COMMISSIONE EUROPEA

Bruxelles, 30.9.2010
SEC(2010) 1123 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA VALUTAZIONE D'IMPATTO

documento di accompagnamento della

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/Gai del Consiglio

COM(2010) 517 final
SEC(2010) 1122 final

SINTESI DELLA VALUTAZIONE D'IMPATTO

1. DEFINIZIONE DEL PROBLEMA

Il numero di attacchi contro i sistemi di informazione è considerevolmente aumentato dall'adozione della decisione quadro relativa agli attacchi contro i sistemi di informazione (in appresso: "DQ"). Una delle principali società specializzate nel settore della sicurezza di Internet ha indicato che le minacce rivolte contro le informazioni riservate (in contrapposizione a quelle pubblicamente disponibili) sono significativamente aumentate nel 2008: in quell'anno sono state individuate difatti 1 656 227 nuove minacce, rispetto alle 624 267 osservate precedentemente.[1] Si è inoltre assistito a una serie di pericolosi attacchi su larga scala prima sconosciuti, come quelli in Estonia e Lituania rispettivamente nel 2007 e 2008. Nel marzo 2009, i sistemi informatici di organismi governativi e privati di 103 paesi sono stati attaccati da una rete di computer compromessi che hanno estratto documenti sensibili e riservati[2]: ciò è accaduto attraverso le "botnet"[3], ossia reti di computer infettati che possono essere controllati a distanza. Si assiste infine, attualmente, al dilagare della botnet chiamata "Conficker" (nota anche come Downup, Downadup e Kido), che dal novembre 2008 si è propagata e manifestata su scala e dimensioni senza precedenti, colpendo milioni di computer in tutto il mondo.[4]

Va in secondo luogo osservato che l'insufficiente cooperazione fra gli Stati membri, e in particolare fra gli organi di contrasto e le autorità giudiziarie nell'UE, rende difficile una risposta coordinata ed efficiente a questi attacchi. Benché secondo la relazione sull'attuazione della DQ la maggioranza degli Stati membri abbia predisposto punti di contatto permanenti come richiesto dall'articolo 11 della stessa DQ, persistono problemi quanto alla loro capacità di risposta e di reazione a urgenti richieste di cooperazione.[5]

L'esistenza di un punto di contatto non è una garanzia di buon funzionamento. Nelle comunicazioni trasmesse alla Commissione, una serie di Stati membri ha indicato di avere effettivamente istituito tali punti di contatto, ma che questi non erano operativi 24 ore al giorno come richiesto dalla DQ. Ciò significa che tali punti di contatto non possono rispondere a richieste urgenti al di fuori delle ore d'ufficio. La scarsa efficienza dei punti di contatto o la loro incapacità di soddisfare le richieste di cooperazione del settore privato sono spesso d'ostacolo alla collaborazione fra questo settore e quello pubblico.

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, pag.10.

2 ww.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 Col termine "botnet" si intende una rete di computer infettati da software maligni (virus informatici). Una tale rete di computer compromessi ("zombie") può essere attivata per eseguire azioni specifiche, ad esempio attacchi ai sistemi d'informazione (attacchi informatici). Questi "zombie" possono essere controllati – spesso ad insaputa dei loro utilizzatori – da un altro computer, noto anche come "centro di comando e di controllo". Le persone che controllano questo centro sono da annoverarsi fra gli autori dell'infrazione, poiché usano i computer compromessi per lanciare attacchi contro i sistemi di informazione. Rintracciare gli autori dell'infrazione è molto difficile, poiché i computer che fanno parte della botnet e che effettuano gli attacchi possono trovarsi in un luogo diverso da quello in cui è localizzato l'autore dell'infrazione.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Relazione della Commissione al Consiglio ai sensi dell'articolo 12 della decisione quadro del Consiglio del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione, COM (2008) 448 definitivo.

In terzo luogo, sono ancora scarsi i dati disponibili sugli attacchi informatici e sul seguito datone dalla polizia e dalle autorità giudiziarie. Non tutti gli Stati membri raccolgono i dati sugli attacchi informatici, e quelli che lo fanno applicano metodi statistici divergenti che non consentono confronti.

Le vittime degli attacchi su larga scala contro i sistemi di informazione sono i cittadini in generale in quanto utilizzatori dei sistemi, così come le amministrazioni centrali e locali, le organizzazioni internazionali e il settore privato.

Gli attacchi contro bersagli situati nell'UE possono infine essere lanciati anche da paesi terzi, e viceversa.

2. SUSSIDIARIETÀ

La criminalità informatica è un vero e proprio problema internazionale che raramente può essere contrastato in un contesto puramente nazionale, e tutti convengono sulla necessità di azioni a livello UE ed internazionale per prevenirlo e affrontarlo. La maggior parte degli attacchi hanno dimensione transfrontaliera, colpiscono tutti gli Stati membri ed è chiaro che molti di essi investono attività che coinvolgono più paesi. I sistemi di informazione sono spesso tecnicamente interconnessi e interdipendenti fra uno Stato e l'altro. Gli esperti sono quindi concordi nell'affermare che sono necessarie azioni sia internazionali che a livello UE, e che l'obiettivo di combattere efficacemente questa forma di criminalità non può essere realizzato in maniera sufficiente dagli Stati membri.

Un approccio nazionale di lotta contro la criminalità informatica rischia di portare a una frammentazione e di essere inefficace a livello europeo. Le differenze fra i sistemi nazionali e la mancanza di una cooperazione transfrontaliera sistematica riducono sensibilmente l'efficacia delle contromisure nazionali, e ciò è in parte dovuto all'interconnessione dei sistemi di informazione: un basso livello di sicurezza in un paese può aumentare la vulnerabilità degli altri.

3. OBIETTIVI

3.1 Obiettivi generali, specifici e operativi

Scopo generale dell'azione dell'UE è combattere e perseguire la criminalità, organizzata o di altro tipo, conformemente all'articolo 67 del trattato sul funzionamento dell'Unione europea, lottando contro gli attacchi su larga scala ai sistemi di informazione.

A **Obiettivo specifico: Perseguire e condannare gli autori di attacchi su larga scala, grazie al ravvicinamento della legislazione penale nel settore degli attacchi contro i sistemi di informazione**

B **Obiettivo specifico: Migliorare la cooperazione transfrontaliera fra gli organi di contrasto**

C **Obiettivo specifico: Introdurre efficaci sistemi di monitoraggio e di raccolta di dati**

4. OPZIONI

4.1 Opzione (1): Status Quo / Nessuna nuova azione dell'UE

Questa opzione implica che l'UE non prenda alcuna iniziativa supplementare per contrastare questo particolare tipo di criminalità informatica, e che siano portate avanti le azioni in corso, in particolare i programmi per il rafforzamento della protezione delle infrastrutture critiche informatizzate e per il miglioramento della cooperazione fra il settore pubblico e quello privato contro la criminalità informatica.

4.2 Opzione (2): Elaborazione di un programma per intensificare l'impegno a contrastare gli attacchi contro i sistemi di informazione per mezzo di misure non legislative

Parallelamente al programma di protezione delle infrastrutture critiche informatizzate, le misure non legislative si concentrerebbero sulle attività di contrasto transfrontaliere e sulla cooperazione pubblico-privato, e sosterrebbero un'azione coordinata a livello UE. Una proposta non legislativa potrebbe includere azioni quali il rafforzamento dell'esistente rete 24/7 dei punti di contatto delle autorità di contrasto, la creazione di una rete UE di punti di contatto pubblico-privati fra esperti in materia di criminalità informatica e organi di contrasto, e l'elaborazione di un accordo standard UE sul livello dei servizi per la cooperazione nelle attività di contrasto con gli operatori del settore privato.

4.3 Opzione (3): Aggiornamento mirato della DQ per affrontare la specifica minaccia degli attacchi su larga scala contro i sistemi di informazione

Questa opzione prevede l'introduzione di specifiche norme mirate (ossia circoscritte) per lottare contro gli attacchi su larga scala, particolarmente pericolosi, a danno dei sistemi di informazione. Tale legislazione mirata sarebbe associata a misure destinate a rafforzare la cooperazione operativa transfrontaliera contro gli attacchi ai sistemi di informazione e ad aumentare le sanzioni minime già previste. Questa opzione rivestirebbe la forma di un aggiornamento dell'esistente DQ, completandola con una serie di misure non legislative, come il miglioramento della preparazione, sicurezza e resilienza delle infrastrutture critiche informatizzate, il rafforzamento degli strumenti e delle procedure per la cooperazione transfrontaliera fra le autorità di contrasto e lo scambio delle migliori prassi.

4.4 Opzione (4): Introduzione di una legislazione UE generale contro la criminalità informatica

La constatazione della necessità di intervenire rapidamente contro lo sviluppo di attacchi sofisticati contro i sistemi di informazione porta a chiedersi se sarebbe opportuno introdurre anche una legislazione più ampia sulla criminalità informatica in generale. Una tale legislazione riguarderebbe non solo gli attacchi contro i sistemi di informazione, ma anche questioni come la criminalità informatica finanziaria, i contenuti illegali del web, la raccolta/conservazione/trasferimento di prove elettroniche, e norme più dettagliate sulla competenza giurisdizionale. Essa sarebbe applicabile parallelamente alla Convenzione del Consiglio d'Europa sulla criminalità informatica, che verrebbe completata da nuove disposizioni considerate necessarie nell'UE.

4.5 Opzione (5): Aggiornamento della Convenzione del Consiglio d'Europa sulla criminalità informatica

Questa opzione richiederebbe una sostanziale rinegoziazione dell'attuale Convenzione, processo lungo e incompatibile con la tabella di marcia proposta nella valutazione d'impatto. Non vi sembra essere del resto alcuna volontà internazionale di rinegoziare la Convenzione, il cui aggiornamento non può quindi essere considerato un'opzione percorribile, poiché andrebbe oltre il termine d'azione previsto.

5. VALUTAZIONE D'IMPATTO

Opzioni	Ripercussioni economiche	Ripercussioni sociali	Ripercussioni sui diritti fondamentali	Ripercussioni sui paesi terzi	Pertinenza per gli obiettivi A,B,C	Coerenza col diritto internazionale
Opzione 1: Status Quo / Nessuna nuova azione dell'UE	0	0	0	-	0	0
Opzione 2: Elaborazione di un programma per intensificare l'impegno a contrastare gli attacchi contro i sistemi di informazione per mezzo di misure non legislative	-/+	++	-/+	++	A + B ++ C +	-/+
Opzione 3: Aggiornamento mirato della DQ per affrontare la minaccia degli attacchi su larga scala contro i sistemi di informazione	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++

Opzione 4: Introduzione di una legislazione UE generale contro la criminalità informatica	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Opzione privilegiata (opzioni 2 e 3): Combinazione di misure non legislative con un aggiornamento mirato della DQ	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. CONFRONTO FRA LE VARIE OPZIONI

6.1 Opzione (1): Status Quo

Questa opzione renderà inevitabilmente più vulnerabile la posizione degli operatori privati, degli Stati membri e dell'Unione nella lotta contro la criminalità informatica, data la natura e l'evoluzione di quest'ultima. Anche mantenendo il livello delle azioni attualmente in corso, sarebbe comunque necessario un coordinamento a livello europeo.

6.2 Opzione (2): Elaborazione di un programma per intensificare l'impegno a contrastare gli attacchi contro i sistemi di informazione per mezzo di misure non legislative

Questa opzione presenta tutti i vantaggi e gli svantaggi di uno strumento non vincolante. L'aspetto positivo è la possibilità di definire ogni opzione in un modo coerente con le migliori prassi nazionali, facilitando così l'individuazione delle misure più efficaci.

Questa opzione è tuttavia meno efficace dal punto di vista del conseguimento degli obiettivi.

6.3 Opzione (3): Aggiornamento mirato della DQ per affrontare la minaccia degli attacchi su larga scala contro i sistemi di informazione

L'opzione in questione offre una risposta tempestiva e mirata ai problemi individuati. Affronta le questioni di diritto penale da prendere in considerazione per perseguire efficacemente gli autori dei reati. Migliora inoltre la cooperazione internazionale introducendo un meccanismo di assistenza internazionale immediata in caso di richieste urgenti di cooperazione, e promuove la collaborazione col settore privato grazie a misure di accompagnamento, ad esempio riunioni di esperti. Questa opzione introduce altresì una serie di circostanze aggravanti, come la dimensione su larga scala degli attacchi e gli attacchi commessi celando la reale identità dell'autore e danneggiando il legittimo proprietario dell'identità.

Infine, per misurare l'entità del problema, sono introdotti obblighi di monitoraggio.

6.4 Opzione (4): Introduzione di una legislazione UE generale contro la criminalità informatica

Come la n. 3, anche questa opzione ha il valore aggiunto di stabilire disposizioni vincolanti, portando quindi a un maggiore livello di efficacia se pienamente attuata. Essa massimizzerebbe inoltre l'impatto positivo degli strumenti sia legislativi che non legislativi non solo per quanto riguarda gli attacchi su larga scala, ma anche per tutta una serie di questioni legate alla criminalità informatica. Affronterebbe inoltre il quadro giuridico penale e al tempo stesso migliorerebbe la cooperazione transfrontaliera fra gli organi di contrasto. Questo approccio globale, tuttavia, non riscuote attualmente il consenso delle parti interessate, anche se la sua attuazione gioverebbe più di tutte le altre opzioni alla lotta contro la criminalità informatica.

7. OPZIONE PRIVILEGIATA

Dall'analisi dell'incidenza economica e sociale e delle ripercussioni sui diritti fondamentali risulta che le opzioni 2 e 3 rappresentano il migliore approccio ai problemi nella prospettiva di realizzare gli obiettivi individuati.

Globalmente, l'opzione privilegiata sarebbe una combinazione delle opzioni 2 e 3, che si completano a vicenda e corrispondono al meglio agli obiettivi definiti, sia come contenuto che per la tempistica.

8. MONITORAGGIO E VALUTAZIONE

Entro 2 anni dalla data di entrata in vigore della direttiva è opportuno pubblicare una relazione sulla sua corretta attuazione da parte degli Stati membri.

Occorre inoltre procedere a valutazioni periodiche per valutare come e in che misura la direttiva avrà contribuito al conseguimento degli obiettivi prefissati. La prima valutazione andrebbe fatta entro 5 anni dalla sua entrata in vigore; la Commissione pubblicherà successivamente relazioni di valutazione ogni 5 anni, che conterranno informazioni relative all'attuazione. Sulla base delle conclusioni e raccomandazioni delle valutazioni, la Commissione dovrebbe prendere in considerazione eventuali modifiche o sviluppi della direttiva.