I

(Risoluzioni, raccomandazioni, orientamenti e pareri)

RISOLUZIONI

CONSIGLIO

RISOLUZIONE DEL CONSIGLIO

del 22 marzo 2007

su una strategia per una società dell'informazione sicura in Europa

(2007/C 68/01)

IL CONSIGLIO DELL'UNIONE EUROPEA,

ADOTTA LA SEGUENTE RISOLUZIONE E

ACCOGLIE CON FAVORE

la comunicazione della Commissione del 31 maggio 2006 al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni — Una strategia per una società dell'informazione sicura — «Dialogo, partenariato e responsabilizzazione».

PRENDE ATTO

della comunicazione della Commissione, del 15 novembre 2006, al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, sulla lotta contro le comunicazioni commerciali non richieste (spam), i programmi spia (spyware) e i software maligni.

RICORDA

1. la risoluzione del Consiglio del 28 gennaio 2002 relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione ([1]);

2. la Risoluzione del Consiglio del 18 febbraio 2003 su un approccio europeo per una cultura della sicurezza delle reti e dell'informazione ([2]);

3. le conclusioni del Consiglio dell'8 e 9 marzo 2004 sulle comunicazioni commerciali non richieste o «spam» e le conclusioni del Consiglio del 9 e 10 dicembre 2004 sulla lotta contro gli spam;

4. le conclusioni del Consiglio europeo del marzo 2005 che rilanciano la strategia di Lisbona e le conclusioni del Consiglio europeo del marzo 2006 che invitano la Commissione e gli Stati membri ad attuare con vigore la nuova strategia i2010;

5. il quadro normativo UE per le comunicazioni elettroniche ([3]), in particolare le disposizioni relative alla sicurezza della comunicazione, alla vita privata e alla riservatezza che hanno contribuito a garantire un livello elevato di protezione dei dati personali e della vita privata e l'integrità e la sicurezza delle reti di comunicazione pubbliche;

6. il 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 ([4]);

7. l'agenda di Tunisi e l'impegno di Tunisi del vertice mondiale sulla società dell'informazione (WSIS) che mettono in evidenza la necessità di continuare la lotta contro la cibercriminalità e gli spam, garantendo al tempo stesso la protezione della vita privata e la libertà di parola, nonché di promuovere, sviluppare ed attuare, in cooperazione con tutti i soggetti interessati, una cultura globale della cibersicurezza;

8. le conclusioni formulate dalla presidenza nella conferenza annuale sulla società europea dell'informazione «i2010 — Verso una società dell'informazione europea onnipresente», svoltasi il 27 e 28 settembre 2006 a Espoo in Finlandia.

([1]) GU C 43 del 16.2.2002, pag. 2.
([2]) GU C 48 del 28.2.2003, pag. 1.
([3]) Direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche), direttiva 2002/20/CE (direttiva autorizzazioni), direttiva 2002/22/CE (direttiva servizio universale) (nell'ordine:GU L 201 del 31.7.2002, pag. 37; GU L 108 del 24.4.2002, pag. 21 e GU L 108 del 24.4.2002, pag. 51).
([4]) GU L 77 del 13.3.2004, pag. 1.

SOTTOLINEA PERTANTO CHE

1. la nostra società sta passando rapidamente ad una nuova fase di sviluppo «verso una società dell'informazione onnipresente», in cui le attività quotidiane dei cittadini ricorrono sempre più alle tecnologie dell'informazione e delle comunicazioni (TIC) e alle reti di comunicazioni elettroniche. La sicurezza delle reti e dell'informazione dovrebbe essere ritenuta un importante catalizzatore dello sviluppo suddetto e del suo successo;

2. la fiducia è un elemento fondamentale del successo della nuova società dell'informazione. È anche connessa alle esperienze degli utilizzatori finali e alla necessità di rispettarne la vita privata, pertanto la sicurezza delle reti e dell'informazione non dovrebbe essere considerata una questione meramente tecnica;

3. la sicurezza delle reti e dell'informazione è una componente essenziale della creazione di uno spazio europeo dell'informazione come parte dell'iniziativa i2010, contribuendo in tal modo al successo della rinnovata strategia di Lisbona. Le TIC costituiscono inoltre una componente fondamentale dell'innovazione, della crescita economica e dell'occupazione in ogni settore dell'economia;

4. già si sviluppano le nuove tecnologie che ci porteranno alla società dell'informazione onnipresente. L'avvento di tecnologie innovative (ad esempio reti senza filo ad alta velocità, dispositivi di identificazione a radiofrequenza (RFID, reti di sensori) e di servizi innovativi, ricchi di contenuti (ad esempio televisione su protocollo internet (IPTV), voice over IP (VoIP), televisione mobile ed altri servizi mobili) richiede adeguati livelli di sicurezza delle reti e dell'informazione fin dall'inizio della fase di sviluppo per raggiungere reale valore commerciale. La tempestiva adozione delle recenti innovazioni promettenti riveste grande importanza per lo sviluppo della società dell'informazione e la competitività dell'Europa. Gli organi e le imprese governativi dovrebbero adottare quanto prima possibile le tecnologie e i servizi nuovi, sicuri ed emergenti per accelerarne l'adozione massiccia;

5. è d'importanza strategica che l'industria europea sia al tempo stesso un utilizzatore esigente e un fornitore competitivo di reti e di prodotti e servizi di sicurezza. La diversità, l'apertura e l'interoperabilità sono parti integranti della sicurezza ed è opportuno promuoverle;

6. la conoscenza e le competenze in materia di sicurezza delle reti e dell'informazione devono inoltre divenire parte integrante della vita quotidiana di ogni persona e parte interessata della società; una serie di campagne di sensibilizzazione è stata lanciata sia a livello nazionale sia a livello di UE, ma in questo settore molto resta ancora da fare, specialmente per quanto riguarda gli utenti finali e le piccole e medie imprese (PMI); occorre prestare particolare attenzione agli utenti con esigenze speciali o poco sensibilizzati alle questioni della sicurezza delle reti e dell'informazione; tutti gli interessati dovrebbero essere consapevoli del fatto di essere parti della catena della sicurezza globale e dovrebbero poter operare in quanto tali; le questioni della sicurezza delle reti e dell'informazione dovrebbero essere prese in considerazione in ogni tipo di istruzione e formazione in materia di TIC;

7. l'istituzione dell'Agenzia europea per la sicurezza delle reti e dell'informazione ha costituito un importante passo in avanti negli sforzi dell'UE volti a rispondere alle sfide connesse con la sicurezza delle reti e dell'informazione; campo d'azione, obiettivi, compiti e durata dell'Agenzia sono definiti dal regolamento n. 460/2004;

8. le risorse impegnate nelle attività di ricerca e sviluppo (R&S) e di innovazione a livello sia nazionale che di UE costituiscono uno degli elementi chiave nel miglioramento del livello della sicurezza delle reti e dell'informazione di nuovi sistemi, applicazioni e servizi; gli sforzi a livello di UE dovrebbero essere potenziati nei settori della ricerca e dell'innovazione connessi con la sicurezza, in particolare attraverso il settimo programma quadro (EP7) e il programma quadro per la competitività e l'innovazione (CIP); gli sforzi dovrebbero inoltre rivolgersi a misure per divulgare e incoraggiare lo sfruttamento commerciale dei risultati ottenuti, compresa la valutazione della loro utilità per la comunità più ampia; in tal modo si rafforzerà la capacità dei fornitori europei di elaborare soluzioni in materia di sicurezza che soddisfino le esigenze specifiche del mercato europeo;

9. la società dell'informazione universale reca grandi vantaggi, ma pone anche sfide significative creando un nuovo panorama di rischi potenziali; le minacce alla sicurezza e alla vita privata, anche attraverso l'intercettazione e l'utilizzazione illecita di dati, stanno diventando sempre più gravi, mirate e chiaramente finalizzate all'ottenimento di vantaggi economici; per le minacce emergenti o già esistenti si dovrebbero trovare in modo innovativo nuove risposte, che dovrebbero riguardare anche problemi derivanti dalla complessità del sistema, da errori, incidenti o orientamenti non chiari; la creazione e lo sviluppo di organismi nazionali di pronto intervento informatico rivolti a vari attori e la cooperazione tra detti organismi nonché con altri interessati dovrebbero essere incoraggiati e ulteriormente promossi;

10. la standardizzazione e la certificazione di prodotti, servizi e sistemi di gestione, forniti in particolare da istituzioni esistenti, meritano particolare attenzione nell'ambito della politica dell'UE in materia di sicurezza delle reti e dell'informazione in quanto costituiscono un mezzo per la diffusione di buone prassi e professionalità nel campo della sicurezza delle reti e dell'informazione; dalla tempestiva adozione di eventuali norme aperte e interoperabili emergenti trarrebbero beneficio specialmente nuove tecnologie emergenti come la RFID (identificazione a radiofrequenza) e la televisione mobile; il funzionamento degli organismi europei di normalizzazione in questo settore dovrebbe essere incoraggiato;

11. dato che i sistemi elettronici delle reti e dell'informazione svolgono un ruolo vieppiù cruciale nel funzionamento globale delle infrastrutture critiche, la loro disponibilità e integrità diventano indispensabili per la sicurezza e la qualità della vita di amministrazioni, imprese e cittadini nonché per il funzionamento globale delle società;

12. cooperazione e approcci pratici sono necessari più che mai; i vari interessati dovrebbero identificare e riconoscere i loro rispettivi ruoli, responsabilità e diritti.

E PERTANTO INVITA GLI STATI MEMBRI A

1. sostenere i programmi di formazione e migliorare la sensibilizzazione della pubblica opinione ai temi della sicurezza delle reti e dell'informazione, per esempio organizzando campagne d'informazione sulle questioni della sicurezza delle reti e dell'informazione, rivolgendosi a tutti i cittadini/utenti e settori dell'economia, specialmente le PMI e gli utenti finali con particolari esigenze o poco sensibilizzati; entro il 2008 potrebbe essere scelta una data comune come giornata per il miglioramento della sensibilizzazione a livello europeo (per es. «Giornata della sicurezza delle reti e dell'informazione») da celebrare su base annuale e volontaria in ogni Stato membro;

2. aumentare il contributo alle attività di R&S connesse con la sicurezza e migliorare l'uso e la divulgazione dei relativi risultati; incoraggiare lo sviluppo di partenariati innovativi per potenziare la crescita dell'industria europea delle TIC in materia di sicurezza e incrementare la rapida utilizzazione di nuove tecnologie e nuovi servizi nel settore della sicurezza delle reti e dell'informazione onde stimolarne la commercializzazione;

3. prestare la dovuta attenzione alla necessità di prevenire e combattere minacce nuove o esistenti alla sicurezza di reti di comunicazione elettronica, comprese l'intercettazione e l'utilizzazione illegale di dati, riconoscere i rischi connessi e farsene carico e incoraggiare, se necessario in cooperazione con l'Agenzia europea per la sicurezza delle reti e dell'informazione, uno scambio di informazioni e una cooperazione efficaci tra organizzazioni e agenzie pertinenti a livello nazionale; impegnarsi nella lotta contro gli spam, programmi spia e software maligni, in particolare attraverso il miglioramento della cooperazione tra le autorità competenti a livello nazionale e internazionale;

4. rafforzare la cooperazione nel quadro dell'iniziativa i2010 allo scopo di individuare prassi efficaci e innovative per migliorare la sicurezza delle reti e dell'informazione e diffondere la conoscenza di tali prassi nell'UE su base volontaria;

5. incoraggiare il costante miglioramento degli organismi nazionali di pronto intervento informatico;

6. promuovere un contesto che incoraggi i fornitori di servizi e gli operatori di rete a fornire servizi validi ai loro clienti e a garantire ai consumatori elasticità e scelta nei servizi e nelle soluzioni che offrono in materia di sicurezza; incoraggiare gli operatori di rete e i fornitori di servizi a garantire ai rispettivi clienti un livello adeguato di sicurezza delle reti e dell'informazione o, se necessario, esigerlo dagli stessi;

7. continuare una discussione strategica in sede di Gruppo ad alto livello «Iniziativa i2010», tenendo conto allo stesso tempo degli sviluppi in atto nella società dell'informazione, e assicurare un approccio coerente tra le dimensioni di regolamentazione, coregolamentazione, R&S e eGovernment unitamente a comunicazione e istruzione;

8. conformemente al piano d'azione eGovernment iniziativa i2010 prevedere la realizzazione di servizi di eGovernment a copertura ininterrotta, promuovere soluzioni interoperabili di gestione dell'identità e intraprendere ogni opportuna modifica nell'organizzazione del settore pubblico; governi e pubbliche amministrazioni dovrebbero servire da esempio in materia di migliori prassi promuovendo servizi sicuri di eGovernment per tutti i cittadini.

ACCOGLIE CON FAVORE L'INTENZIONE DELLA COMMISSIONE DI

1. portare avanti l'elaborazione di una strategia completa e dinamica a livello comunitario per la sicurezza delle reti e dell'informazione. L'approccio globale proposto dalla Commissione riveste speciale importanza;

2. ritenere la sicurezza delle reti e dell'informazione come uno degli obiettivi nel riesame del quadro normativo delle comunicazioni elettroniche dell'UE;

3. continuare a svolgere il proprio ruolo così da poter raggiungere maggiore consapevolezza dell'esigenza di un impegno politico generale nella lotta agli spam, ai programmi spia e ai software maligni; rafforzare il dialogo e la cooperazione con i paesi terzi, in particolare tramite gli accordi con i paesi terzi che includono la tematica della lotta allo spam, ai programmi spia e ai software maligni;

4. rafforzare il coinvolgimento dell'Agenzia europea per la sicurezza delle reti e dell'informazione nel sostegno alla strategia per una società dell'informazione sicura in Europa, come indicato nella presente risoluzione, in linea con gli obiettivi e i compiti fissati nel regolamento (CE) N. 460/2004, nonché in una collaborazione più stretta e in relazioni di cooperazione più forti con gli Stati membri e le parti interessate;

5. sviluppare nel contesto dell'iniziativa i2010, in cooperazione con gli Stati membri e tutte le parti interessate, specialmente con gli esperti di statistica e di sicurezza dell'informazione degli Stati membri, gli indicatori opportuni per le inchieste comunitarie sugli aspetti relativi alla sicurezza e alla fiducia;

6. incoraggiare gli Stati membri ad esaminare, per mezzo di un dialogo con tutte le parti interessate, i fattori economici, commerciali e societari allo scopo di sviluppare una politica specifica per il settore delle TIC per migliorare la sicurezza e la resistenza delle reti e dei sistemi informatici, quale potenziale contributo al previsto programma europeo per la protezione delle infrastrutture critiche;

7. continuare gli sforzi, in coordinamento con gli Stati membri, per promuovere il dialogo con i partner e le organizzazioni internazionali pertinenti al fine di favorire una cooperazione globale sulla sicurezza delle reti e dell'informazione, segnatamente tramite l'attuazione delle linee d'azione elaborate dal vertice mondiale sulla società dell'informazione (WSIS) e la presentazione di relazioni al Consiglio su base regolare.

E INVITA

1. l'Agenzia europea per la sicurezza delle reti e dell'informazione a continuare a operare in stretta collaborazione con gli Stati membri, la Commissione e le altre pertinenti parti interessate, al fine di realizzare compiti e obiettivi che sono definiti nel regolamento (CE) n. 460/2004 e di assistere la Commissione e gli Stati membri nei loro sforzi tesi a rispettare i requisiti della sicurezza delle reti e dell'informazione, contribuendo così all'attuazione e allo sviluppo ulteriore della strategia per una società dell'informazione sicura in Europa come indicato nella presente risoluzione;
2. tutte le parti interessate a migliorare la sicurezza dei software e la sicurezza e resistenza delle reti e dei sistemi informatici in linea con la strategia per una società dell'informazione sicura in Europa come indicato nella presente risoluzione, nonché a impegnarsi in un dibattito strutturato tra tutte le parti interessate sulla migliore modalità di utilizzare gli strumenti generali e normativi esistenti;
3. le imprese ad assumere un atteggiamento positivo nei confronti della sicurezza delle reti e dell'informazione al fine di creare prodotti e servizi più evoluti e sicuri, e a considerare un vantaggio competitivo gli investimenti in tali prodotti e servizi;
4. i produttori e i fornitori di servizi a inserire, se opportuno, requisiti di sicurezza, riservatezza e segretezza nella progettazione dei loro prodotti e servizi e nella diffusione dell'infrastruttura delle reti, delle applicazioni e dei software, a ad attuare e controllare soluzioni di sicurezza;
5. le parti interessate a cooperare e ad avviare contesti sperimentali per testare e indirizzare le tecnologie e i servizi nuovi in maniera sicura; ad adottare tempestivamente le nuove tecnologie sicure e i nuovi servizi sicuri dopo che ne è stata avviata la commercializzazione;
6. tutte le parti interessate ad impegnarsi ulteriormente nella lotta agli spam e agli altri abusi informatici e a cooperare attivamente con le autorità competenti a livello nazionale e internazionale;
7. i fornitori di servizi e l'industria delle TIC a concentrarsi sul miglioramento della sicurezza, della riservatezza e dell'utilizzabilità dei prodotti, dei processi e dei servizi in modo da risultare affidabili, e impedire e combattere il furto di identità e altre minacce alla vita privata;
8. gli operatori della rete, i fornitori di servizi e il settore privato a condividere e attuare le buone prassi di sicurezza e a favorire una cultura di analisi e gestione del rischio nelle organizzazioni e nel settore commerciale tramite il sostegno a opportuni programmi di formazione e lo sviluppo di un piano di emergenza, nonché mettendo a disposizione dei loro clienti soluzioni di sicurezza come parte dei loro servizi.