COMMISSIONE EUROPEA

Bruxelles, 31.3.2011
COM(2011) 163 definitivo

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

relativa alla protezione delle infrastrutture critiche informatizzate

"Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"

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

relativa alla protezione delle infrastrutture critiche informatizzate

"Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"

1. INTRODUZIONE

Il 30 marzo 2009 la Commissione ha pubblicato una comunicazione sulla protezione delle infrastrutture critiche informatizzate – "Rafforzare la preparazione,la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni[1] che prevede un piano d'azione (il "piano d'azione CIIP") destinato a rafforzare la preparazione e la resilienza delle infrastrutture TIC fondamentali. Scopo di tale comunicazione era incentivare e sostenere lo sviluppo, sia a livello europeo che a livello nazionale, di un elevato livello di preparazione, sicurezza e capacità di resilienza. Questo approccio è stato ampiamente sostenuto dal Consiglio nel 2009[2].

Il piano d'azione CIIP si basa su cinque pilastri: preparazione e prevenzione, individuazione e risposta, mitigazione e recupero, cooperazione internazionale e criteri per le infrastrutture critiche europee nel settore delle TIC. Stabilisce il lavoro che la Commissione, gli Stati membri e/o il settore industriale devono realizzare nell'ambito di ogni pilastro, con l'aiuto dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

L'Agenda digitale europea[3], adottata nel maggio 2010, e le relative conclusioni del Consiglio[4], riflettono la convinzione comune che la fiducia e la sicurezza sono condizioni fondamentali per un'ampia diffusione delle TIC e dunque per il conseguimento degli obiettivi della dimensione di "crescita intelligente" della strategia Europa 2020[5]. L'Agenda digitale europea sottolinea la necessità per tutte le parti interessate di unire le forze in un impegno globale per rafforzare la sicurezza e la resilienza delle infrastrutture TIC, incentrando il loro intervento sulla prevenzione, la preparazione e la sensibilizzazione e per istituire meccanismi efficaci e coordinati per rispondere a nuove forme di attacchi e di criminalità informatici sempre più sofisticati. Questo approccio consente di garantire che, alle prese con queste sfida, si terrà adeguatamente conto sia dell'aspetto "prevenzione" sia dell'aspetto "reazione".

Nei mesi precedenti, come annunciato nell'Agenda digitale, sono state adottate le misure seguenti: nel settembre 2010 la Commissione ha adottato una proposta di direttiva relativa agli attacchi contro i sistemi di informazione[6] che mira a rafforzare la lotta contro la criminalità informatica mediante il ravvicinamento delle legislazioni penali degli Stati

---

1 COM(2009) 149.

2 Risoluzione del Consiglio, del 18 dicembre 2009, su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione (2009/C-321/01).

3 COM(2010) 245.

4 Conclusioni del Consiglio del 31 maggio 2010 su un'Agenda digitale europea (10130/10).

5 COM(2010) 2020 e Conclusioni del Consiglio europeo del 25 e 26 marzo 2010 (EUCO 7/10).

6 COM(2010) 517 definitivo.

membri e migliorando la cooperazione tra autorità giudiziarie e altre autorità competenti. Tale proposta introduce inoltre disposizioni che consentono di far fronte a nuovi tipi di attacchi informatici, in particolare le offensive da "botnet". Ad integrazione di questo testo, la Commissione ha presentato nel contempo una proposta[7] relativa ad un nuovo mandato per rafforzare ed ammodernare l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) al fine di rafforzare la fiducia e la sicurezza delle reti. Il rafforzamento e la modernizzazione dell'ENISA aiuteranno anche l'Unione europea, gli Stati membri e i partner privati a sviluppare le loro capacità e il loro grado di preparazione nel prevenire, individuare e combattere i problemi di sicurezza informatica.

L'Agenda digitale europea, il piano d'azione per l'attuazione del programma di Stoccolma[8] e la strategia di sicurezza interna dell'UE in azione[9] rispecchiano l'impegno della Commissione a costruire un ambiente digitale in cui tutti i cittadini europei possano esprimere il proprio potenziale economico e sociale.

La presente comunicazione riepiloga i risultati ottenuti dall'adozione del piano d'azione CIIP nel 2009. Descrive le prossime tappe previste per ogni azione sia a livello europeo che internazionale. Si sofferma inoltre sulla dimensione mondiale delle sfide e sull'importanza di un rafforzamento della cooperazione tra gli Stati membri e il settore privato a livello nazionale, europeo e internazionale, in modo da affrontare le questioni di interdipendenza a livello mondiale.

2. SCENARIO IN EVOLUZIONE

La valutazione di impatto che accompagna il piano d'azione CIIP[10] e numerosi analisi e studi effettuati da parti interessate private e pubbliche pongono in evidenza non solo la dipendenza sociale, economica e politica dell'Europa dalle TIC, ma anche l'aumento costante del numero, della portata, della sofisticazione e dell'impatto potenziale delle minacce – sia naturali che causate dall'uomo.

Sono emerse minacce nuove e più sofisticate dal punto di vista tecnologico la cui dimensione geopolitica globale sta diventando sempre più chiara. Si delinea attualmente la tendenza ad utilizzare le TIC per ottenere l'egemonia politica, economica e militare, anche avvalendosi delle capacità offensive. La "guerra informatica" o il "terrorismo informatico" sono menzionati a volte in questo contesto.

Inoltre, come lo dimostrano i recenti avvenimenti nel sud del Mediterraneo, alcuni regimi sono pronti, a scopo politico, a interrompere o a privare arbitrariamente l'accesso della loro popolazione ai mezzi di comunicazione elettronici (come internet e le comunicazioni mobili) e sono in grado di farlo. Questi interventi nazionali unilaterali possono avere serie ripercussioni in altre parti del mondo[11].

---

7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.
11 Comunicazione congiunta su un partenariato per la democrazia e la prosperità condivisa con il Mediterraneo meridionale, COM(2011) 200 dell'8.3.2011.

Per disporre di un quadro più chiaro delle diverse minacce, può essere utile suddividerle nelle categorie seguenti:

– finalità di **sfruttamento**, come le "minacce persistenti avanzate"[12] a fini di spionaggio economico e politico (GhostNet[13], ad esempio), i furti di identità, i recenti attacchi contro il sistema di scambio dei diritti di emissioni[14] o contro sistemi informatici delle autorità pubbliche[15];

– finalità di **perturbazione**, come attacchi di interruzione del servizio con origine da più fonti (*Distribution Denial of Service*) o lo spamming mediante botnet (ad esempio la rete Conficker che ha coinvolto 7 milioni di macchine e la rete Mariposa in Spagna che ne ha coinvolto 12,7 milioni[16]), Stuxnet[17] e l'interruzione dei mezzi di comunicazione;

– **finalità** di distruzione. Questo scenario non si è ancora concretizzato ma, vista la diffusione sempre più ampia delle TIC nelle infrastrutture critiche (reti elettriche e sistemi idrici intelligenti), non si può escludere per il futuro[18].

3. L'UNIONE EUROPEA E IL CONTESTO MONDIALE

Le sfide che si profilano non riguardano esclusivamente l'Unione europea (UE) e quest'ultima non potrà affrontarle da sola. L'onnipresenza delle TIC e di internet consente di rendere la comunicazione, il coordinamento e la cooperazione tra parti interessate più efficaci e più economici e favorisce lo sviluppo di un ecosistema dell'innovazione dinamico in tutti i settori. Le minacce, ormai, possono provenire da qualsiasi luogo del mondo e, visto che il mondo intero è interconnesso, colpire qualsiasi luogo del mondo.

Per affrontare queste problematiche non basta un approccio puramente europeo. L'obiettivo di istituire un approccio coerente e cooperativo in seno all'UE rimane di primaria importanza ma deve iscriversi in una strategia di coordinamento mondiale esteso ai principali partner, sia che si tratti di nazioni o di organizzazioni internazionali interessate da questi problemi.

Dobbiamo lavorare a favore di una comprensione globale dei rischi inerenti all'utilizzo massiccio e generalizzato delle TIC da tutti i settori della società. Dobbiamo inoltre concepire strategie per gestire in modo adeguato e appropriato questi rischi tramite la prevenzione, il contrasto, l'attenuazione e la reazione. L'Agenda digitale europea afferma che "*occorre organizzare a livello mondiale la cooperazione tra gli attori più importanti, in modo da lottare in maniera efficace contro le minacce alla sicurezza e contenerle*" e fissa l'obiettivo di "*collaborare con le parti interessate a livello mondiale, in particolare per rafforzare una*

---

12 Ossia, attacchi continui e coordinati contro le agenzie governative e il settore pubblico. Sta diventando un vero problema per il settore pubblico (vedi "RSA 2011 cybercrime trends report").

13 Vedi le relazioni nell'ambito del progetto "Information Warfare Monitor: Tracking GhostNet: investigating a Cyber Espionage Network" (2009) e "Shadows in the Cloud: Investigating Cyber Espionage 2.0" (2010).

14 Vedi domande e risposte http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr

15 Ad esempio i recenti attacchi contro il governo francese.

16 Vedi il progetto OCSE/IFP "Future Global Shocks", "Reducing systemic cyber-security risks", del 14 gennaio 2011 http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Vedi http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis

18 Vedi World Economic Forum, Global Risks 2011.

gestione globale dei rischi *sia nel mondo fisico che in quello digitale e promuovere azioni mirate, coordinate a livello internazionale, contro la criminalità informatica e gli attacchi contro la sicurezza".*

4. ATTUAZIONE DEL PIANO D'AZIONE CIIP: ALCUNI ELEMENTI IMPORTANTI

In allegato figura la relazione completa sulle realizzazioni e le tappe future del piano d'azione CIIP. Qui di seguito sono illustrati alcuni elementi fondamentali relativi alla situazione attuale.

4.1. Preparazione e prevenzione

- Il **Forum europeo degli Stati membri** (EFMS) ha contribuito in modo significativo alla promozione delle discussioni e degli scambi tra autorità competenti sulle buone pratiche in materia di sicurezza e resilienza delle infrastrutture TIC. Gli Stati membri considerano l'EFMS una piattaforma importante per il dialogo e lo scambio di buone pratiche[19]. Le sue future attività continueranno a beneficiare del sostegno dell'ENISA e riguarderanno la cooperazione tra le squadre di pronto intervento informatico (CERT) nazionali/governative, la definizione di incentivi di natura economica e regolamentare, a favore della sicurezza e della resilienza (nel rispetto delle regole applicabili nel settore della concorrenza e degli aiuti di Stato), la valutazione della situazione della sicurezza informatica in Europa, l'organizzazione di esercitazioni paneuropee nonché l'esame delle priorità da trattare in un quadro internazionale in materia di sicurezza e resilienza.

- Il **Partenariato pubblico-privato europeo per la resilienza** (EP3R) costituisce un quadro di *governance* europeo per la resilienza delle infrastrutture TIC che mira ad incentivare la cooperazione tra il settore pubblico e il settore privato su questioni strategiche della politica dell'UE in materia di sicurezza e resilienza. L'ENISA ha svolto un ruolo di sostegno per le attività dell'EP3R e, conformemente alla proposta della Commissione del 2010 relativa alla modernizzazione dell'ENISA, fornirebbe un quadro sostenibile e di lungo termine per l'EP3R. L'EP3R fungerebbe anche da piattaforma di portata internazionale per le questioni attinenti alla politica pubblica, all'economia e ai mercati rilevanti dal punto di vista della sicurezza e della resilienza, in particolare per rafforzare la gestione mondiale dei rischi nel settore delle infrastrutture TIC.

- Sono stati elaborati l'**insieme minimo di capacità e servizi di base**[20] e le relative **raccomandazioni strategiche**[21] per le squadre di pronto intervento informatico (CERT) nazionali o governative affinché possano operare efficacemente e fungere da elemento principale della capacità nazionale in termini di preparazione, condivisione delle informazioni, coordinamento e reazione. Su questa base entro il 2012 si potrà istituire, con il sostegno dell'ENISA, una rete di CERT nazionali/governative operative in tutti gli Stati membri. Questa rete sarà la pietra angolare di un sistema europeo di condivisione delle

---

19 Nella sua risposta alla quinta relazione del comitato sull'Unione europea della Camera dei Lord concernente il piano d'azione CIIP, il governo britannico ha dichiarato che il Forum europeo degli Stati membri è un'iniziativa coronata da successo che risponde ad un'effettiva esigenza fornendo ai responsabili politici un quadro nel quale condividere le proprie esperienze.

20 Vedi http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Vedi http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

informazioni e di allarme (EISAS) per i cittadini e le PMI, da costruire con le risorse e le capacità nazionali entro il 2013.

4.2. Individuazione e risposta

- L'ENISA ha stabilito una tabella di marcia di alto livello per promuovere entro il 2013 lo sviluppo di un sistema europeo di condivisione delle informazioni e di allarme (**EISAS)**[22] fondato sull'attuazione di *servizi di base* a livello delle CERT nazionali/governative e di *servizi di interoperabilità* in vista dell'integrazione dei sistemi nazionali di condivisione delle informazioni e di allarme nell'EISAS. Uno degli elementi chiave di questa attività sarà l'adeguata protezione dei dati personali.

4.3. Mitigazione e recupero

- Finora solo 12 Stati membri hanno organizzato esercitazioni riguardanti la reazione in caso di incidenti su larga scala e il ripristino[23]. L'ENISA ha pubblicato **una guida di buone pratiche per le esercitazioni a livello nazionale**[24] e **raccomandazioni strategiche** per lo sviluppo di strategie nazionali[25] al fine di sostenere le attività degli Stati membri che dovrebbero essere intensificate.

- La prima **esercitazione paneuropea relativa ad incidenti di ampia portata che incidono sulla sicurezza delle reti** (Cyber Europe 2010) si è svolta il 4 novembre 2010 con la partecipazione di tutti gli Stati membri, 19 dei quali hanno preso parte attivamente all'esercitazione, e della Svizzera, della Norvegia e dell'Islanda. Sarebbe indubbiamente opportuno che le future esercitazioni paneuropee si inserissero in un quadro comune fondato sui piani di emergenza nazionali e operante in interazione con questi ultimi, in modo da fornire meccanismi e procedure di base per le comunicazioni e la cooperazione tra Stati membri.

4.4. Cooperazione internazionale

- Nell'ambito dell'EFMS sono stati discussi ed elaborati **principi e orientamenti europei per la resilienza e la stabilità di internet**[26]. La Commissione esaminerà e promuoverà questi principi con le parti interessate, in particolare nel settore privato (mediante l'EP3R), bilateralmente con importanti partner internazionali, in particolare gli Stati Uniti, ma anche a livello multilaterale. Svolgerà queste attività, nel limite delle sue competenze, in sedi quali il G8, l'OCSE, la NATO (in particolare sulla base del suo nuovo concetto strategico adottato nel novembre 2010 e delle attività del Centro di eccellenza per la difesa informatica in cooperazione), l'UIT (nell'ambito del rafforzamento delle capacità nel settore della sicurezza informatica), l'OCSE (tramite il suo Forum per la cooperazione in materia di sicurezza), l'ASEAN, Meridian[27] ecc. L'obiettivo è trasformare questi principi e

---

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Fonte: ENISA.

24 Vedi http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Vedi http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

26 Vedi http://ec.europa.eu/information_society/policy/nis/index_en.htm

27 L'iniziativa Meridian mira a fornire ai governi del mondo intero uno strumento per discutere sulle modalità di una collaborazione a livello strategico in materia di protezione delle infrastrutture di informazione critiche (CIIP). Vedi http://meridianprocess.org/

linee guida in un quadro comune per un impegno collettivo internazionale sulla resilienza e la stabilità a lungo termine di internet.

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

- Le discussioni tecniche in seno al Forum europeo degli Stati membri hanno condotto ad **una prima versione dei criteri specifici del settore delle TIC** per individuare le infrastrutture critiche europee, che pone un accento particolare sulle **comunicazioni fisse e mobili e su Internet.** Le discussioni tecniche, che proseguiranno, beneficeranno del contributo delle consultazioni nazionali ed europee con il settore privato (tramite EP3R) sulla prima versione dei criteri. La Commissione esaminerà inoltre con gli Stati membri gli elementi specifici del settore delle TIC di cui tenere conto per il riesame della direttiva relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione nel 2012[28].

5. FASI SUCCESSIVE

Nell'ambito dell'attuazione del piano CIIP si sono già registrati risultati positivi, in particolare il riconoscimento dell'esigenza di adottare un approccio cooperativo nella sicurezza delle reti e dell'informazione che coinvolga tutte le parti interessate. L'attuazione del piano d'azione inoltre rispetta, almeno a grandi linee, le tappe e il calendario stabiliti nel 2009. Tuttavia non dovremmo riposarci sugli allori in quanto resta ancora molto da fare a livello nazionale ed europeo affinché gli sforzi profusi diano dei frutti.

Occorre inoltre inserire questi sforzi in una strategia mondiale di coordinamento e dunque dar loro una dimensione internazionale, con tutti i partner interessati, per coinvolgere altre regioni, nazioni o organizzazioni alle prese con problemi analoghi, e istituire partenariati al fine di condividere le strategie e le attività associate ed evitare la duplicazione degli sforzi.

Dobbiamo promuovere una cultura mondiale della gestione dei rischi incentrata su azioni coordinate destinate a prevenire, individuare e attenuare tutte le forme di perturbazione, naturali o causate dall'uomo, e ad apportarvi una risposta, ma anche a perseguire i reati informatici. A tal fine, occorrerà portare avanti azioni mirate per lottare contro le minacce che gravano sulla sicurezza informatica e contro la criminalità informatica.

A tal fine la **Commissione intende**:

- **promuovere principi per la resilienza e la stabilità di internet** – Sarebbe opportuno elaborare, in concertazione con altri paesi, organizzazioni internazionali e, se del caso, con organismi privati di dimensione mondiale, principi internazionali per la resilienza e la stabilità di internet. A tal fine ci si potrebbe avvalere di consessi e di meccanismi esistenti, come quelli legati alla *governance* di internet. Questi principi dovrebbero fungere da quadro di riferimento per tutte le attività delle parti interessate in materia di stabilità e resilienza di internet. In questo senso, i principi e le linee guida europee potrebbero fungere da base.

- **istituire partenariati strategici di dimensione internazionale –** Sarebbe opportuno fondare partenariati strategici sulle attività in corso in settori critici, come la gestione degli

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

incidenti informatici, ivi comprese le esercitazioni e le misure di cooperazione tra CERT. Il coinvolgimento del settore privato che opera a livello mondiale è di fondamentale importanza. La creazione, in occasione del vertice UE-USA di novembre 2010, di un gruppo di lavoro congiunto UE-USA sulla sicurezza e la criminalità informatiche costituisce un passo importante in questa direzione. L'attività di questo gruppo si incentrerà sulla gestione degli incidenti informatici, i partenariati pubblico-privato, la sensibilizzazione e la criminalità informatica. Potrà inoltre considerare la possibilità di coinvolgere altri paesi o regioni alle prese con problemi analoghi al fine, se del caso, di condividere le strategie adottate e le relative attività o di evitare inutili doppioni. Occorre continuare a sviluppare le azioni realizzate e il coordinamento in consessi internazionali, in particolare nell'ambito del G8. In Europa il principale fattore di successo sarà un adeguato coordinamento tra tutte le istituzioni dell'Unione, gli organismi interessati (in particolare l'ENISA ed Europol) e gli Stati membri;

- **rafforzare la fiducia nel cloud computing (**"**nuvola informatica**") – Occorre assolutamente intensificare le discussioni sule migliori strategie di *governance* per le tecnologie emergenti che hanno un impatto mondiale, come la nuvola informatica. Queste discussioni dovrebbero indubbiamente riguardare anche il quadro di *governance* adeguato per la protezione dei dati personali. La fiducia è indispensabile per trarre il massimo beneficio da questa realtà[29].

Tutti siamo responsabili della sicurezza, pertanto tutti gli Stati membri devono assicurarsi che le misure adottate e gli sforzi profusi contribuiscano collettivamente ad un approccio europeo coordinato destinato a prevenire, individuare e attenuare tutte le forme di perturbazioni e attacchi informatici e ad apportarvi una risposta. A questo proposito, **gli Stati membri dovrebbero impegnarsi a**:

- **rafforzare la preparazione dell'UE istituendo una rete di CERT nazionali/governative operative entro la fine del 2012.** Da parte loro, le istituzioni dell'UE istituiranno anch'esse una CERT a loro livello entro il 2012. Tutti questi sforzi dovrebbero basarsi sulla base minima di capacità e servizi e sulle raccomandazioni strategiche ad essi associati elaborate dall'ENISA, che continuerà ad apportare il proprio sostegno a queste raccomandazioni. Queste attività contribuiranno all'istituzione, entro il 2013, di un sistema europeo di condivisione delle informazioni e di allarme (EISAS) per il grande pubblico;

- **elaborare un piano di emergenza europeo in caso di incidenti informatici e organizzare esercitazioni paneuropee periodiche nel settore della sicurezza informatica entro il 2012.** Le esercitazioni sono un elemento essenziale di una strategia coerente per un piano di emergenza europeo in caso di incidenti informatici e di recupero, sia a livello nazionale che europeo. La future esercitazioni paneuropee dovrebbero essere varate sulla base di un piano di emergenza europeo in caso di incidenti informatici che si basi e si colleghi ai piani di emergenza nazionali. Questo piano dovrebbe fornire i meccanismi e le procedure di base per la comunicazione tra Stati membri nonché un sostegno per definire la portata delle future esercitazioni paneuropee e per organizzarle.

---

[29] Cfr. ad esempio le relazioni dell'ENISA "Cloud Computing Information Assurance Framework" (2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) e "Security and resilience in governmental clouds" (2011), http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

L'ENISA collaborerà con gli Stati membri affinché questo piano di emergenza europeo in caso di incidenti informatici sia elaborato entro il 2012. Per questa stessa data tutti gli Stati membri dovrebbero istituire piani di emergenza nazionali e esercitazioni periodiche di reazione e ripristino;

- **realizzare sforzi coordinati a livello europeo nell'ambito di consessi internazionali ed avviare discussioni sul rafforzamento della sicurezza e della resilienza di internet.** Gli Stati membri dovrebbero cooperare tra loro e con la Commissione per promuovere lo sviluppo di un approccio fondato su principi o norme sulla questione della stabilità e della resilienza mondiali di internet. L'obiettivo dovrebbe essere la promozione delle prevenzione e della preparazione a tutti i livelli e presso tutte le parti interessate, riequilibrando in questo modo la tendenza attuale ad incentrare le discussioni sugli aspetti militari o di sicurezza nazionale.

6. CONCLUSIONE

L'esperienza dimostra che applicare approcci strettamente nazionali o regionali per affrontare i problemi di sicurezza e resilienza non basta. La cooperazione europea si è considerevolmente sviluppata dal 2009 e i risultati ottenuti sono incoraggianti, in particolare nell'ambito dell'esercitazione "Cyber Europe 2010". L'Europa dovrebbe comunque perseverare nei suoi sforzi destinati per istituire un approccio coerente e cooperativo nell'insieme dell'UE. Una volta modernizzata, l'ENISA dovrebbe rafforzare il sostegno che apporta agli Stati membri, alle istituzioni dell'UE e al settore privato in questa impresa a lungo termine.

Per essere efficaci, gli sforzi europei devono inserirsi in un approccio coordinato a livello mondiale. A tal fine, la Commissione promuoverà, in tutte le appropriate sedi internazionali, dibattiti sulla sicurezza informatica.

Organizzata dalla presidenza ungherese dell'UE, il 14 e 15 aprile 2011 si svolgerà una conferenza ministeriale CIIP. Questa riunione costituirà un'ottima occasione per ribadire l'impegno a favore di un coordinamento e una cooperazione rafforzati tra gli Stati membri, a livello europeo e internazionale.

ALLEGATO

Piano d'azione CIIP: presentazione dettagliata delle realizzazioni e tappe future

I risultati delle attività svolte nell'ambito del piano d'azione CIIP corrispondono in linea di massima al calendario e alle tappe fissati dalla Commissione nel 2009. Nei paragrafi seguenti sono descritte le "realizzazioni" e le "tappe future" per tutti gli assi. Questo quadro della situazione tiene conto del fatto che alcune attività sono state ulteriormente elaborate nell'ambito dell'Agenda digitale europea e della Strategia di sicurezza interna dell'UE in azione.

1. **Preparazione e prevenzione**

Base comune di capacità e servizi per la cooperazione paneuropea

Realizzazioni

– Nel 2009 l'ENISA e la comunità delle squadre di pronto intervento informatico (CERT) dell'UE hanno stabilito e approvato una base minima di capacità e di servizi che le CERT nazionali/governative devono possedere per operare adeguatamente a sostegno della cooperazione paneuropea. Si è raggiunto un consenso su un elenco di requisiti "essenziali" nei settori del funzionamento, delle capacità tecniche, del mandato e della cooperazione[30].

– Nel 2010 l'ENISA ha collaborato con la rete delle CERT in Europa per trasformare i requisiti operativi summenzionati in un insieme di raccomandazioni strategiche[31] che permetteranno alle CERT nazionali/governative di fungere da elemento chiave delle capacità nazionali in termini di preparazione, scambio di informazioni, coordinamento e reazione.

– Oggi 20 Stati membri[32] hanno creato delle CERT nazionali/governative e quasi tutti gli altri Stati intendono istituirle. Come preannunciato nell'Agenda digitale europea e ulteriormente chiarito nella strategia di sicurezza interna dell'UE in azione, la Commissione ha proposto misure per istituire una CERT per le istituzioni dell'UE entro il 2012.

Prossime tappe

– L'ENISA continuerà a sostenere gli Stati membri che non hanno ancora creato una CERT governativa/nazionale rispondente ai requisiti di base approvati già menzionati, al fine di garantire il conseguimento dell'obiettivo di disporre di CERT governative/nazionali adeguatamente funzionanti entro la fine del 2011. Una volta superata questa tappa, si potrà riflettere all'istituzione di una rete operativa di CERT a livello nazionale **entro il 2012** come previsto dall'Agenda digitale europea.

---

30 Vedi http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations

32 Fonte ENISA.

– L'ENISA, in collaborazione con le CERT nazionali/governative, valuterà la possibilità di ampliare le "capacità di base" e le eventuali modalità di questa estensione al fine di adeguare la capacità delle CERT di aiutare gli Stati membri a garantire la resilienza e la stabilità delle infrastrutture TIC fondamentali e diventerà l'asse portante del Sistema europeo di condivisione delle informazioni e di allarme (EISAS) per i cittadini e le PMI. Questo sistema deve essere istituito **entro il 2013** avvalendosi di risorse e mezzi nazionali, come indicato nella strategia di sicurezza interna dell'UE in azione.

Partenariato pubblico-privato europeo per la resilienza (EP3R)

Realizzazioni

– Nel 2009 è stato varato il partenariato pubblico-privato europeo per la resilienza (EP3R) che costituisce un quadro europeo di *governance* per la resilienza delle infrastrutture TIC destinato ad incentivare la cooperazione tra il settore pubblico e il settore privato su obiettivi in materia di sicurezza e resilienza, requisiti di base, buone pratiche e provvedimenti adeguati. Come affermato nella strategia di sicurezza interna dell'UE, l'EP3R dovrebbe "*inoltre impegnarsi con i partner internazionali a rafforzare la gestione globale dei rischi delle reti informatiche*." L'ENISA ha agevolato le attività dell'EP3R.

– Per definire gli obiettivi, i principi e la struttura dell'EP3R e per stabilire quali incentivi potrebbero essere utilizzati per incoraggiare gli interessati a partecipare in modo attivo ai lavori[33] sono state consultate parti interessate del settore pubblico e del settore privato. La proposta relativa alla modernizzazione dell'ENISA individua i settori d'azione prioritari per l'EP3R[34].

– Parallelamente alla concezione della struttura dell'EP3R, alla fine del 2010 sono stati istituiti tre gruppi di lavoro su a) punti di forza, risorse e funzioni principali per la fornitura sicura e continua di comunicazioni elettroniche tra paesi; b) requisiti di base in materia di sicurezza e resilienza delle comunicazioni elettroniche; c) esigenze di coordinamento e cooperazione e meccanismi di preparazione e di reazione nel caso di disfunzioni su larga scala che incidono sulle comunicazioni elettroniche.

– Nel 2010 la proposta della Commissione relativa alla modernizzazione dell'ENISA prevedeva un quadro sostenibile a lungo termine per l'EP3R proponendo che l'ENISA sostenesse "*la cooperazione tra le parti interessate del settore pubblico e di quello privato a livello di Unione, tra l'altro promuovendo la condivisione di informazioni e la sensibilizzazione e aiutandole nell'impegno a definire e adottare norme in materia di gestione dei rischi e di sicurezza dei prodotti, delle reti e dei servizi elettronici*".

Prossime tappe

– Nel 2011 l'EP3R continuerà a rafforzare la cooperazione tra il settore pubblico e il settore privato per migliorare la sicurezza e la resilienza mediante misure e strumenti innovativi e per determinare le responsabilità delle parti interessate. I gruppi di lavoro EP3R forniranno i loro primi risultati, sfruttando il ruolo di appoggio e il sostegno dell'ENISA. Le attività

[33] Vedi http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

[34] COM(2010) 521.

future riguarderanno i problemi di sicurezza informatica sollevati dalle reti intelligenti, sulla base del lavori preparatori realizzati dalla Commissione e dall'ENISA.

– L'EP3R fungerà da piattaforma di portata mondiale per le questioni di politica pubblica, economia e mercati attinenti alla sicurezza e alla resilienza. La Commissione intende avvalersi dell'EP3R per sostenere le attività del gruppo di lavoro congiunto UE-Stati Uniti sulla sicurezza e la criminalità informatiche al fine di istituire un quadro coerente per la cooperazione tra il settore pubblico e quello privato, nel rispetto delle regole vigenti nel settore della concorrenza e degli aiuti di Stato.

– A lungo termine e conformemente alla proposta di un nuovo regolamento concernente l'ENISA si prevede di fare dell'EP3R un'attività essenziale di un'ENISA modernizzata.

Forum europeo degli Stati membri (EFMS)

Realizzazioni

– Nel 2009 è stato istituito il Forum europeo degli Stati membri (EFMS) destinato a favorire la discussione e gli scambi tra autorità pubbliche competenti sulle buone pratiche per condividere obiettivi e priorità strategiche in relazione alla sicurezza e alla resilienza delle infrastrutture TIC, traendo diretto vantaggio dall'attività dell'ENISA e dal sostegno che fornisce. L'EFMS, i cui membri si riuniscono a cadenza trimestrale, si è dotato alla metà del 2010 di un portale web specifico gestito dall'ENISA.

– Il Forum ha compiuto significativi passi avanti per quanto riguarda: a) la definizione dei criteri per l'individuazione delle infrastrutture TIC europee nel contesto della direttiva relativa all'individuazione e alla designazione delle infrastrutture critiche europee[35]; b) l'individuazione delle priorità, dei principi e degli orientamenti europei per la resilienza e la stabilità di internet; c) lo scambio di buone pratiche strategiche, in particolare per le esercitazioni nel settore della sicurezza informatica.

– Gli Stati membri considerano l'EFMS una piattaforma importante per il dialogo e lo scambio di nuove pratiche[36].

Prossime tappe

– Nel 2011 il Forum completerà le discussioni tecniche sui criteri TIC per le infrastrutture critiche europee e elaborerà orientamenti e priorità a lungo termine per quanto riguarda le esercitazioni paneuropee su incidenti di ampia portata che incidono sulla sicurezza delle reti e delle informazioni.

– L'EFMS parteciperà più attivamente ai dibattiti sulle priorità di portata internazionale in materia di sicurezza e di resilienza, in particolare in collegamento con le attività del gruppo di lavoro congiunto UE-Stati Uniti sulla sicurezza e la criminalità informatiche.

---

35 Direttiva 2008/114/CE del Consiglio.

36 Nella sua risposta alla quinta relazione del comitato sull'Unione europea della Camera dei Lord concernente il piano d'azione CIIP, il governo britannico ha dichiarato che il Forum europeo degli Stati membri è un'iniziativa coronata da successo che risponde ad un'effettiva esigenza fornendo ai responsabili delle decisioni un quadro nel quale condividere le proprie esperienze.

– Le aree prioritarie delle future attività dell'EFMS, che beneficeranno del sostegno diretto dell'ENISA, comprendono[37]: l'elaborazione di metodi che consentano di istituire una cooperazione efficace tra le CERT nazionali/governative; il ricorso a prescrizioni minime negli appalti pubblici per rafforzare la sicurezza informatica; la definizione di incentivi, di carattere economico e normativo, a favore della sicurezza e della resilienza (nel rispetto delle regole vigenti nel settore della concorrenza e degli aiuti di Stato); valutazione dello stato della "sicurezza informatica" in Europa.

2. Individuazione e risposta

Sistema europeo di condivisione delle informazioni e di allarme (EISAS)

Realizzazioni

– La Commissione ha finanziato due progetti pilota (FISHAS e NEISAS) che attualmente stanno generando i loro risultati finali.

– Sulla base della sua relazione di fattibilità del 2007[38] e dell'analisi di progetti pertinenti a livello nazionale ed europeo, l'ENISA ha elaborato una tabella di marcia di alto livello per promuovere lo sviluppo, entro il 2013, del sistema europeo di condivisione delle informazioni e di allarme[39].

Prossime tappe

– Nel 2011 l'ENISA assisterà gli Stati membri nella attuazione di una tabella di marcia EISAS elaborando i "servizi di base" di cui gli Stati membri hanno bisogno per istituire il loro sistema nazionale di condivisione delle informazioni e di allarme (ISAS) basato sulle capacità delle loro CERT nazionali/governative.

– Nel 2012 l'ENISA svilupperà i "servizi di interoperabilità" che consentiranno l'integrazione di tutti i sistemi ISAS nazionali nell'EISAS. Assisterà inoltre gli Stati membri nella fase di test di questi servizi che consisterà nell'integrare progressivamente i sistemi nazionali.

– Nel corso del biennio 2011-2012 l'ENISA inviterà le CERT nazionali/governative ad integrare la funzione ISAS nei loro servizi.

3. Mitigazione e recupero

Piani di emergenza ed esercitazioni nazionali

37 COM(2010) 251.

38 Vedi http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

Realizzazioni

– Alla fine del 2010 12 Stati membri avevano elaborato un piano nazionale di emergenza e/o organizzato esercitazioni sulla reazione in casi di incidenti di ampia portata che incidono sulla sicurezza delle reti e sul ripristino[40].

– Sulla base dell'esperienza maturata a livello nazionale ed internazionale, l'ENISA ha elaborato una guida di buone pratiche per le esercitazioni nazionali[41]; ha organizzato, con gli Stati membri e le CERT del mondo intero, eventi relativi alle esercitazioni nazionali; e, più di recente, ha pubblicato raccomandazioni strategiche sullo sviluppo di strategie nazionali che attribuiscono ai CERT/CSIRT nazionali/governativi un ruolo fondamentale nella gestione di esercitazioni sui piani di emergenza e nei test a livello nazionale, con la partecipazione di parti interessate del settore pubblico e del settore privato[42].

Prossime tappe

– Per contribuire a rafforzare il coordinamento paneuropeo, l'ENISA continuerà a sostenere l'impegno degli Stati membri nell'elaborazione di piani di emergenza nazionali e nell'organizzazione di esercitazioni periodiche sulla reazione in caso di incidenti di ampia portata a danno della sicurezza delle reti e sul ripristino.

Esercitazione paneuropea su incidenti di ampia portata a danno della sicurezza delle reti

Realizzazioni

– La prima esercitazione paneuropea relativa ad incidenti di ampia portata che incidono sulla sicurezza delle reti (*Cyber Europe 2010*) si è svolta il 4 novembre 2010 con la partecipazione di tutti gli Stati membri, 19 dei quali hanno preso parte attivamente all'esercitazione, e della Svizzera, della Norvegia e dell'Islanda. L'esercitazione è stata organizzata e valutata[43] dall'ENISA con la partecipazione attiva nell'equipe di pianificazione di otto Stati membri e il sostegno tecnologico del Centro comune di ricerca (JRC).

Prossime tappe

– Nel 2011 gli Stati membri discuteranno dell'obiettivo e della portata della prossima esercitazione paneuropea in materia di sicurezza informatica prevista per il 2012. Si esaminerà la possibilità di un approccio graduale, con esercitazioni più approfondite che coinvolgono un numero più limitato di Stati membri ed, eventualmente, attori internazionali. L'ENISA continuerà a sostenere questo processo.

– La Commissione sta finanziando il progetto EuroCybex che prevede l'organizzazione di un'esercitazione di simulazione nel corso del secondo semestre del 2011.

---

40 http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

43 Vedi http://www.enisa.europa.eu/

– Le esercitazioni nel settore della sicurezza informatica sono un elemento essenziale di una strategia coerente relativa ai piani di emergenza in caso di incidenti informatici, a livello nazionale ed europeo. La future esercitazioni paneuropee dovrebbero pertanto essere varate sulla base di un piano di emergenza europeo in caso di incidenti informatici che si fonda e si collega ai piani di emergenza nazionali. Questo piano dovrebbe fornire i meccanismi e le procedure di base per la comunicazione tra Stati membri nonché un sostegno per definire la portata delle future esercitazioni paneuropee e per organizzarle. L'ENISA collaborerà con gli Stati membri affinché questo piano di emergenza europeo in caso di incidenti informatici sia elaborato entro il 2012. Per questa stessa data tutti gli Stati membri devono istituire piani di emergenza nazionali e esercitazioni periodiche di reazione e ripristino. L'EFMS sarà responsabile del coordinamento degli interventi necessari per ottenere questi risultati.

Cooperazione rafforzata tra le squadre nazionali o governative di pronto intervento informatico (CERT)

Realizzazioni

– La cooperazione tra le CERT nazionali/governative si è intensificata. Il lavoro di ENISA sulla base minima di capacità delle CERT nazionali/governative, le esercitazioni delle CERT e le esercitazioni nazionali, e la gestione degli incidenti informatici hanno contribuito ad incentivare e sostenere il rafforzamento della cooperazione paneuropea tra le CERT nazionali/governative.

Prossime tappe

– L'ENISA continuerà a sostenere la cooperazione tra le CERT nazionali/governative. A tal fine effettuerà nel 2011 un'analisi dei requisiti e fornirà degli orientamenti sulla scelta di un canale sicuro e adeguato di comunicazione con le CERT, ivi compresa una tabella di marcia per l'attuazione e lo sviluppo futuro. L'ENISA analizzerà anche le carenze operative a livello europeo e riferirà sulla possibilità di rafforzare la collaborazione transnazionale tra CERT e parti interessate, in particolare per il coordinamento delle reazioni in caso di incidenti.

– Nell'Agenda digitale europea si invitano gli Stati europei ad istituire una rete efficiente di CERT a livello nazionale **entro il 2012**.

4. Cooperazione internazionale

Stabilità e resilienza di internet

Realizzazioni

– Sulla base del lavoro effettuato dell'EFMS sono stati elaborati principi e orientamenti europei per la resilienza e la stabilità di internet[44].

Prossime tappe

[44] Vedi http://ec.europa.eu/information_society/policy/nis/index_en.htm

– Nel 2011 la Commissione promuoverà e analizzerà questi principi nell'ambito di una cooperazione bilaterale con partner internazionali, in particolare gli USA, e nell'ambito di discussioni multilaterali in seno al G8, all'OCSE, al Meridian e all'UIT; consulterà le parti interessate, in particolare il settore privato, a livello europeo (mediante l'EP3R) ed internazionale (tramite il forum sulla governance di Internet e altre sedi appropriate); e promuoverà il dibattito con attori/organizzazioni importanti di internet.

– Nel 2012 i partner internazionali si attiveranno per trasformare questi principi e questi orientamenti in un quadro comune favorevole ad un impegno collettivo internazionale sulla resilienza e la stabilità a lungo termine di internet.

Esercitazioni globali in materia di recupero e attenuazione in caso di incidenti di ampia portata a danno di internet

Realizzazioni

– Sette Stati membri[45] hanno partecipato, in qualità di partner internazionali, all'esercitazione statunitense nel settore della sicurezza informatica "Cyber Storm III". La Commissione e l'ENISA hanno partecipato a questa esercitazione in qualità di osservatori.

Prossime tappe

– Nel 2011 la Commissione svilupperà con gli USA, sotto l'egida del gruppo di lavoro congiunto UE-USA sulla sicurezza e la criminalità informatiche, un programma comune e una tabella di marcia relativi all'organizzazione nel 2012/2013 di esercitazioni transcontinentali comuni o sincronizzate nel settore della sicurezza informatica. Si considererà anche un coinvolgimento di altre regioni o altri paesi che affrontano problemi analoghi al fine di condividere gli approcci e le attività associate.

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

Criteri settoriali per l'individuazione delle infrastrutture critiche europee nel settore delle TIC

Realizzazioni

– Le discussioni tecniche sui criteri specifici per le TIC in seno al Forum europeo degli Stati membri hanno portato ad una prima versione di questi criteri per le comunicazioni fisse e mobili e internet.

Prossime tappe

[45] FR, DE, HU, IT, NL, SE e UK.

– Le discussioni sui criteri settoriali proseguiranno in seno al Forum e dovrebbero terminare alla fine del 2011. Parallelamente in alcuni Stati membri e a livello europeo si prevedono delle consultazioni con il settore privato sulla prima versione dei criteri settoriali nell'ambito dell'EP3R.

– La Commissione esaminerà anche con gli Stati membri gli elementi specifici del settore delle TIC di cui tenere conto nel 2012 nell'ambito del riesame della direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee.

–