CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 27 maggio 2009 (03.06)
(OR. en)

10125/09

TELECOM 115
DATAPROTECT 39
JAI 319
PROCIV 78

NOTA

del:	Gruppo "Telecomunicazioni e società dell'informazione"
al:	Coreper/Consiglio
n. prop. Com:	8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46
Oggetto:	Politica europea per la sicurezza delle reti e dell'informazione - Orientamenti per uno scambio di opinioni

In vista della sessione del Consiglio TTE dell'11 giugno 2009, si allegano per le delegazioni, per informazione, gli orientamenti definiti dalla presidenza per lo scambio di opinioni tra i ministri.

ORIENTAMENTI PER UNO SCAMBIO DI OPINIONI SUL

FUTURO DELLA POLITICA EUROPEA PER LA SICUREZZA DELLE RETI E DELL'INFORMAZIONE

CONSIGLIO TTE, 11 GIUGNO 2009

1. INTRODUZIONE

Le reti di comunicazione e i sistemi d'informazione sono diventati il sistema nervoso della nostra società moderna. Molti servizi e processi della nostra economia e società dipendono sempre più dal loro buon funzionamento e la loro sicurezza e resilienza sono motivo di una preoccupazione in rapida crescita.

I rischi legati alle tecnologie dell'informazione e della comunicazione rappresentano una sfida costante per l'Europa, principalmente per via dell'incessante evoluzione delle minacce informatiche, della loro crescente complessità e della loro globalizzazione. Tale sfida è acuita dalle interdipendenze globali delle infrastrutture, dalle tecnologie emergenti, dall'onnipresenza delle tecnologie dell'informazione e della comunicazione, dalla mancanza di norme minime e dalla continua convergenza delle tecnologie.

Le sfide legate alla sicurezza delle reti e dell'informazione richiederanno una risposta europea forte e coordinata. I recenti attacchi informatici contro singoli paesi hanno dimostrato che un solo paese, preso isolatamente, può essere molto vulnerabile. Un approccio su scala UE che integri ed apporti un valore aggiunto alle iniziative nazionali è un elemento essenziale della politica per la sicurezza delle reti e dell'informazione.

2. ENISA - AGENZIA EUROPEA PER LA SICUREZZA DELLE RETI E DELL'INFORMAZIONE

Per affrontare le sfide legate alla sicurezza della società dell'informazione, nel 2004 la Comunità europea ha istituito l'Agenzia europea per la sicurezza delle reti e dell'informazione[1] (ENISA) al fine di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle amministrazioni dell'UE.

[1] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pagg. 1-11).

L'ENISA è stata istituita inizialmente per un periodo di cinque anni (2004-2009).
Il 24 settembre 2008 il Consiglio e il Parlamento europeo hanno adottato un regolamento che proroga, senza modificarlo, per un periodo di tre anni - con scadenza il 13 marzo 2012 - il mandato dell'ENISA[1]. Per il periodo 2004-2012, l'ENISA dispone di un bilancio annuale che si aggira sugli otto milioni di euro e di un organico di circa 50 persone.

Al fine di vagliare le opzioni per il futuro dell'ENISA dopo marzo 2009, la Commissione ha avviato una valutazione, affidata ad un gruppo di esperti esterni, dei risultati conseguiti dall'Agenzia dalla sua istituzione[2]. Nel giugno 2007 la Commissione ha pubblicato una comunicazione sulla valutazione dell'ENISA[3] contenente una valutazione della relazione del gruppo di esperti esterni e le raccomandazioni del consiglio di amministrazione dell'ENISA. I risultati principali della relazione del gruppo di esperti hanno confermato la validità delle politiche alla base della creazione dell'ENISA e dei suoi obiettivi originari e, in particolare, il suo contributo alla realizzazione di un autentico mercato interno delle comunicazioni elettroniche.

Il consiglio di amministrazione dell'ENISA ha formulato raccomandazioni sulle eventuali modifiche da apportare al regolamento ENISA[4]. Secondo le principali raccomandazioni è opportuno rivedere il regolamento ENISA per prolungare il mandato dell'Agenzia, è opportuno fissare nuovamente una data di revisione del mandato, non si deve cambiare materialmente il campo di attività dell'Agenzia ed è opportuno rivedere il regolamento in modo da combinare gli articoli 2 e 3[5] per definire obiettivi chiave improntati ai risultati che siano realistici e rientrino nel campo di attività dell'Agenzia.

---

1 Regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 293 del 31.10.2008).

2 "Evaluation of the European Network and Information Security Agency," (Valutazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione), relazione finale del gruppo di esperti, IDC EMEA, 8.1.2007{disponibile all'indirizzo: http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm }

3 COM(2007) 285 definitivo.

4 Disponibile all'indirizzo: http://enisa.europa.eu/pages/03_02.htm Le raccomandazioni in questione sono trattate anche nel documento COM(2007) 285 definitivo.

5 Riguardanti, rispettivamente, gli obiettivi e i compiti.

3. CONTESTO POLITICO DELLO SCAMBIO DI OPINIONI

Il 2 settembre 2008, nel suo intervento dinanzi al Parlamento europeo riunito in seduta plenaria, la Commissione ha invitato il Parlamento europeo e il Consiglio ad avviare, all'inizio del 2009, un'intensa discussione sull'approccio dell'Europa alla sicurezza delle reti e sul modo in cui affrontare gli attacchi informatici e ad includere il futuro dell'ENISA in queste riflessioni.

Il 24 settembre 2008, nei considerando del regolamento recante proroga del mandato dell'ENISA, il Consiglio e il Parlamento europeo hanno invitato ad "un'ulteriore discussione sull'Agenzia" e "sull'orientamento generale degli sforzi europei volti ad aumentare la sicurezza della rete e delle informazioni".

4. PASSI PREPARATORI

Per agevolare il dibattito, i servizi della Commissione hanno in primo luogo proceduto, dal 7 novembre 2008 al 9 gennaio 2009, ad una consultazione pubblica sugli eventuali obiettivi di una politica rafforzata a livello UE in materia di sicurezza delle reti e dell'informazione e sui mezzi per raggiungere tali obiettivi. I servizi della Commissione hanno altresì organizzato un seminario, tenutosi il 15 dicembre 2008, nel quale esperti in materia di sicurezza delle reti e dell'informazione provenienti dagli organi competenti degli Stati membri hanno discusso del quadro mutevole delle sfide nel settore della sicurezza, di eventuali priorità e obiettivi politici per affrontare queste sfide in evoluzione e degli strumenti e meccanismi necessari ad una politica per la sicurezza delle reti e dell'informazione rafforzata a livello europeo.

Nel quadro della consultazione pubblica riguardante il futuro dell'ENISA, la grande maggioranza dei rispondenti ha espresso sostegno ad una proroga del mandato dell'Agenzia e si è detta favorevole ad un ruolo più importante della medesima nella cooperazione nell'ambito delle attività legate alla sicurezza delle reti e dell'informazione a livello europeo nonché ad un incremento delle sue risorse.

5. AZIONI IN CORSO NEL SETTORE DELLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Nell'ambito dell'iniziativa quadro concernente il programma europeo per la protezione delle infrastrutture critiche (EPCIP), la Commissione europea ha adottato di recente una comunicazione sulla protezione delle infrastrutture critiche informatizzate intitolata "Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni".[1]

[1] COM(2009) 149.

La comunicazione propone una serie di azioni a breve e medio termine (fino al 2011) nel settore della sicurezza e della resilienza delle infrastrutture critiche informatizzate, quali: favorire la cooperazione paneuropea tra CERT nazionali o governativi; stimolare il settore privato alla condivisione di informazioni e buone pratiche con il settore pubblico; sostenere la condivisione di informazioni e buone pratiche politiche tra Stati membri, per stimolare in tal modo una più intensa cooperazione europea tra Stati membri attraverso piani di emergenza nazionali e multinazionali e esercitazioni periodiche sulla reazione a incidenti gravi e diffusi a danno della sicurezza delle reti e sul ripristino in caso di disastro, e proseguire l'elaborazione dei criteri per individuare le infrastrutture critiche europee nel settore delle TIC.

6. CONFERENZA MINISTERIALE DI TALLINN

Il 27 e 28 aprile 2009 si è tenuta a Tallinn una conferenza ministeriale dedicata alla protezione delle infrastrutture critiche informatizzate. La conferenza è stata organizzata dall'Estonia sotto gli auspici della presidenza ceca dell'UE.

Nelle conclusioni della conferenza è stato espresso sostegno ai lavori in corso nel settore della protezione delle infrastrutture critiche informatizzate ed è stato sottolineato che tali lavori dovrebbero concentrarsi su azioni volte a rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate, a costituire partenariati pubblico-privati efficaci a livello UE e ad intensificare la cooperazione e il coordinamento nell'UE e a livello internazionale. Dalla conferenza è emerso che gli ultimi anni hanno dimostrato che gli attacchi informatici hanno raggiunto un livello inedito di sofisticazione e sono sempre più spesso realizzati per motivi di lucro o politici e l'enorme numero di virus, vermi informatici (worm) e altre forme di programmi maligni (malware), l'espansione delle reti di bot nonché la moltiplicazione dei messaggi indesiderati confermano la gravità del problema. Ne è emerso inoltre che tali minacce richiedono una risposta europea forte e coordinata.

Per quanto riguarda l'ENISA, la conferenza ha concluso che l'Agenzia costituisce uno strumento prezioso per rafforzare gli sforzi di cooperazione in questo settore a livello UE. Tuttavia, le sfide nuove e durature che abbiamo davanti richiedono che il mandato dell'Agenzia venga profondamente ripensato e riformulato per incentrare maggiormente l'attenzione sulle priorità e le esigenze dell'UE, raggiungere una capacità di reazione più flessibile, sviluppare le capacità e competenze europee e rafforzare l'efficienza operativa e l'impatto globale dell'Agenzia. Secondo la conferenza, in questo modo l'ENISA potrebbe diventare una risorsa permanente per ciascuno Stato membro e l'Unione europea nel suo insieme.

La conferenza ha inoltre concluso che entro il 2010 dovrebbe essere organizzata e condotta un'esercitazione comune dell'UE sulla protezione delle infrastrutture critiche informatizzate, conformemente al piano d'azione della Commissione. Un'espressione di sostegno da parte del Consiglio TTE a favore di tale esercitazione ne metterebbe in risalto il significato quale primo passo tangibile verso un forte coordinamento e cooperazione tra gli Stati membri e quale strumento per contribuire a individuare i settori che richiedono azioni immediate.

7. RIESAME DEL QUADRO NORMATIVO PER LE COMUNICAZIONI ELETTRONICHE

Conformemente al nuovo quadro normativo per le comunicazioni elettroniche, all'ENISA è assegnato un ruolo di sostegno degli organi degli Stati membri e della Commissione relativamente agli aspetti della sicurezza delle reti e dell'informazione.

8. QUESITI PER ORIENTARE LO SCAMBIO DI OPINIONI

1. Quali dovrebbero essere le due o tre principali finalità a medio/lungo termine di una politica per la sicurezza delle reti e dell'informazione rafforzata a livello europeo, affinché siano garantiti una cooperazione transnazionale tra tutti i soggetti interessati e strumenti politici permanenti o a lungo termine?

2. Anche se un'agenzia sembra essere uno strumento efficace per rafforzare la politica per la sicurezza delle reti e dell'informazione in Europa, sarebbe opportuno prevedere altri mezzi a medio/lungo termine?

3. Come si dovrebbe riformare l'ENISA per incentrare maggiormente l'attenzione sulle sfide principali, con una maggiore flessibilità per adeguarsi all'evolversi del quadro delle minacce informatiche, una garanzia permanente o a lungo termine di continuità, adeguate valutazioni dei suoi risultati e una struttura amministrativa rafforzata? Sarebbe necessario un incremento delle risorse per far fronte a queste sfide?