COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 30.3.2009
COM(2009) 149 definitivo

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, 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"

{SEC(2009)399}
{SEC(2009)400}

(presentata dalla Commissione)

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, 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"

1. INTRODUZIONE

Le tecnologie dell'informazione e delle comunicazioni (TIC) sono sempre più presenti nelle nostre attività quotidiane. Alcuni di questi sistemi, servizi, reti e infrastrutture TIC (o in breve le infrastrutture TIC) costituiscono una parte vitale dell'economia e della società europee in quanto forniscono beni e servizi essenziali oppure fungono da piattaforma su cui si basano altre infrastrutture critiche. In generale sono chiamate infrastrutture critiche informatizzate (ICI)[1] in quanto la loro perturbazione o distruzione avrebbe gravi ripercussioni su funzioni vitali della società. Esempi recenti di questo tipo di perturbazioni sono i ciberattacchi su ampia scala di cui è stata vittima l'Estonia nel 2007 e la rottura dei cavi transcontinentali nel 2008.

Nel 2008 il Forum economico globale ha stimato che nei prossimi 10 anni la probabilità di un'avaria grave delle infrastrutture critiche informatizzate è del 10-20%, con un costo economico potenziale a livello globale di circa 250 miliardi di dollari[2].

La presente comunicazione si concentra sulle azioni di prevenzione, preparazione e sensibilizzazione e definisce un piano di azioni immediate destinate a rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate. Quest'impostazione riflette il dibattito avviato su richiesta del Consiglio e del Parlamento europeo per approfondire le problematiche e le priorità connesse alla politica della sicurezza delle reti e dell'informazione e analizzare gli strumenti più appropriati per affrontarle a livello europeo. Le azioni proposte sono inoltre complementari a quelle destinate a prevenire, contrastare e perseguire le attività criminali e terroristiche che prendono di mira le infrastrutture critiche informatizzate, in sinergia con le attività di ricerca in corso e previste a livello dell'UE nel campo della sicurezza delle reti e dell'informazione e con le attività internazionali in questo campo.

2. CONTESTO POLITICO

La presente comunicazione è destinata ad elaborare la strategia europea per rafforzare la sicurezza della società dell'informazione e la fiducia nella medesima. Già nel 2005 la Commissione[3] aveva sottolineato l'urgenza di coordinare le azioni per rafforzare la fiducia di tutti gli interessati nelle comunicazioni e nei servizi elettronici. Per questo nel 2006 è stata

---

1 Nella comunicazione COM(2005) 576 definitivo è stata proposta una definizione delle infrastrutture critiche informatizzate.

2 Global Risks 2008.

3 COM(2005) 229.

adottata una strategia per una società dell'informazione sicura[4]. Il Consiglio ha approvato i suoi elementi principali, come la sicurezza e la resilienza delle infrastrutture TIC, con la risoluzione 2007/068/01. Tuttavia i soggetti interessati non sembrano aderire sufficientemente a tali principi, né metterli in pratica. Tale strategia rafforza anche il ruolo, sul piano tattico e operativo, dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), istituita nel 2004 per dare un contributo al raggiungimento degli obiettivi di garantire un livello elevato ed efficace di sicurezza delle reti e dell'informazione nella Comunità e di approfondire una cultura della sicurezza a vantaggio dei cittadini, dei consumatori, delle imprese e delle amministrazioni dell'Unione europea.

Nel 2008 il mandato dell'ENISA è stato prolungato tal quale fino al marzo 2012[5]. Nello stesso tempo il Consiglio e il Parlamento europeo hanno invitato a *approfondire il dibattito sul futuro dell'ENISA e sull'orientamento generale delle attività europee tese a rafforzare la sicurezza delle reti e dell'informazione*. Per favorire il dibattito la Commissione ha avviato nel novembre scorso una consultazione pubblica in linea[6] i cui risultati dovrebbero essere disponibile a breve.

Le attività pianificate nella presente comunicazione sono condotte nell'ambito e in parallelo col programma europeo per la protezione delle infrastrutture critiche (EPCIP)[7]. Un elemento chiave del programma EPCIP è la direttiva[8] relativa all'individuazione e alla designazione delle infrastrutture critiche europee[9] che indica il settore delle TIC come un settore prioritario del futuro. Un altro elemento importante del programma EPCIP è la rete informativa di allarme sulle infrastrutture critiche (CIWIN)[10].

Sul piano normativo, la proposta della Commissione di riformare il quadro normativo comune per le reti ed i servizi di comunicazione elettronica[11] contiene nuove disposizioni sulla sicurezza e l'integrità, miranti in particolare a rafforzare gli obblighi degli operatori di provvedere all'adozione di idonee misure per far fronte ai rischi individuati, garantire la continuità della fornitura di servizi e comunicare le violazioni della sicurezza[12]. Quest'impostazione è funzionale all'obiettivo generale di rafforzamento della sicurezza e della resilienza delle infrastrutture critiche informatizzate. Il Parlamento europeo e il Consiglio sostengono ampiamente tali disposizioni.

Le azioni proposte nella presente comunicazione integrano le misure esistenti e di cui si prevede l'adozione nel settore della cooperazione di polizia e giudiziaria per prevenire, contrastare e perseguire le attività criminali e terroristiche contro le infrastrutture TIC, come prevede tra l'altro la decisione quadro del Consiglio sugli attacchi contro i sistemi informatici[13] e nel suo previsto aggiornamento[14].

---

4 COM(2006) 251.
5 Regolamento (CE) n. 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 definitivo.
8 2008/114/CE.
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 COM(2008) 676 definitivo.
11 Documenti COM(2007) 697, COM(2007) 698, COM(2007) 699.
12 Articolo 13 della direttiva quadro.
13 2005/222/JAI.
14 COM(2008) 712.

Tale iniziativa tiene conto delle attività della NATO sulla politica comune per la ciberdifesa, vale a dire l'autorità di gestione della ciberdifesa e il centro di eccellenza per la ciberdifesa.

Infine, si tiene adeguatamente conto degli sviluppi della politica internazionale, in particolare dei principi affermati dal G8 sulla protezione delle infrastrutture critiche informatizzate[15], 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 della raccomandazione recente dell'OCSE sulla protezione delle infrastrutture critiche informatizzate.

3. LA POSTA IN GIOCO

3.1. Le infrastrutture critiche informatizzate sono vitali per la crescita dell'economia e della società dell'Unione europea

Il ruolo economico e sociale del settore delle TIC e delle infrastrutture TIC sono evidenziati in recenti rapporti sull'innovazione e la crescita economica, tra cui la comunicazione sul riesame intermedio dell'iniziativa i2010[16], il rapporto del gruppo Aho[17] e le relazioni economiche annuali dell'Unione europea[18]. L'OCSE sottolinea l'importanza delle TIC e di internet per *migliorare le prestazioni economiche e il benessere sociale e rafforzare la capacità delle società di migliorare la qualità della vita dei cittadini in tutto il mondo*[19] e raccomanda l'adozione di politiche per rafforzare la fiducia nell'infrastruttura di internet.

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 dei loro processi interni. Le TIC costituiscono una componente fondamentale dell'innovazione e contribuiscono per quasi il 40% della crescita di produttività[20]. Le TIC pervadono le attività delle pubbliche amministrazioni: i servizi di amministrazione on-line a tutti i livelli e applicazioni nuove, ad esempio nei settori della salute, dell'energia e della partecipazione politica, rendono il settore pubblico fortemente dipendente dalle TIC. Anche i normali cittadini utilizzano sempre più le tecnologie TIC nelle loro attività quotidiane: una maggiore sicurezza delle infrastrutture critiche informatizzate permetterebbe di accrescere la fiducia dei cittadini nelle TIC, anche grazie ad una maggiore protezione dei dati personali e della vita privata.

3.2. I rischi per le infrastrutture critiche informatizzate

I rischi connessi ad attentati intenzionali, a catastrofi naturali o a guasti tecnici non sempre sono compresi o analizzati in maniera abbastanza approfondita per cui il grado di consapevolezza degli interessati non è sufficiente per elaborare misure di salvaguardia o contromisure efficaci.

I ciberattacchi hanno raggiunto un livello inedito di sofisticazione. Da semplici esperimenti si sta passando ad attività sofisticate, realizzate per motivi di lucro o politici. Gli esempi di

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf
16 COM(2008) 199 definitivo.
17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm
18 EU Economy 2007 Review http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf
19 http://www.oecd.org/dataoecd/1/29/40821707.pdf
20 http://epp.eurostat.ec.europa.eu/ - Scienza e tecnologia/ Società dell'informazione.

questa tendenza generale che hanno avuto un ampio riscontro mediatico sono i recenti 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[21].

L'elevata dipendenza dalle infrastrutture critiche informatizzate, la loro interconnessione a livello internazionale e la loro interdipendenza reciproca da altre infrastrutture, la vulnerabilità e i rischi a cui sono esposte 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.

3.3. Aumentare la sicurezza e la resilienza delle infrastrutture critiche informatizzate per rafforzare la fiducia nella società dell'informazione

Per garantire la massima utilizzazione delle infrastrutture TIC e cogliere tutti i vantaggi delle opportunità offerte dalla società dell'informazione a livello economico e sociale è necessario che tutti gli interessati abbiano piena fiducia in queste infrastrutture. Questo dipende da vari elementi di cui il più importante è la garanzia della massima sicurezza e resilienza. La diversità, l'apertura, l'interoperabilità, la fruibilità, la trasparenza, l'obbligo di rendicontazione, la verificabilità delle varie componenti e la concorrenza sono i principali motori che permettono di sviluppare la sicurezza e di promuovere la diffusione di prodotti, processi e servizi destinati a migliorare la sicurezza. Come la Commissione ha già avuto modo di sottolineare[22], la responsabilità è condivisa: non esistono parti che possiedano da sole gli strumenti per garantire la sicurezza e la resilienza delle infrastrutture critiche informatizzate e in grado di accollarsi tutte le relative responsabilità.

Assumersi tali responsabilità presuppone una cultura e un approccio alla gestione del rischio, la capacità di rispondere a minacce note e di prevederne di sconosciute, senza reazioni eccessive e senza soffocare la nascita di applicazioni e servizi innovativi.

3.4. Le sfide per l'Europa

A complemento di tutte le attività connesse con l'attuazione della direttiva relativa all'individuazione e alla designazione delle infrastrutture critiche europee, in particolare l'individuazione dei criteri specifici per il settore delle TIC, occorre affrontare tutta una serie di problematiche per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate.

3.4.1. Attività nazionali diseguali e non coordinate

Anche se i problemi e gli ostacoli da affrontare hanno dei punti in comune, le misure e i regimi in atto negli Stati membri per garantire la sicurezza e la resilienza delle infrastrutture critiche informatizzate e il livello di competenza e di preparazione variano da uno Stato membro all'altro.

Un approccio esclusivamente nazionale comporta il rischio di produrre frammentazione e inefficienza a livello europeo. I diversi approcci nazionali e l'assenza di una cooperazione

[21] COM(2006) 688 definitivo.
[22] COM(2006) 251 definitivo.

internazionale sistematica riduce l'efficacia delle contromisure adottate a livello nazionale, tra l'altro perché vista l'interconnettività delle infrastrutture critiche di informazione, uno scarso livello di sicurezza e resilienza in un paese può aggravare la vulnerabilità e i rischi in altri paesi.

Per ovviare a questa situazione è necessaria un'azione a livello europeo per rafforzare i programmi e le politiche nazionali favorendo una maggiore sensibilizzazione e comprensione dei problemi, l'adozione di obiettivi e priorità politiche condivisi, il rafforzamento della cooperazione tra Stati membri e l'integrazione delle politiche nazionali in una dimensione più europea e globale.

3.4.2. Necessità di un nuovo modello europeo di governanza per le infrastrutture critiche informatizzate

Per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate occorre riflettere sulle problematiche di governanza. Se i responsabili ultimi della definizione delle politiche in materia di infrastrutture critiche informatizzate restano comunque gli Stati membri, l'attuazione di tali politiche dipende dal coinvolgimento del settore privato che detiene o controlla un ampio numero di infrastrutture critiche. D'altro canto, i mercati non sempre offrono 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.

Per far fronte a questo aspetto di governanza ha fatto la sua comparsa a livello nazionale un modello di riferimento costituito dai partenariati pubblico-privati (PPP). Ma anche se tutti sono concordi nel riconoscere che sarebbe auspicabile la comparsa di simili partenariati anche a livello europeo, finora non ne sono sorti. Definire un quadro per una governanza su scala europea plurilaterale, con un ruolo dell'ENISA rafforzato, permetterebbe di promuovere il coinvolgimento del settore privato nella definizione di obiettivi strategici pubblici e di misure e priorità operative. Questo quadro permetterebbe anche di avvicinare le distanze tra i decisori politici e la realtà operativa sul campo.

3.4.3. Capacità europea limitata di allarme rapido e di reazione in caso di incidenti

I meccanismi di governanza saranno efficaci solo se tutte le parti in causa dispongono di informazioni affidabili in base alle quali intervenire. Quest'aspetto è particolarmente pertinente per i governi, cui spetta la responsabilità ultima di garantire la sicurezza e il benessere dei cittadini.

I processi e le pratiche applicati per monitorare e riferire in merito agli incidenti a danno della sicurezza delle reti sono però molto diversi da uno Stato membro all'altro. Alcuni non hanno un'organizzazione di riferimento che funga da punto unico di monitoraggio. E quel che più conta è che la collaborazione e la condivisione di informazioni tra Stati membri, in particolare di dati affidabili e che permettano di agire in caso di incidenti a carico della sicurezza, sono poco sviluppate perché sono informali o si limitano a scambi bilaterali o multilaterali limitati. Riveste inoltre un'importanza strategica per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate la simulazione di incidenti e l'esecuzione di esercitazioni per testare le capacità di risposta, in particolare incentrate su strategie e processi flessibili per far fronte all'imprevedibilità delle eventuali crisi. A livello UE le esercitazioni in materia di

cibersicurezza sono ancora in una fase embrionale e solo in casi limitati si conducono esercitazioni al di là dei confini nazionali. Come hanno dimostrato eventi recenti[23], l'aiuto reciproco costituisce un elemento essenziale per dare una risposta appropriata a minacce e attacchi alle infrastrutture critiche informatizzate su ampia scala.

Per disporre di una forte capacità di allarme rapido e di reazione a livello europeo in caso di incidenti si deve poter contare su 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. Questi organismi devono agire come catalizzatori nazionali degli interessi e della capacità delle parti in causa di realizzare attività di utilità pubblica (come quelle connesse ai sistemi di condivisione delle informazioni e di allarme destinate ai cittadini e alle PMI) e impegnarsi attivamente nella cooperazione transnazionale e nello scambio di informazioni, appoggiandosi possibilmente su organismi esistenti come il gruppo europeo governativo CERT (gruppo EGC) [24].

3.4.4. Cooperazione internazionale

Tra le infrastrutture critiche informatizzate, internet ha assunto una tale importanza da richiedere un'attenzione particolare quanto alla sua resilienza e stabilità. Data la sua configurazione distribuita e ridondante l'infrastruttura di internet si è rivelata molto robusta. Ma la sua crescita fenomenale ha prodotto una crescente complessità fisica e logica e l'apparizione di nuovi servizi e usi: è quindi legittimo interrogarsi sulla capacità di internet di resistere al numero crescente di ciberperturbazioni e ciberattacchi.

La divergenza di opinioni sulle criticità degli elementi che compongono internet spiega in parte la diversità delle posizioni governative espresse nelle sedi internazionali e la percezione spesso contraddittoria dell'importanza di questa problematica. Tutto questo può ostacolare la corretta prevenzione, il processo di preparazione e la capacità di riprendersi dalle minacce di cui può essere vittima internet. Ad esempio, occorrerebbe valutare le conseguenze del passaggio dal protocollo IPv4 al protocollo IPv6 sotto il profilo della sicurezza delle infrastrutture critiche informatizzate.

Internet è una rete di reti globale e diffusamente distribuita, i cui centri di controllo non rispettano necessariamente i confini nazionali. È perciò necessario un approccio speciale e mirato per garantirne la resilienza e la stabilità attraverso due misure convergenti. Innanzitutto occorre pervenire a un consenso sulle priorità europee in materia di resilienza e stabilità di internet, in termini di politica pubblica e di uso operativo. In secondo luogo occorre fare in modo che la comunità globale elabori una serie di principi, che riflettano i valori centrali europei, in materia di resilienza e stabilità di internet, nell'ambito del nostro dialogo e della nostra collaborazione con i paesi terzi e le organizzazioni internazionali. Queste attività prenderanno le mosse dal riconoscimento dell'importanza fondamentale attribuita alla stabilità di internet dal Vertice mondiale sulla società dell'informazione[25].

---

23 http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

24 http://www.egc-group.org/

25 Agenda di Tunisi per la società dell'informazione, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

4. LA PROSSIMA TAPPA: VERSO UNA MAGGIORE COOPERAZIONE E UN MAGGIORE COORDINAMENTO A LIVELLO UE

La dimensione comunitaria e internazionale del problema richiede un approccio integrato a livello UE per rafforzare la sicurezza e la resilienza delle infrastrutture critiche informatizzate, che completi e dia valore aggiunto ai programmi nazionali e ai regimi bilaterali e multilaterali di cooperazione esistenti tra gli Stati membri.

Dai dibattiti sulle politiche pubbliche che hanno fatto seguito agli attacchi di cui è stata vittima l'Estonia è emerso che gli effetti di simili attacchi si possono contrastare con misure preventive e attraverso l'azione coordinata durante la crisi vera e propria. Uno scambio di informazioni e buone pratiche più strutturato in tutta l'Unione europea permetterebbe di facilitare considerevolmente la lotta internazionale contro questo tipo di minacce.

È necessario rafforzare gli strumenti di cooperazione esistenti, incluso il ruolo dell'ENISA, e se necessario crearne di nuovi. È essenziale un approccio corale, che coinvolga un gran numero di parti in causa e a vari livelli, da attuare su scala europea pur se nel pieno rispetto delle competenze nazionali e a loro complemento.

È necessaria una profonda comprensione del contesto e dei vincoli in cui operare: ad esempio, la configurazione distribuita di internet nella quale i nodi periferici possono essere usati come vettori di attacchi (come le reti di bot) desta preoccupazioni. Ma questa configurazione distribuita è nello stesso tempo una componente chiave della stabilità e della resilienza di internet e può contribuire a un recupero più rapido che in presenza di procedure di tipo discendente ed eccessivamente formalizzate. Occorre però procedere ad un'analisi cauta, caso per caso, delle politiche pubbliche e delle procedure operative da mettere in atto.

Anche il calendario è importante: è evidente che occorre agire subito e mettere in essere rapidamente gli elementi necessari per creare un quadro che dia modo di rispondere alle sfide attuali e che confluirà nella strategia futura della sicurezza delle reti e dell'informazione.

Per contrastare questi problemi si propongono i cinque assi d'azione seguenti:

(1) preparazione e prevenzione, per tenersi pronti a tutti i livelli;

(2) individuazione e reazione, per dotarsi di meccanismi adeguati di allarme rapido;

(3) mitigazione e recupero, per rafforzare i meccanismi europei di difesa delle infrastrutture critiche informatizzate;

(4) cooperazione internazionale, per promuovere le priorità UE a livello internazionale;

(5) criteri per il settore delle TIC, per sostenere l'attuazione della direttiva relativa all'individuazione e alla designazione delle infrastrutture critiche europee[26].

[26] Direttiva 2008/114/CE del Consiglio.

5. IL PIANO D'AZIONE

5.1. Preparazione e prevenzione

Base comune di capacità e servizi per la cooperazione paneuropea. La Commissione invita gli Stati membri e le parti interessate a

- definire, con il sostegno dell'ENISA, un livello minimo di capacità e servizi per i gruppi nazionali o governativi di pronto intervento informatico (CERT) e per operazioni di reazione in caso di incidenti, a supporto della cooperazione paneuropea;

- attribuire ai gruppi CERT nazionali o governativi un ruolo chiave nella capacità nazionale di preparazione, scambio di informazioni, coordinamento e reazione.

Obiettivo: entro la fine del 2010 per la definizione di norme comuni e entro la fine del 2011 per la costituzione di gruppi nazionali o governativi di pronto intervento informatico ben rodati in tutti gli Stati membri.

Partenariati pubblico-privati europei per la resilienza. La Commissione:

- incoraggerà la cooperazione tra il settore pubblico e privato in materia di obiettivi di sicurezza e resilienza, di requisiti di base e di adozione di buone pratiche politiche e misure adeguate. L'obiettivo primario di questo tipo di partenariato europeo sarà la dimensione europea vista secondo una prospettiva strategica (buone pratiche politiche) e tattico-operativa (adozione industriale). Il partenariato europeo dovrebbe basarsi sulle iniziative nazionali esistenti e sulle attività operative della ENISA e completarle.

Obiettivo: entro la fine del 2009 per stabilire una tabella di marcia ed un piano per il partenariato europeo, entro la prima metà del 2010 per la costituzione del partenariato europeo e entro la fine del 2010 perché il partenariato europeo produca i suoi primi risultati.

Forum europeo di condivisione di informazioni tra gli Stati membri. La Commissione:

- istituirà 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. Confluiranno nel forum anche i risultati delle attività di altri organismi, come l'ENISA.

Obiettivo: entro la fine del 2009 per lanciare il forum e entro la fine del 2010 per i primi risultati.

5.2. Individuazione e risposta

Sistema europeo di condivisione delle informazioni e di allarme. La Commissione sostiene

l'elaborazione e l'adozione di un sistema europeo di condivisione delle informazioni e di allarme (EISAS), destinato a tutti cittadini e alle PMI, basato sui sistemi nazionali e privati di condivisione di informazioni e di allarme. La Commissione sostiene finanziariamente due

progetti prototipi complementari[27]. L'ENISA è invitata valutare i risultati di questi progetti e di altre iniziative nazionali e a elaborare una tabella di marcia per l'ulteriore sviluppo e adozione di sistemi europei di condivisione di informazioni e di allarme.

Obiettivo: entro la fine del 2010 per portare a termine progetti prototipo e entro la fine del 2010 per la tabella di marcia per l'istituzione del sistema europeo.

5.3. Mitigazione e recupero

Piani di emergenza ed esercitazioni nazionali La Commissione invita gli Stati membri a

- elaborare piani di emergenza nazionali e organizzare esercitazioni periodiche sulla reazione a incidenti gravi e diffusi a danno della sicurezza delle reti e sul recupero dopo il disastro, per contribuire a rafforzare il coordinamento paneuropeo. Si potrebbero incaricare i gruppi nazionali o governativi di pronto intervento informatico di condurre esercitazioni sui piani di emergenza e di testarli a livello nazionale, con la partecipazione delle parti interessate del settore pubblico e del settore privato. Si caldeggia il coinvolgimento dell'ENISA per sostenere lo scambio di buone pratiche tra gli Stati membri.

Obiettivo: entro la fine del 2010 per l'esecuzione di almeno un'esercitazione nazionale in ogni Stato membro.

Esercitazioni paneuropee su incidenti gravi e diffusi a danno della sicurezza delle reti. La Commissione:

- contribuirà finanziariamente alla realizzazione di esercitazioni paneuropee sugli incidenti a danno della sicurezza di internet[28], che potrebbero anche costituire una piattaforma operativa per la partecipazione europea ad esercitazioni internazionali su incidenti a danno della sicurezza delle reti, come Cyber Storm negli Stati Uniti.

Obiettivo: entro la fine del 2010 per l'elaborazione e la conduzione della prima esercitazione paneuropea; entro la fine del 2010 per la partecipazione paneuropea ad esercitazioni internazionali.

Cooperazione rafforzata tra i gruppi nazionali o governativi di pronto intervento informatico (CERT). La Commissione invita gli Stati membri a

- rafforzare la cooperazione tra i gruppi nazionali o governativi CERT utilizzando e ampliando i meccanismi di cooperazione esistenti come l'EGC (gruppo dei CERT governativi europei)[29]. Si invita l'ENISA a svolgere un ruolo attivo per incoraggiare e sostenere la collaborazione paneuropea tra i CERT nazionali o governativi, che dovrebbe tradursi in una preparazione migliore, in una maggiore capacità dell'Europa di reagire in caso di incidenti e nella realizzazione di esercitazioni paneuropee (e/o regionali).

---

27 Nell'ambito del programma CE "*Prevenzione, preparazione e gestione delle conseguenze di atti di terrorismo e di altri rischi connessi alla sicurezza*". http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

28 Supra 27.

29 Supra 24.

Obiettivo: entro la fine del 2010 per raddoppiare il numero di enti nazionali che partecipano al gruppo EGC e entro la fine del 2010 perché l'ENISA elabori materiale di riferimento per sostenere la collaborazione paneuropea.

5.4. Cooperazione internazionale

Stabilità e resilienza di internet. Sono previste le tre seguenti attività complementari:

- Priorità europee per la stabilità e la resilienza di internet a lungo termine La Commissione darà vita a un dibattito su scala europea a cui parteciperanno tutte le parti interessate, pubbliche e private, per definire le priorità europee della stabilità e della resilienza di internet a lungo termine.

Obiettivo: entro la fine del 2010 per stabilire le priorità europee sugli aspetti e sulle componenti critiche di internet.

- Principi e orientamenti per la stabilità e la resilienza di internet (a livello europeo). La Commissione collaborerà con gli Stati membri per definire orientamenti per la resilienza e la stabilità di internet, concentrandosi tra l'altro su interventi correttivi regionali, su accordi di mutua assistenza, su strategie coordinate di recupero e di continuità, sulla distribuzione geografica delle risorse critiche di internet, sulle precauzioni tecnologiche nell'architettura e nei protocolli di internet, sulla replicazione e la diversità dei servizi e dei dati. La Commissione sta già fondando una task force per la resilienza dei sistemi dei nomi di dominio di internet (DNS) che, insieme ad altri progetti e rilevanti servirà a rafforzare il consenso[30].

Obiettivo: entro la fine del 2009 per definire una tabella di marcia europea per l'elaborazione di principi e orientamenti in materia di stabilità e resilienza di internet e entro la fine del 2010 per l'adozione del primo progetto di tali principi e orientamenti.

- Principi e orientamenti per la stabilità e la resilienza di internet (a livello globale). La Commissione collaborerà con gli Stati membri all'elaborazione di una tabella di marcia per promuovere l'adozione di principi e orientamenti a livello globale. Sarà sviluppata la cooperazione strategica con i paesi terzi in particolare nell'ambito di dialoghi sulla società dell'informazione come mezzo per costruire un consenso globale[31].

Obiettivo: inizio del 2010 per definire una tabella di marcia della cooperazione internazionale su principi e orientamenti in materia di sicurezza e resilienza; fine del 2010 per la discussione del primo progetto di principi e orientamenti riconosciuti a livello internazionale con i paesi terzi e nelle sedi appropriate, come ad esempio l'Internet Governance Forum.

Esercitazione globale in materia di recupero e attenuazione degli incidenti gravi e diffusi a danno di internet. La Commissione invita le parti europee interessate a

- riflettere sul modo pratico di estendere alla scala globale le esercitazioni in atto in materia di attenuazione e recupero, basandosi sui piani di emergenza e sulle capacità regionali.

---

30 Supra 27.

31 COM(2008) 588 definitivo.

Obiettivo: entro la fine del 2010 perché la Commissione proponga un quadro e una tabella di marcia per sostenere il coinvolgimento e la partecipazione europea ad esercitazioni globali sul recupero e l'attenuazione degli incidenti gravi a danno di internet.

5.5. Criteri per le infrastrutture critiche europee nel settore delle TIC

Criteri specifici per il settore delle TIC. Basandosi sull'attività iniziale svolta nel 2008 la Commissione

- continuerà a elaborare, in collaborazione con gli Stati membri e tutte le parti interessate, i criteri per individuare le infrastrutture critiche europee del settore delle TIC. A tal fine le informazioni pertinenti saranno tratte da uno studio specifico appena avviato[32].

Obiettivo: prima metà del 2010 perché la Commissione definisca i criteri delle infrastrutture critiche europee per il settore delle TIC.

6. CONCLUSIONI

La sicurezza e la resilienza delle infrastrutture critiche informatizzate costituiscono il fronte di difesa nei confronti di ciberattacchi e ciberperturbazioni: per questo motivo, è essenziale rafforzarle in tutta l'Unione europea se si vuole trarre i massimi benefici dalla società dell'informazione. Per conseguire questo obiettivo ambizioso si propone di attuare un piano d'azione per rafforzare la cooperazione operativa e tattica a livello europeo. Il successo di queste azioni dipende non solo dalla loro capacità di rafforzare le attività dei settori pubblico e privato, per il loro vantaggio reciproco, ma anche dall'impegno e dalla piena partecipazione degli Stati membri, delle istituzioni europee e delle parti interessate.

A tal fine il 27-28 aprile 2009 si terrà una Conferenza ministeriale per discutere le iniziative proposte con gli Stati membri e per ottenere il loro contributo al dibattito su una politica per la sicurezza delle reti e dell'informazione in Europa più moderna e più forte.

Da ultimo, il rafforzamento della sicurezza e della resilienza delle infrastrutture critiche informatizzate è un obiettivo a lungo termine, la cui strategia e i cui provvedimenti richiedono valutazioni periodiche. Per questo, dato che l'obiettivo è coerente con il dibattito generale in atto sul futuro della politica di sicurezza delle reti e dell'informazione dell'UE dopo il 2012, la Commissione comincerà a fare il punto della situazione alla fine del 2010 per valutare la prima serie di azioni e individuare e proporre ulteriori misure, se del caso.

[32] Supra 27.