiente**. La maggior parte degli incidenti non è segnalata e passa inosservata perché le imprese sono restie a condividere questo tipo di informazioni per paura di subire danni in termini di immagine o di responsabilità. Lo scambio di informazioni sulle attuali piattaforme o partenariati pubblico-privati, come EFMS e EP3R, si limita alle buone pratiche.

4. EFFICACIA DELLE MISURE ESISTENTI

4.1. Lacune del quadro regolamentare in vigore

Le norme attuali fanno obbligo soltanto alle compagnie di telecomunicazione di adottare misure di gestione del rischio di incidenti di sicurezza delle reti e dell'informazione e di segnalare questo tipo di incidenti, anche se a correre rischi di sicurezza sono tutti gli attori la

cui attività dipende dalle reti e dai sistemi informativi. Ne conseguono disparità di trattamento poiché, per lo stesso incidente che ad es. colpisca un fornitore di telecomunicazioni e una società fornitrice di servizi telefonici su protocollo internet (IP), l'obbligo di segnalazione alle competenti autorità nazionali vige soltanto per il primo e non per la seconda.

Il quadro regolamentare in materia di protezione dei dati fa obbligo a tutti gli attori con funzione di responsabili del trattamento dei dati (ad esempio una banca o un ospedale) di instaurare misure di sicurezza proporzionate ai rischi incorsi, ma i responsabili del trattamento dei dati sono tenuti a segnalare soltanto le violazioni di sicurezza che compromettono dati personali.

La direttiva 2008/114/CE del Consiglio, relativa all'individuazione e alla designazione delle infrastrutture critiche europee, contempla solo i settori dell'energia e dei trasporti e a tutt'oggi gli Stati membri hanno individuato solo poche infrastrutture critiche europee. La direttiva non obbliga gli operatori a segnalare importanti violazioni di sicurezza e non istituisce alcun meccanismo attraverso il quale gli Stati membri possono collaborare o reagire agli incidenti.

I colegislatori stanno attualmente discutendo una proposta di direttiva della Commissione relativa agli attacchi contro i sistemi di informazione[1], che copre solo la punibilità di comportamenti specifici, ma non riguarda la prevenzione di rischi e incidenti di sicurezza delle reti e dell'informazione e l'attenuazione delle loro conseguenze.

4.2. I limiti di un approccio facoltativo

L'approccio di tipo facoltativo finora seguito ha dato luogo a un livello disuguale di preparazione e ad una cooperazione limitata.

L'EFMS ha un mandato limitato poiché gli Stati membri non si scambiano informazioni su incidenti, rischi e minacce, né collaborano per contrastare minacce transnazionali, per cui tale organo non può chiedere ai suoi membri di dotarsi di capacità minime.

L'ENISA non ha poteri operativi e, per es., non può intervenire per rimediare a problemi di sicurezza delle reti e dell'informazione.

Il partenariato europeo EP3R non ha uno statuto ufficiale e non può obbligare il settore privato a segnalare incidenti alle autorità nazionali. Al suo interno non esiste un quadro per lo scambio sicuro di informazioni e la comunicazione di informazioni su minacce, rischi e incidenti a carico della sicurezza delle reti e dell'informazione.

5. NECESSITÀ DELL'INTERVENTO DELL'UE, SUSSIDIARIETÀ E PROPORZIONALITÀ

Garantire la sicurezza delle reti e dell'informazione è vitale per il corretto funzionamento del mercato interno e il benessere della nostra società. L'articolo 114 del TFUE costituisce una base giuridica adeguata per armonizzare le disposizioni in materia di SRI e introdurre un livello minimo di sicurezza comune in tutta l'Unione europea.

L'intervento dell'Unione nel settore della sicurezza delle reti e dell'informazione è giustificato in termini di **sussidiarietà** dalla dimensione transnazionale del problema e dall'accresciuta efficacia (e quindi dal valore aggiunto) che tale intervento conferirebbe alle politiche nazionali attuali.

Per garantire che la collaborazione coinvolga tutti gli Stati membri è necessario che tutti loro dispongano del livello minimo di capacità necessario. Inoltre è chiaro che interventi concertati di tipo collaborativo in materia di sicurezza delle reti e dell'informazione possono avere un

[1] COM(2010) 517, **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:IT:PDF**

impatto molto benefico sulla tutela effettiva dei diritti fondamentali, in particolare il diritto alla protezione dei dati personali e della vita privata.

Le misure previste dall'opzione preferita sono giustificate per motivi di **proporzionalità** poiché le condizioni imposte agli Stati membri corrispondono a quanto è strettamente necessario per raggiungere un livello adeguato di preparazione e permettere una collaborazione basata sulla fiducia, mentre gli obblighi in materia di gestione dei rischi e di segnalazione degli incidenti imposti alle imprese e alle pubbliche autorità riguardano soltanto le entità critiche, comportano misure proporzionate al rischio e interessano gli incidenti con un impatto significativo. Inoltre, le misure previste dall'opzione preferita non comportano costi sproporzionati.

6. OBIETTIVI

L'obiettivo generale è aumentare il livello di protezione contro incidenti, rischi e minacce a carico della sicurezza delle reti e dell'informazione nell'UE. Gli obiettivi specifici sono i seguenti:

- **Obiettivo 1**: istituire un livello comune minimo di sicurezza delle reti e dell'informazione negli Stati membri aumentando così il livello generale di preparazione e risposta;
- **Obiettivo 2**: migliorare la collaborazione a livello dell'Unione in materia di sicurezza delle reti e dell'informazione per lottare efficacemente contro le minacce e gli incidenti transfrontalieri;
- **Obiettivo 3**: creare una cultura di gestione del rischio e migliorare lo scambio di informazioni tra i settori pubblico e privato.

7. OPZIONI STRATEGICHE

Le opzioni strategiche prese in considerazione dalla presente valutazione dell'impatto sono le seguenti: status quo, approccio regolamentare e approccio misto. È stata invece scartata l'opzione che prevede la cessazione di qualsiasi attività dell'UE in questo campo.

7.1. Opzione 1 - Status quo (scenario di riferimento)

La Commissione continuerebbe, con l'aiuto dell'ENISA, a seguire l'attuale approccio facoltativo invitando gli Stati membri a mettere a disposizione capacità nazionali a favore della sicurezza delle reti e dell'informazione (ad esempio squadre CERT, piani nazionali di emergenza in caso di incidenti informatici e strategie nazionali di cibersicurezza) e a collaborare al livello dell'UE (ad esempio attraverso una rete di squadre CERT in Europa e un piano europeo di emergenza/cooperazione in caso di incidente informatico).

7.2. Opzione 2 - Approccio regolamentare

La Commissione chiederebbe a tutti gli Stati membri di istituire almeno un livello minimo di capacità nazionali (squadre CERT, autorità competenti, piani nazionali di emergenza in caso di incidente informatico, strategie nazionali di cibersicurezza).

In base a questa opzione, le autorità nazionali competenti e le squadre CERT farebbero parte di una **rete** di collaborazione a livello UE. Attraverso la rete le autorità e le squadre CERT scambierebbero informazioni e collaborerebbero per contrastare le minacce e gli incidenti a carico della sicurezza delle reti e dell'informazione in base ad un **piano europeo di emergenza/collaborazione in caso di incidente cibernetico,** approvato dagli Stati membri.

Le imprese (diverse dalle microimprese) in settori critici specifici, come banche, energia (elettricità e gas naturale), trasporti, sanità, facilitatori di servizi internet fondamentali e

amministrazioni pubbliche, sarebbero tenute a valutare i rischi che corrono e ad adottare misure adeguate e proporzionate alle dimensioni dei rischi effettivi. Questi soggetti sarebbero inoltre tenuti a segnalare alle autorità competenti gli incidenti suscettibili di compromettere gravemente il funzionamento delle loro reti e dei loro sistemi informativi e aventi quindi un impatto significativo sulla continuità dei servizi e sulla fornitura di beni che dipendono da tali reti e sistemi informativi. Questo schema si riferisce a quello previsto dagli articoli 13 *bis* e 13 *ter* della direttiva quadro per quanto riguarda le comunicazioni elettroniche.

7.3. Opzione 3 - Approccio misto

La Commissione combinerebbe iniziative facoltative basate sulla buona volontà degli Stati membri, volte a creare o rafforzare capacità in materia di sicurezza delle reti e dell'informazione e a istituire meccanismi di collaborazione a livello dell'UE, con disposizioni regolamentari per i principali attori privati e le amministrazioni pubbliche.

Le iniziative facoltative sarebbero sostanzialmente analoghe a quelle previste dall'opzione 1, mentre le disposizioni regolamentari sarebbero identiche a quelle previste dall'opzione 2 sia per quanto riguarda i soggetti a cui si applicherebbero che la sostanza degli obblighi imposti.

L'ENISA fornirebbe supporto e assistenza tecnica alla Commissione, agli Stati membri e al settore privato, ad esempio attraverso orientamenti tecnici e raccomandazioni.

8. ANALISI DEGLI IMPATTI

L'analisi copre, oltre al livello di sicurezza, gli impatti socioeconomici delle tre opzioni considerate e i costi che dovrebbero essere sostenuti nell'ambito delle opzioni 2 e 3.

Nessuna delle opzioni di cui sopra avrà un impatto ambientale che possa essere previsto con precisione.

8.1. Opzione 1 - Status quo (scenario di riferimento)

Livello di sicurezza: È poco probabile che tutti gli Stati membri raggiungano livelli nazionali comparabili in termini di capacità e preparazione necessaria per migliorare la sicurezza e rendere possibile la cooperazione e lo scambio sicuro di informazioni nell'UE. Né si raggiungerebbe un livello equivalente per quanto riguarda le norme in materia di gestione del rischio e di trasparenza sugli incidenti e, a livello di regolamentazione, continuerebbero a esistere le lacune attuali.

Impatti economici: L'impatto dipenderebbe dalla misura in cui gli Stati membri seguono le raccomandazioni della Commissione. L'insufficiente livello di sicurezza degli Stati membri meno avanzati ne comprometterebbe la competitività e la crescita e li esporrebbe a rischi e incidenti. Stanti le tendenze attuali, gli incidenti a carico della sicurezza delle reti e dell'informazione si farebbero sempre più evidenti per le imprese e i consumatori ostacolando il completamento del mercato interno.

Impatti sociali: Il proseguimento e il previsto aggravamento di incidenti, rischi e minacce si ripercuoterebbe negativamente sulla fiducia del pubblico nei servizi in linea.

8.2. Opzione 2 - Approccio regolamentare

Livello di sicurezza. Gli obblighi loro imposti garantirebbero un'adeguata preparazione di tutti gli Stati membri e contribuirebbero a creare quel clima di fiducia reciproca che costituisce un prerequisito per l'effettiva collaborazione a livello dell'UE.

L'imposizione alle amministrazioni pubbliche e ai principali operatori privati dell'obbligo di gestione dei rischi in materia di sicurezza delle reti e dell'informazione costituirebbe un forte incentivo alla gestione efficace e al contenimento dei rischi di sicurezza. Il costo aggiuntivo

complessivo, livello dell'UE, a carico di tutti i settori indistintamente per soddisfare queste condizioni sarebbe compreso **tra 1 e 2 miliardi EUR**. Il costo di messa in conformità **per piccola e media impresa** sarebbe compreso tra **2 500 e 5 000 EUR.**

Impatto economico: Un livello di sicurezza più elevato permetterebbe di ridurre le perdite finanziarie connesse a rischi e incidenti SRI. Si rafforzerebbe la fiducia dei consumatori e delle imprese nel mondo digitale, a tutto vantaggio del mercato interno. La diffusione di una cultura di gestione del rischio permetterebbe anche di stimolare la domanda di prodotti e soluzioni TIC sicuri.

Impatto sociale: Un più elevato livello di sicurezza accrescerebbe la fiducia dei cittadini nell'ambiente in linea e permetterebbe loro di trarre i massimi vantaggi dal mondo digitale (ad es. media sociali, apprendimento in linea, sanità in linea).

8.3. Opzione 3 - Approccio misto

Livello di sicurezza: Come per l'opzione 1, le iniziative facoltative non offrono nessuna garanzia di miglioramento del livello di sicurezza in termini di capacità nazionali in materia di SRI o di collaborazione a livello UE. D'altro canto, l'imposizione di obblighi di sicurezza alle amministrazioni pubbliche e ai principali operatori privati costituirebbe un forte incentivo alla gestione e al contenimento dei rischi di sicurezza. Questi meccanismi non avrebbero tuttavia alcuna efficacia negli Stati membri che non seguono le raccomandazioni della Commissione per la creazione di capacità a favore della sicurezza delle reti e dell'informazione.

Impatti economici: Il ritmo di sviluppo sarebbe molto diseguale tra Stati membri. L'insufficiente livello di sicurezza degli Stati membri meno avanzati ne comprometterebbe la competitività e la crescita e li esporrebbe agli impatti negativi di rischi e incidenti.

Impatti sociali: Il proseguimento e il previsto aggravamento di incidenti, rischi e minacce si ripercuoterebbe negativamente sulla fiducia del pubblico nei servizi in linea, soprattutto negli Stati membri che non considerano prioritaria la sicurezza delle reti e dell'informazione.

9. LE OPZIONI A CONFRONTO

Le opzioni 1 e 3 non si considerano adeguate per il raggiungimento degli obiettivi strategici e pertanto non sono raccomandate: la loro efficacia dipende infatti dai risultati incerti di un approccio facoltativo in termini di raggiungimento di un livello minimo di sicurezza delle reti e dell'informazione e, per quanto riguarda l'opzione 3, dalla buona volontà degli Stati membri di creare capacità e di collaborare con gli altri Stati.

L'opzione preferita è l'opzione 2 perché garantisce un notevole miglioramento della protezione dei consumatori, delle imprese e delle amministrazioni dell'UE contro incidenti, minacce e rischi per la sicurezza delle reti e dell'informazione. Inoltre, mettendo ordine al suo interno, l'Unione potrebbe imporsi a livello internazionale e diventare una partner ancora più credibile per la collaborazione a livello bilaterale e multilaterale. In più, potrebbe promuovere con più forza i diritti e i valori fondamentali dell'UE al suo esterno.

10. MONITORAGGIO E VALUTAZIONE

Il capitolo 10 della valutazione di impatto contiene una serie di indicatori principali di avanzamento verso il raggiungimento degli obiettivi, tra cui ad esempio:

- per l'obiettivo 1, il numero di Stati membri che hanno designato un'autorità competente in materia di sicurezza delle reti e dell'informazione e una squadra CERT, o che hanno adottato una strategia nazionale in materia di cibersicurezza e un piano nazionale di emergenza/cooperazione in caso di ciberincidente;

- per l’obiettivo 2, il numero di autorità competenti degli Stati membri e di squadre CERT che partecipano alla rete e il volume di informazioni scambiate attraverso la rete sui rischi e gli incidenti SRI;
- per l’obiettivo 3, il livello di investimenti nella sicurezza delle reti e dell’informazione effettuati dai principali attori privati e dalle amministrazioni pubbliche e il numero di segnalazioni di incidenti SRI aventi un impatto significativo.