

**Protezione delle Infrastrutture Critiche
da Attacchi e/o Danni Informatici: Una
Panoramica delle Iniziative
Internazionali**

Dr Lorenzo Valeri

Senior Policy Analyst

Rand Europe

36 Regents Street

CB2 1DB Cambridge UK

Tel: 0044-1223-353329

Tel: 0044-7815-784383

Email: lvaleri@rand.org

Web: <http://www.randeurope.org>

***Questa presentazione riflette esclusivamente
le opinioni del suo autore. Niente di
quanto detto e scritto e' da attribuire alla
Rand Europe e/o la Rand Corporation***

- ***1994: Verso una Nuova Definizione di Sicurezza Nazionale (non militare)***
- ***1996: Executive Order 13010: Verso la Creazione della President's Commission on Critical Infrastructure Protection (PCCIP)-Rapporto Finale 10/1997***
- ***5/1998 PDD 63 Creazione del Critical Infrastructure Assurance Office***
- ***5/1998: PDD 63 Creazione del National Infrastructure Protection Centre (FBI)***
- ***1/2000 National Plan for Infrastructure Assurance Office 1.0***
- ***1/2001 Rapporto al Presidente sulle Attivita' di CIAO***

Cosa fare dopo 11 Settembre?

- ***16/10/2001: Critical Infrastructure Protection in the Information Age (sostituzione P.D.D. 63)***
 - *Critical Infrastructure Protection Board (CIPB)*
 - *Infrastructure Interdependency Committee*
 - *Office of Science and Technology (Casa Bianca)*
 - *International Information Infrastructure Protection (Dipartimento di Stato)*
- ***New Strategy for Information Security (Settembre 2002)***
- ***Creazione del Homeland Security Department (essenzialmente il Ministero degli Interni degli Stati Uniti)***

- ***Ricerca e Sviluppo (DARPA, NSA, NSF, etc..)***
- ***Threat Assessment (NIPC in prevalenza)***
- ***Education***
- ***Verso gli Auditors (forse niente di nuovo!)***
- ***Standards: sempre chiamati...mai definiti...Common Criteria (?) e IS 17799 Parte 1***
- ***Quale ruolo per l'industria?***
- ***Quale ruolo per la ricerca (molti soldi almeno a parole....)***

Linee Guida per la Protezione delle Infrastrutture negli USA: Partnership Pubblico-Privata

- ***Partnership for Critical Infrastructure Protection (PCIS)***
- ***70 società (molte di quelle presenti a Infosecurity 2001)***
- ***Budget limitato...***
- ***Partecipazione su Base Volontaria***
- ***Working groups:***
 1. ***Interdependency/Risk Assessment***
 2. ***Information Sharing***
 3. ***Research and Development***
 4. ***Public Policy***

- ***Information Sharing and Analysis Centres (ISACs)***
- ***Organizzazioni Private***
- ***Per Settore (finanza, elettricità, IT)***
- ***Outsourced (ISS-IT ISACs or Predictive Systems FISAC)***
- ***Problemi legali (Anti-trust, Freedom of Information Act...)***
- ***Problemi di Immagine***
- ***Sono CERTs privati?***
- ***Ma se CERTs sbagliassero?***

Protezione delle Infrastrutture Critiche: Regno Unito

- ***National Information Infrastructure Security Centre (NISCC)***
- ***Rapporti tra Ministeri (Cabinet Office, Home Office, Ministry of Defence, Department of Trade and Industry)***
- ***C:Cure (BS7799): problemi***
- ***Standards, Education, Ricerca...part II del BS7799 come standards...***
- ***Problemi di Fondi (ma non per studi non-tecnologici)***
- ***Quale Ruolo per CESG?***

Dialogo Pubblico-Privato negli UK: IAAC

- ***Information Assurance Advisory Council (IAAC)***
- ***50+ societa' presenti (diversi livelli di membership)***
- ***Obiettivo: aiutare il dialogo pubblico-privato***
- ***Non scambio di dati specifici sulle vulnerabilities***
- ***Aiutare Public Policy***
- ***<http://www.iaac.org.uk>***

- ***BSI***
- ***Il Progetto KRITIS***
- ***Forte focus sul problema della privacy***
- ***Warning e Information Sharing***
- ***Ricerca: Franhoufer Institute (Berlin e Darmstadt)***

- ***Il Progetto KWINT***
- ***Vulnerability of the Internet***
- ***Forte coscienza dell'interdipendenza tra infrastrutture***
- ***Non tanto diretto alla lotta al crimine informatico***
- ***Attività' di ricerca: TNO ma non solo...***

Protezione delle Infrastrutture Critiche: Cosa Fa l'Unione Europea

- ***DG Societa' dell'Informazione***
- ***DG Mercato Interno***
- ***DG Giustizia e Affari Interni***

- ***E-Europe Action Plan 2005***
- ***Investimenti in R&D***
- ***VI Programma di Ricerca (Priorita 1.2 del WP 2003-2004 – Dependability)***
- ***Ma sono sufficienti?***

Iniziativa DEPPY (Dependability Initiative)

- ***Parte del programma IST***
- ***Workshops (50 organizzazioni EU/15 US)***
- ***3 Linee d'Azione in Piano di Lavoro IST
(1999-2000-2001)***
- ***16 Progetti con oltre 100 Organizzazioni
e Universita' coinvolte***

- ***Awareness***
- ***Ricerca e Sviluppo***
- ***Verso un CERT europeo? European Warning and Information System (EWIS)***
- ***Un ISACs Europeo?***

Warning and Information Sharing (EWIS)

- ***Obiettivo: raccolta and scambio informazioni su fornire all'utente Internet informazioni su possibili vulnerabilita' o altri rischi-***
- ***Problemi:***
- ***Relazione con i CERTs o i managed security services***
- ***Quali informazioni?***
- ***Problemi legali e tecnologici?***

- ***Consiglio Europeo di Tampere (1997)***
- ***Studio ComCrime (1998)***
- ***Comunicazione sulla lotta al crimine informatico (Gennaio 2001)***
- ***Verso una Strategia Europea per la Lotta al Crimine Organizzato (2001)***
- ***Decision Quadro (bozza) per la Lotta contro i Sistemi Informatici (solo alcuni aspetti)***
- ***Problema delle aggravanti: cosa e' un "significant damage" su Internet? Come lo si calcola? Come lo si misura?***

Convenzione sul Cybercrime del Consiglio d'Europa

- ***Firmata a meta del mese dopo quattro anni di negoziazioni***
- ***Non solo stati membri del Consiglio d'Europa+Stati Uniti+Canada+Giappone+Australia***
- ***Verso un regime internazionale uniforme nella lotta al crimine informatico***
- ***Riferimenti diretti all'hacking, denial of service, virus, intercettazione.***
- ***Coordinamento Internazionale***
- ***Futuro?***

- ***Opzioni per il Futuro***
- ***Common Criteria ISO 15408?***
- ***IS 17799-1 Information Security Management (?)***
- ***Open Source?***

- ***Direttiva sulla Firma Elettronica (1999)***
- ***Attivita' EESSI-standards***
- ***Certificati multipli?***
- ***Ma applicazioni pratiche?***
- ***E il consumatore si domanda: ma come posso utilizzare la firma elettronica?***

- ***Una voce unica in Europa per il problema della sicurezza informatica***
- ***E' una proposta della Commissione...deve andare in Consiglio....non facile***
- ***Obiettivo interessante: sostenere CERTs***
- ***Dal 2004....vediamo come andra' a finire..***

- ***Non solo governo...industria e societa' civile***
- ***Maggiore coordinamento tra amministrazioni***
- ***Verso un migliore dialogo pubblico-privato?***
- ***Verso la conquista del consumatore e utente Internet?***
- ***Protezione delle Infrastrutture Critiche significa far sviluppare la Societa' dell'Informazione***