CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 2 aprile 2009 (03.04)
(OR. en)

8375/09
ADD 4

TELECOM 69
DATAPROTECT 24
JAI 192
PROCIV 46

NOTA DI TRASMISSIONE

Origine:	Signor Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	31 marzo 2009
Destinatario:	Signor Javier SOLANA, Segretario Generale/Alto Rappresentante
Oggetto:	Documento di lavoro dei servizi della Commissione che accompagna la comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni Proteggere le infrastrutture critiche informatizzate "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'europa dai ciberattacchi e dalle ciberperturbazioni" Sintesi della valutazione d'impatto

Si trasmette in allegato, per le delegazioni, il documento della Commissione SEC(2009) 400.

All.: SEC(2009) 400

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 30.3.2009
SEC(2009) 400

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

che accompagna la

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO, AL PARLAMENTO EUROPEO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Proteggere le infrastrutture critiche informatizzate
"Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni"

SINTESI DELLA VALUTAZIONE D'IMPATTO

{COM(2009) 149}
{SEC(2009) 399}

SINTESI DELLA VALUTAZIONE D'IMPATTO

1. IL PROBLEMA

Il settore delle TIC è vitale per l'economia e la società dell'Unione europea

Le tecnologie dell'informazione e delle comunicazioni (TIC) fanno ormai parte integrante dell'economia e della società dell'Unione europea. **Il settore delle TIC è di importanza vitale per tutte le fasce della società. Le imprese si basano sulle TIC** sia per le attività di vendita che per una maggiore efficienza ed efficacia dei loro processi interni. Le TIC **pervadono inoltre sempre più il funzionamento e le attività delle pubbliche amministrazioni**: la diffusione dei servizi di amministrazione in linea a tutti i livelli, nel garantire procedure più efficienti, rende il settore pubblico fortemente dipendente dalle TIC per molte operazioni. Infine, anche **i cittadini utilizzano sempre più i servizi della società dell'informazione e usano le tecnologie TIC nelle loro attività quotidiane**: oltre agli effetti negativi che le eventuali ciberperturbazioni potrebbero avere su queste attività, non va dimenticata la quantità crescente di dati personali che i cittadini trasmettono per via elettronica. Misure di sicurezza inadeguate comportano il rischio di perdite di dati personali sensibili e di furti d'identità o frodi di altro tipo[1]. **Rafforzare la sicurezza e la resilienza di queste infrastrutture è quindi assolutamente fondamentale per proteggere i dati personali dei cittadini e dare adeguata applicazione al diritto di tutela della vita privata.**

I sistemi e i servizi delle TIC, oltre ad essere un'infrastruttura essenziale di per sé, costituiscono la piattaforma su cui si basano altre infrastrutture critiche in termini tecnologici e sociali, come si riconosce nel libro verde della Commissione europea relativo a un Programma europeo per la protezione delle infrastrutture critiche, nel quale si fanno rientrare nel concetto di **infrastrutture critiche informatizzate (ICI)** tutti "*i sistemi che sono infrastrutture critiche di per sé oppure che sono essenziali per il funzionamento di infrastrutture critiche (telecomunicazioni, computer, software, internet, satelliti ecc.)*"[2], analogamente all'approccio seguito dall'OCSE[3].

Nonostante le differenze terminologiche, **quel che importa è che il concetto di infrastrutture critiche informatizzate favorisce una prospettiva sistemica incentrata sul funzionamento sicuro e ininterrotto dei sistemi, dei servizi, delle reti e delle infrastrutture TIC** ("infrastrutture TIC"), **di cui internet costituisce una componente importantissima** data la sua vastissima diffusione e il processo di convergenza tecnologica (in corso).

---

1 http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece
2 COM(2005) 576 definitivo
3 http://www.oecd.org/dataoecd/1/13/40825404.pdf.

La posta in gioco

La diffusione delle infrastrutture critiche informatizzate fa sì che le ripercussioni di eventuali ciberperturbazioni possono **farsi sentire pesantemente nella società intera**.

I rischi connessi ad attentati dolosi, a catastrofi naturali o a guasti tecnici non sempre sono compresi o analizzati in maniera approfondita, per cui il grado di consapevolezza delle parti in causa non è sufficiente per elaborare misure di salvaguardia o contromisure adeguate.

I ciberattacchi hanno raggiunto un livello inedito di sofisticazione e spesso sono sferrati da gruppi criminosi o singoli individui per motivi di lucro o politici. **Questa tendenza generale è esemplificata dagli attacchi cibernetici su ampia scala di cui sono state vittima l'Estonia, la Lituania e la Georgia.** La gravità del problema è confermata dall'enorme numero di virus, vermi informatici (*worm*) e altre forme di programmi maligni (*malware*), dall'espansione delle reti di bot e dalla moltiplicazione dei messaggi indesiderati[4]. **Le infrastrutture TIC sono costantemente fatte bersaglio di attacchi** il cui impatto sarà ancora più grave se l'Europa non si prepara.

L'elevata dipendenza dalle infrastrutture critiche informatizzate, la loro interconnessione a livello internazionale e la loro interdipendenza reciproca da altre infrastrutture rendono assolutamente necessario **affrontare il problema della loro sicurezza e resilienza in una prospettiva sistemica, che costituisca il fronte di difesa** contro ciberperturbazioni e ciberattacchi e adottare in via complementare misure per prevenire, contrastare e perseguire le attività criminali e terroristiche contro le infrastrutture critiche informatizzate.

Natura del problema

Attualmente **il problema della sicurezza e della resilienza delle infrastrutture critiche informatizzate si affronta perlopiù a livello nazionale, con uno scarso coordinamento paneuropeo**. **L'assenza di una cooperazione sistematica transnazionale riduce notevolmente l'efficacia delle contromisure adottate a livello interno.** Inoltre, lo **scarso livello di sicurezza e resilienza delle infrastrutture critiche informatizzate in un paese può aggravare la vulnerabilità e i rischi in altri paesi**.

Poiché **le infrastrutture critiche informatizzate sono globali, strettamente interconnesse e interdipendenti** da altre infrastrutture, **non è possibile garantirne la sicurezza e la resilienza con un approccio esclusivamente nazionale e non coordinato**. Inoltre, **l'impressione diffusa è che le forze di mercato non sono in grado di offrire incentivi sufficienti per investimenti del settore privato nella protezione delle infrastrutture critiche informatizzate a un livello pari a quello che di norma richiederebbero i governi**.

Le cause soggiacenti al problema generale sopra descritto sono le seguenti:

- **approccio diseguale tra gli Stati membri alle politiche pubbliche per la sicurezza e la resilienza delle infrastrutture critiche informatizzate**. Le politiche applicate dagli Stati membri per la sicurezza e la resilienza delle infrastrutture critiche informatizzate non sono uniformi. Inoltre, il livello di competenza e preparazione non appare uniformemente distribuito, come sottolinea l'analisi degli approcci nazionali eseguita dalla Commissione e confermata da una relazione dell'**Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)**[5];

---

4 COM(2006) 688 definitivo

5 http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

- **difficoltà di adozione di nuovi modelli di governanza europei**. Per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate occorre riflettere sulle **problematiche di governanza**. I **governi sono responsabili** della definizione delle politiche relative alle infrastrutture critiche informatizzate, ma **il coinvolgimento del settore privato è fondamentale per metterle in pratica**. I **partenariati pubblico-privati** (PPP) hanno fatto la loro comparsa a livello nazionale come un modello di riferimento per gestire questa condivisione di responsabilità. Ma nonostante il consenso generale a favore della comparsa di simili partenariati anche a livello europeo, finora non ne sono sorti;
- **capacità europea limitata di allarme rapido e di reazione in caso di incidenti.** Le consultazioni evidenziano differenze nei sistemi nazionali di allarme rapido e risposta agli incidenti. Alcuni Stati membri non sono informati regolarmente degli incidenti a carico della sicurezza delle reti (anche se in certi casi ciò avviene in via informale tra determinati operatori) e/o non hanno creato un organismo di riferimento unico che centralizzi questo tipo di notifiche. La cooperazione e lo scambio di informazioni tra **enti governativi non** sembrano **sufficientemente sviluppati** e sono ostacolati dall'assenza di meccanismi affidabili di coordinamento e condivisione, che a loro volta **richiedono l'esistenza di gruppi nazionali o governativi di pronto intervento informatico (Computer Emergency Response Teams, CERT), ben rodati e dotati di una base comune in termini di capacità**. Inoltre, **le esercitazioni e le simulazioni pratiche a livello UE,** che costituiscono l'elemento chiave del rafforzamento della sicurezza e della resilienza, sono ancora in una **fase embrionale**;
- **scarsa consapevolezza dei rischi per la sicurezza e la resilienza di internet**. Data la sua configurazione distribuita e ridondante **l'infrastruttura** di internet si è rivelata finora **piuttosto robusta e resiliente**. Ma è ragionevole **interrogarsi** sulla capacità di internet di continuare a opporre resistenza al **numero crescente** di ciberperturbazioni e ciberattacchi in considerazione della sua **crescita fenomenale**, della sua **crescente complessità** e dell'**apparizione di nuovi servizi**.

Nessun paese è isolato. La natura globale delle infrastrutture critiche informatizzate, in particolare di internet, richiede un **approccio globale comune** alla sicurezza e alla resilienza. **Solo attraverso un forte coordinamento europeo si potranno ottenere impatti diretti su scala internazionale.**

2. MOTIVAZIONE DI UN'AZIONE A LIVELLO COMUNITARIO

Un **approccio puramente nazionale per affrontare i problemi sopra descritti non può essere sufficiente**. Date le significative ripercussioni internazionali, molte minacce alla sicurezza delle reti e dell'informazione possono causare gravi esternalità oltre confine, a cui non si può far fronte efficacemente limitandosi al livello nazionale e che possono causare perturbazioni in altri paesi.

Un approccio integrato a livello UE per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate potrebbe utilmente completare e dare valore aggiunto ai programmi nazionali di protezione delle infrastrutture critiche informatizzate e ai regimi di cooperazione esistenti tra gli Stati membri. A fronte di problemi e tematiche comuni è vantaggioso per tutti adottare un approccio comune.

Dal dibattito che ha fatto seguito agli attacchi subiti dall'Estonia è emerso che gli effetti di eventi simili possono essere limitati da **misure di prevenzione**, come ad esempio uno scambio di informazioni più strutturato a livello europeo, e da **un'azione coordinata** durante la crisi vera e propria. Nel pieno rispetto del **principio di sussidiarietà** la Commissione è

nella posizione ideale per coordinare tali attività, in stretta cooperazione con gli Stati membri e altri organismi internazionali.

Inoltre le problematiche della sicurezza nazionale, pur avendo un ruolo importante nella definizione delle politiche e degli obblighi in materia di sicurezza delle reti e dell'informazione, possono dar luogo a una frammentazione normativa e incidere negativamente sulla competitività dell'Unione europea nel suo insieme e sulla capacità del mercato unico europeo di creare ricchezza.

Nel 2006 la Commissione annunciava l'intenzione[6] di elaborare, nell'ambito del Programma europeo per la protezione delle infrastrutture critiche (EPCIP)[7], una politica specifica per il settore delle TIC "*per migliorare la sicurezza e la resilienza delle reti e dei sistemi informatici*". L'annuncio è stato accolto favorevolmente dal Consiglio europeo nel 2007[8].

Quest'iniziativa tiene adeguatamente conto della dimensione internazionale e in particolare dei principi affermati dal G8 sulla protezione delle infrastrutture critiche informatizzate, della risoluzione 58/199 dell'Assemblea generale dell'ONU sulla Creazione di una cultura mondiale della cibersicurezza e la protezione delle infrastrutture critiche informatizzate e infine della recente Raccomandazione dell'OCSE sulla protezione delle infrastrutture critiche informatizzate.

Infine, l'iniziativa politica proposta tiene conto e non costituisce un doppione delle attività della NATO in materia di cibersicurezza, focalizzate sulla difesa militare, ossia la politica comune di ciberdifesa, le attività dell'Autorità di gestione della ciberdifesa e quelle del Centro di eccellenza per la ciberdifesa cooperativa della NATO.

3. OBIETTIVI

Gli obiettivi dell'iniziativa sono **rafforzare il livello di preparazione e di risposta in tutta Europa** nei confronti dei rischi e delle minacce sopra descritti, evitando un approccio frammentato degli Stati membri. Si mette a fuoco la definizione di processi condivisi per far fronte in modo flessibile a minacce note e sconosciute. Le parti pubbliche e private si impegneranno a mettere in atto un **numero sufficiente e adeguato di misure di prevenzione, individuazione, emergenza e recupero** per raggiungere **il livello adeguato di sicurezza e resilienza delle infrastrutture critiche informatizzate e garantire la continuità dei servizi**. Una maggiore sicurezza e resilienza avranno anche un **impatto positivo sulla protezione dei dati personali e della vita privata dei cittadini dell'UE**.

L'obiettivo generale della proposta, cioè **garantire la sicurezza e la resilienza delle infrastrutture critiche informatizzate come fronte di difesa**, si può raggiungere attraverso quattro obiettivi specifici:

(1) colmare i divari tra le politiche nazionali in materia di sicurezza e resilienza delle infrastrutture critiche informatizzate;

(2) rafforzare la governanza europea per la sicurezza e la resilienza delle infrastrutture critiche informatizzate;

(3) rafforzare la capacità operativa di risposta agli incidenti in Europa;

(4) migliorare la sicurezza e la resilienza di internet.

---

6 COM(2006) 251.
7 COM(2006) 786.
8 Risoluzione 2007/C 68/01 del Consiglio.

4. OPZIONI POLITICHE

Opzione 1: status quo

Non proporre nessun tipo di azione non costituisce un'opzione percorribile. Senza un'azione trasversale a livello dell'UE gli Stati membri continueranno ad agire individualmente o nell'ambito di accordi bilaterali o multilaterali limitati. Ci sarebbe **un rischio connesso all'evoluzione di approcci nazionali diversi** che potrebbero essere incompatibili. Inoltre, la collaborazione al di là dei confini nazionali sarebbe ad hoc e potrebbe rivelarsi inefficace di fronte alla sofisticazione e all'ampiezza dei ciberattacchi.

Poiché gli Stati membri continuerebbero ad affrontare questi problemi secondo ritmi diversi, le parti interessate **sarebbero restie a effettuare investimenti nella sicurezza e nella resilienza** in quanto la molteplicità delle norme e degli obblighi ne ridurrebbe la competitività. La dimensione transnazionale del problema non farebbe che acuire le differenze di sicurezza, resilienza e preparazione su scala europea. La vulnerabilità delle infrastrutture critiche informatizzate in Europa rimarrebbe elevata e potrebbe perfino aumentare, nonostante gli sforzi individuali.

Opzione 2: quadro non vincolante

La Commissione proporrebbe un **quadro di coordinamento e cooperazione** che assumerebbe la forma di una Comunicazione e di un Piano di azione nel quale sarebbero coinvolti gli Stati membri, il settore privato e la società civile. La comunicazione dovrebbe essere approvata dal Consiglio e anche il Parlamento europeo potrebbe decidere di dare un contributo alla discussione.

L'iniziativa si focalizzerebbe sugli obiettivi sopra evidenziati e proporrebbe in particolare di:

(1) **promuovere la coerenza tra le politiche nazionali in materia di sicurezza e resilienza delle infrastrutture critiche informatizzate** attraverso

- l'identificazione di esempi trasmissibili di buone pratiche politiche e punti comuni;
- l'istituzione di un forum europeo per permettere agli Stati membri di condividere informazioni e buone pratiche politiche in materia di sicurezza e resilienza delle infrastrutture critiche informatizzate;

(2) **rafforzare la governanza europea per la sicurezza e la resilienza delle infrastrutture critiche informatizzate** attraverso

- la creazione di **partenariati pubblico-privati europei per la resilienza**, destinati a rafforzare la collaborazione tra i settori pubblico e privato sugli obiettivi della resilienza e della sicurezza, sui requisiti di base e sulle buone pratiche politiche e misure;

(3) **rafforzare la capacità operativa di risposta agli incidenti in Europa** attraverso

- la costituzione di gruppi nazionali o governativi di pronto intervento informatico (CERT)[9] ben rodati, che abbiano un ruolo chiave nella capacità nazionale di preparazione, scambio di informazioni, coordinamento e reazione;
- l'approvazione di un livello minimo di capacità e servizi dei suddetti gruppi di pronto intervento informatico;

[9] Gruppi di pronto intervento informatico

- una migliore cooperazione a livello europeo tra i gruppi di pronto intervento informatico nazionali o governativi; cooperazione e contatti più agevoli tra le capacità nazionali di risposta; organizzazione di esercitazioni paneuropee e/o regionali su incidenti simulati di ampia portata;
- la promozione dell'elaborazione di piani di emergenza per reagire in caso di incidenti a danno delle reti e riprendersi dopo il disastro;
- il finanziamento dell'elaborazione di esercitazioni europee su incidenti a danno della sicurezza delle reti simulati di ampia portata;
- lo sviluppo e l'adozione di un Sistema europeo di condivisione delle informazioni e di allarme in grado di raggiungere efficacemente e in pari tempo i cittadini e le piccole e medie imprese;

(4) **migliorare la sicurezza e la resilienza di internet** attraverso

- la definizione di priorità europee per la stabilità e la resilienza di internet a lungo termine;
- l'approvazione di una serie di principi, prima europei e poi internazionali, per la sicurezza e la resilienza di internet.

Opzione 3: quadro vincolante

La maggior parte delle problematiche sopra descritte sarebbero affrontate con una serie di misure vincolanti che potrebbero assumere la forma di una direttiva, di un regolamento o di una decisione, a seconda dei casi.

La Commissione potrebbe proporre l'adozione di misure vincolanti al fine di:

(1) **definire una base per armonizzare le politiche nazionali**. Si tratterebbe di misure finalizzate ad aumentare la sicurezza e la resilienza delle infrastrutture critiche informatizzate al di là della normativa di mercato già proposta;

(2) **definire il ruolo e le responsabilità delle parti pubbliche e private** in materia di sicurezza e resilienza delle infrastrutture critiche informatizzate;

(3) **migliorare la preparazione operativa**, ad esempio attraverso

(a) una serie minima di norme per funzioni e servizi armonizzati dei gruppi di pronto intervento informatico nazionali o governativi;

(b) un quadro per i piani nazionali d'emergenza ai fini dell'elaborazione di piani europei di emergenza.

5. RAFFRONTO DELLE DIVERSE OPZIONI

Lo status quo non ha **alcun vantaggio** per il miglioramento della sicurezza e della resilienza delle infrastrutture critiche informatizzate in Europa. Si deve quindi scegliere tra un quadro vincolante o non vincolante. Attualmente, l'opzione del quadro vincolante non sembra attuabile fra l'altro per i seguenti motivi:

- la **realtà politica** degli Stati sovrani, di cui deve tener conto adeguatamente qualsiasi politica in materia di sicurezza delle reti e dell'informazione a livello comunitario;
- la necessità di prendere in considerazione le responsabilità operative ampiamente distribuite del settore privato;

- l'assenza di esperienza cumulativa in fatto di condivisione di informazioni e cooperazione tra settore pubblico e settore privato sulle politiche in materia di infrastrutture critiche informatizzate.

A ciò si aggiunge la **scarsa qualità dei dati** attualmente disponibili sugli incidenti a danno della sicurezza, a causa di asimmetrie nell'informazione e di preoccupazioni legate alla sicurezza nazionale, che ostacola la definizione di misure regolamentari in una prospettiva di politica pubblica ed economica coerente e solleva il problema del **rispetto del principio di proporzionalità**, giacché è impossibile proporre azioni proporzionate se si ignora quale sia la portata precisa del problema.

Da ultimo, la lunghezza delle procedure necessarie per l'adozione eventuale di un quadro vincolante sarebbe incompatibile con l'esigenza di tutte le parti in causa di agire con rapidità.

In conclusione la presente valutazione di impatto indica come preferibile, a breve e medio termine, l'opzione politica 2, vale a dire il varo immediato delle azioni proposte e la revisione dei loro risultati entro termini ragionevoli, tenendo conto anche del dibattito pubblico su una politica per la sicurezza delle reti e dell'informazione in Europa più moderna e più forte. Questi risultati costituirebbero la base di valutazione delle necessità e delle opzioni per l'eventuale adozione futura di misure vincolanti.

In seguito a tale valutazione si potrebbe raccomandare la realizzazione di azioni analoghe a quelle previste dall'opzione 3.