

Indice

1. **ONLINE SICURO**
2. **INFOSECURITY ROMA: I CONVEGNI**
3. **IL CLUSIT IN VISITA ALL'ITU**
4. **UN NUOVO QUADERNO CLUSIT**
5. **SICUREZZA AZIENDALE CON IL SOLE 24 ORE**
6. **EVENTI SICUREZZA**

1. **ONLINE SICURO**

Nel corso dell'Assemblea generale del Clusit, il 30 maggio 2007, è stato presentato uno dei più importanti progetti a cui abbia mai lavorato la nostra associazione.

ONLINE SICURO - PROGETTO DI WEB SECURITY AWARENESS E ASSISTENZA ON LINE PER CITTADINI E PMI

Lo Scenario

Più del 95% delle Aziende europee dispone di una connessione a internet.

Indipendentemente dalle applicazioni professionali, l'informazione e le tecnologie preposte alla sua gestione sono ormai una componente essenziale della nostra vita quotidiana. Di conseguenza, la loro sicurezza è diventata una preoccupazione assoluta. I malfunzionamenti di tali apparati siano essi accidentali o intenzionali (i cosiddetti "attacchi informatici") non sono più dei problemi specifici di competenza dei soli informatici, ma hanno conseguenze dirette per tutti: cittadini, imprese e pubbliche amministrazioni.

Gestire la sicurezza di tali apparati è però oggi un compito complesso e difficile a causa della complessità della tecnologia, e delle infrastrutture che su di essa si appoggiano. Non va inoltre trascurato il fattore umano che spesso risulta determinante nel concorrere alla soluzione o all'aggravio di una situazione compromessa.

Per contro lo sviluppo economico e sociale impongono alla nostra società, nel suo insieme, ed ai singoli individui, di imparare a convivere con le suddette tecnologie, il che significa anche imparare a gestire i rischi che dal loro uso derivano. Purtroppo ad oggi, sono davvero pochi gli utenti che sembrano coscienti delle vulnerabilità dei sistemi e dei corrispondenti rimedi.

Le iniziative europee

Da diversi anni il Consiglio Europeo, l'OCSE e l'ENISA (l'Agenzia Europea per la sicurezza delle informazioni e delle reti) raccomandano ai Governi

Nazionali di avviare campagne nazionali di sensibilizzazione, con l'obiettivo di:

- estendere a cittadini ed imprese una cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti d'informazione.
- Favorire una maggior fiducia nei confronti delle nuove tecnologie, dei servizi di e-government e dello sviluppo del commercio elettronico.

Sulla scorta di queste sollecitazioni sono diversi i paesi che hanno realizzato, nel corso di questi ultimi anni, campagne ed iniziative nazionali mirate a sensibilizzare i cittadini sul tema della sicurezza delle informazioni e dei sistemi. Ad oggi l'Italia non ha ancora realizzato nessuna iniziativa del genere, che sia dedicata ai cittadini.

La creazione di un portale, di supporto a cittadini e piccole e medie imprese, è un'iniziativa che va proprio in questa direzione.

La campagna italiana

Abbiamo previsto la creazione di un portale che sia uno strumento a disposizione di cittadini e imprese (PMI) per avere risposte ed aiuto qualificato nell'affrontare le problematiche di sicurezza dei sistemi informatici e dell'informazione in generale.

Nel sito Web si illustreranno al cittadino le principali problematiche di sicurezza relative all'utilizzo di Internet: la sicurezza del proprio pc, la sicurezza delle transazioni on line, l'e-government, la tutela dei minori su Internet, i virus, la posta elettronica, la Privacy, la tutela dei diritti d'autore, lo spamming, il phishing, i codici di comportamento, ecc. ecc.

Alle imprese si illustreranno le principali problematiche di sicurezza dei sistemi informatici e dell'informazione in ambito aziendale: le misure minime di sicurezza, gli obblighi inerenti la legislazione sulla privacy, le problematiche specifiche del settore sanitario, quelle del settore finanziario, l'e-commerce, la formazione e la certificazione del personale addetto ai sistemi, ecc. ecc.

Tramite il portale, si potrà inoltre ottenere un servizio di assistenza, a disposizione dei cittadini che desiderassero ottenere ulteriori informazioni e/o aiuto.

Le Istituzioni, promotrici dell'iniziativa

L'iniziativa sarà promossa direttamente dalla Presidenza del Consiglio ed avrà il sostegno di:

- Ministero Comunicazioni
- Ministero Pubblica Istruzione
- Ministero Università e Ricerca
- Ministero Sviluppo economico
- Autorità Garante per la protezione dei dati personali
- Autorità Garante per le Comunicazioni
- Confederazioni Industriali e di Confcommercio
- Associazioni dei Consumatori.

Realizzazione e gestione del Portale. Attività di assistenza on-line.

Le attività saranno coordinate da Fiera Milano International (Infosecurity) e portate avanti dal Clusit e dal CERT.IT (Computer Emergency Response

Team c/o il Dipartimento di informatica e Comunicazione dell'Università degli Studi di Milano).

Copertura finanziaria

In Europa, le campagne nazionali sono state finanziate direttamente dalle Istituzioni dei singoli paesi. In Italia, non essendo possibile accedere in tempi rapidi ad un finanziamento pubblico, l'operazione sarà finanziata da un gruppo di aziende private (appartenenti sia al settore IT che al mondo industriale, finanziario e dei servizi).

Tempistica

L' iniziativa sarà annunciata il 5 giugno a Infosecurity Roma e la presentazione alla stampa è prevista tra giugno-luglio e settembre.

La realizzazione del Portale e la messa in funzione del servizio di assistenza on-line prenderanno circa quattro mesi. Il Portale sarà operativo entro il 2007.

2. INFOSECURITY ROMA: I CONVEGNI

Riportiamo di seguito il programma definitivo dei Convegni organizzati dal Clusit, che si terranno a Infosecurity Roma.

Martedì 5 giugno – 10.30-13.00

« Sicurezza delle informazioni e dei sistemi come servizio per il cittadino e le imprese »

Una Tavola Rotonda con i rappresentanti delle Istituzioni, ai massimi livelli. La protezione dei dati e dei sistemi è oggi un compito che dovrebbe coinvolgere tutti gli attori della nostra società. Purtroppo, il problema è ancora sottovalutato a tutti i livelli, e valori importanti quali la privacy dei cittadini e la competitività delle imprese sono continuamente messi a repentaglio. Come uscire da questa situazione? Su questo tema si confronteranno gli invitati alla tavola rotonda.

Moderatore: Luca De Biase, Capo Redattore Nova24 (Sole24Ore)

Partecipanti alla Tavola Rotonda:

- Luigi Vimercati, Sottosegretario di Stato - Ministero delle Comunicazioni
- Nicola Mazzocca, Consigliere del Ministro per le Riforme e l'Innovazione nella Pubblica Amministrazione
- Francesco Pizzetti, Presidente dell'Autorità Garante per la protezione dei dati personali
- Ennio Lucarelli, Presidente AITech-Assinform e Vicepresidente Confindustria-Servizi Innovativi e Tecnologici
- Danilo Bruschi, Presidente Onorario Clusit

Martedì 5 giugno – 14.30-17.30

"La protezione dei contenuti digitali"

La libera circolazione delle informazioni è il concetto su cui è stata originariamente fondata Internet, per contro il perfetto controllo sulla circolazione delle informazioni è un principio basilare per la realizzazione di profitti nella società dell'informazione. Far convivere i due principi non

è cosa facile, nell'ambito di questo convegno si discuteranno strumenti legali e tecnologici per il controllo della circolazione dell'informazione in azienda ed il loro impatto sulla rete.

Moderatore: Danilo Bruschi, Professore Ordinario di Informatica presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, Presidente Onorario Clusit.

Relatori:

- Giuseppe Corasaniti, Magistrato, che affronterà la problematica dell'art. 4 dello statuto dei lavoratori e i recenti provvedimenti dell'Autorità Garante per la protezione dei dati.
- Roberto Patano, Business Development Manager - Network Appliance Italia

"NetApp: come gestire le informazioni e la loro sicurezza all'interno del ciclo di vita"

I livelli di sicurezza sono diversi e possono essere raggiunti in modalità differenti e con costi differenti, a seconda della disponibilità dell'informazione che si vuole raggiungere. Inoltre questo livello di sicurezza cambia a seconda del ciclo di vita dell'informazione stessa e di questo bisogna tener conto. Si parla quindi di back up, di disaster recovery, di business continuity, di encryption. Inoltre i clienti hanno la necessità di semplificare ed unificare lo storage rendendolo multifunzione e scalabile.

-
- Roberto Salucci, Solution Consultant di Hitachi Data Systems.

"Lo storage che fa bene al business".

-
- Roberto Caso, Professore Associato di Diritto Privato Comparato presso la Facoltà di Giurisprudenza dell'Università degli Studi di Trento

"Forme di controllo delle informazioni digitali: il Digital Rights Management"

Attualmente è in atto una guerra per il controllo dell'informazione digitale. Da una parte c'è chi vuole mantenere e rafforzare il controllo privato, basato sulla proprietà esclusiva, dall'altra c'è chi ritiene che le tecnologie informatiche sono alla base di una vera e propria rivoluzione, la quale muta il mercato e le istituzioni sulle quali esso tradizionalmente si fonda - la proprietà privata e il contratto - e determina la necessità di un controllo distribuito dell'informazione, basato su nuove istituzioni; alcuni dicono: su una nuova forma di proprietà paragonabile alle antiche proprietà collettive (commons).

Il controllo delle informazioni digitali si basa principalmente su tre strumenti normativi: il contratto, le leggi sulla proprietà intellettuale (per quel che più rileva in questo ragionamento, il copyright) e gli standard tecnologici (in particolare, quelli che riguardano le misure tecnologiche di protezione). La scelta a favore di un controllo privato (e rigido) o di un controllo distribuito (ed elastico) dell'informazione digitale dipende dal modo in cui vengono configurati e coordinati questi tre strumenti.

Nei sistemi di Digital Rights Management la configurazione ed il coordinamento sono puntati ad esasperare il controllo privato delle informazioni. Licenze d'uso sui contenuti, licenze d'uso sui sistemi di DRM,

standard delle varie componenti dei sistemi di DRM e leggi sulla tutela giuridica delle misure tecnologiche di protezione (in particolare, Digital Millennium Copyright Act del 1998 e Dir. 29/2001) distruggono il bilanciamento degli interessi che è alla base del copyright. In particolare, contraddicono la tradizione giuridica e la logica economica che predicano la limitazione del copyright. Inoltre, la regolamentazione derivante dai sistemi di DRM funziona necessariamente in modo diverso dalle regole tradizionali: allo stato attuale non è possibile incorporare nella tecnologia regole elastiche come principi giuridici e norme sociali. Infine, i sistemi di DRM pongono problemi sul piano della privacy, del diritto antitrust e della regolamentazione di Internet.

-
- Manuel Leone, Security Program Manager di Telecom Italia - Security Innovation e
 - Pierluigi Urizio, Business Development Manager del Gruppo Italtel

"DDoS Mitigation: il valore della connettività"

La connettività di rete rappresenta ormai una condizione imprescindibile per il business della maggior parte delle aziende. Non a caso negli ultimi anni il Distributed Denial of Service ha fortemente catalizzato la creatività di "buoni" e "cattivi". In questo intervento affronteremo l'evoluzione degli attacchi Denial of Service ed analizzeremo i paradigmi piu' promettenti per il loro contenimento. In particolare approfondiremo le tecniche di tipo network-centric, a dimostrazione del fatto che non solo il problema, ma anche la sua soluzione puo' provenire dalla rete.

Seguirà sessione di domande e risposte tra i relatori ed il pubblico.

Mercoledì 6 giugno – 10.30-13.00

"La Computer forensic in azienda"

Nato come settore per fornire i necessari supporti alle forze dell'ordine coinvolte nell'investigazione di computer crime la computer forensic sta ora trovando applicazioni particolarmente accattivanti in ambito aziendale, con particolare riferimento all'individuazione di attività di spionaggio industriale o abuso delle risorse aziendali. Per svolgere questa attività però è necessario avere un importante bagaglio di competenze in campo tecnologico ma anche legale al fine di non svolgere attività che finiscano con il ledere i diritti degli interessati. Di questi temi si tratterà nel corso di questo evento a cui parteciperanno sia produttori di tecnologie che rappresentanti del mondo legale.

Moderatore: Gigi Tagliapietra, Presidente Clusit

Relatori:

- Giovanni Ziccardi, Professore Associato di Informatica Giuridica e Informatica Giuridica Avanzata presso la Facoltà di Giurisprudenza dell'Università degli Studi di Milano.

"La computer and network forensics e le investigazioni digitali tra tecnologia, diritto, etica e responsabilità: un approccio accademico"

In questo intervento Giovanni Ziccardi affronterà le tematiche della computer and network forensics e delle investigazioni digitali con un

approccio accademico: analisi delle definizioni, evoluzione scientifica della materia, rapporti con il diritto, problemi etici e di responsabilità.

-
- Sandro De Santis, IT Certified Specialist, IBM Systems & Technology Group

"Soluzioni storage per la prevenzione dei crimini informatici"

Prevenire è meglio che curare: panoramica con esempi delle soluzioni e delle tecnologie storage che sono state sviluppate per prevenire la perdita, cancellazione, alterazione non autorizzate ed accessi fraudolenti alle risorse di memorizzazione. Come è possibile proteggere i contenuti dei dispositivi di memoria facilmente asportabili ed utilizzati per il trasporto sicuro delle informazioni. Soluzioni software per il controllo diretto delle risorse di memorizzazione al fine di prevenire utilizzi non conformi alle politiche aziendali e alle normative vigenti.

-
- Gerardo Costabile, CIFI Poste Italiane Spa Security & Safety - Responsabile Sicurezza Logica - Presidente Italian Chapter IISFA (www.iisfa.it)

"Information Forensics aziendale: graduazione dei controlli interni alla luce delle nuove indicazioni del Garante della Privacy"

Il primo marzo il Garante della Privacy ha emanato le linee guida circa l'utilizzo della posta elettronica e di internet negli ambienti di lavoro, a completamento di un lavoro di raccolta ed armonizzazione delle indicazioni emanate nel tempo in materia di protezione dei dati dei dipendenti e di controllo datoriale. L'utilizzo di Internet e della posta elettronica da parte dei lavoratori può potenzialmente formare oggetto di analisi, profilazione e integrale ricostruzione, generalmente mediante elaborazione di file di log. Appare necessario, da parte del datore di lavoro nell'ambito dei cosiddetti controlli difensivi, ispirarsi a principi di trasparenza, pertinenza, non eccedenza, indicando le ragioni legittime - specifiche e non generiche- per cui gli stessi verrebbero effettuati e le relative modalità. Nell'effettuare controlli sull'uso degli strumenti elettronici dovrà essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. Il Garante Privacy indica che, nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro potrà adottare eventuali misure che consentano la verifica di comportamenti anomali, preferendo ove possibile un controllo preliminare su dati aggregati (il c.d. controllo graduale), riferiti all'intera struttura lavorativa o a sue aree. L'intervento si ispira a tali indicazioni, approfondendo l'applicabilità in un contesto di Information Security Governance in una organizzazione aziendale complessa. Sarà poi illustrato un case study di un incidente informatico aziendale da parte di un insider.

-
- Danilo Bruschi e Mattia Monga, Cert.It – Computer Emergency Response Team Italy, Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano

"Forensic in Azienda: alcune esperienze del Cert.It"

Seguirà sessione di domande e risposte tra i relatori ed il pubblico.

Mercoledì 6 giugno – 14.30-17.30

"La sicurezza nella PA: le ultime iniziative"

Sicuramente tra i settori con un maggiore tasso d'innovazione la PA è anche un settore che ha prestato molta attenzione al settore della sicurezza informatica. Nell'ambito di questo convegno saranno presentate le ultime iniziative intraprese in questo importante settore in ambito di sicurezza privilegiando le iniziative di portata nazionale.

Moderatore: Claudio Manganelli, Componente del CNIPA, già Presidente del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle PA.

Relatori:

- Emilio Frezza, Responsabile dell'Area "Infrastrutture nazionali condivise" del CNIPA, che ci aggiornerà sulle iniziative di sicurezza nell'ambito del progetto "Sistema Pubblico di Connettività" (SPC), in fase di realizzazione.
- Guido Orsi, Adobe Systems Italia

"La protezione persistente dei documenti nel ciclo di vita documentale della Pubblica Amministrazione"

Il relatore, durante il suo intervento, affronterà e illustrerà casi concreti realizzati nell'ambito della Pubblica Amministrazione

-
- William Gabriele, Channel Sales Manager RSA Italy

"Security Compliance e Data Protection. L'approccio RSA"

-
- Gianfranco Pontevolpe, Responsabile dell'Ufficio Tecnologie per la sicurezza del CNIPA, che presenterà i risultati di un'indagine sulla sicurezza informatica nella Pubblica Amministrazione
 - Tiberio MolinoRuolo, PMM Trend Micro

"Next Generation Security Solutions e Pubblica Amministrazione"

Le soluzioni di ultima generazione si possono applicare anche senza grandi investimenti. Come? Sfruttando i servizi dei security vendors e le loro partnership.

-
- Giuseppe Rossano, Corporate Account Manager Citrix Systems

"Rendere più sicura la PDL grazie alla Virtualizzazione"

Nel corso dell' intervento si affronteranno i seguenti temi:

- Benefici di sicurezza di una infrastruttura di Application Delivery;
- Sicurezza dei dati e delle applicazioni aumentando la Mobilità dei propri collaboratori e dipendenti;
- Abilitazione al Telelavoro sicuro;
- Continuità di esercizio e Disaster Recovery.

Seguirà sessione di domande e risposte tra i relatori ed il pubblico.

3. IL CLUSIT IN VISITA ALL'ITU

Nel corso delle ultime settimane Paolo Giudice, segretario generale del Clusit, ha avuto occasione di incontrare le più alte istanze dell'ITU (International Telecommunication Union).

L'incontro è stato estremamente cordiale e costruttivo ed è emerso che per il Segretario Generale dell'ITU, Mr. Hamadoun Touré, entrato in funzione all'inizio dell'anno, la sicurezza delle informazioni e la lotta al cybercrime sono tra le priorità del suo mandato.

A tal proposito, segnaliamo: www.itu.int/cybersecurity/itu_activities.html

Paolo Giudice, che ha incontrato l'ITU su incarico del Ministero delle Comunicazioni, ha avuto modo di presentare i CLUSI ed in particolare il Clusit e le sue attività.

In pratica, il Clusit è ora accreditato presso l'ITU come l'organizzazione di riferimento per la sicurezza delle informazioni in Italia. Inoltre, sono state messe le basi per l'organizzazione di una Conference internazionale sulla Cybersecurity, da tenersi in Italia nel corso del 2008, promossa dall'ITU, dal Ministero delle Comunicazioni e dal Clusit.

4. UN NUOVO QUADERNO CLUSIT

Segnaliamo la pubblicazione di un nuovo Quaderno Clusit:

Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.), scritto dal socio Enzo M. Tieghi.

Una copia del quaderno è stata distribuita ai soci presenti all'assemblea del 30 maggio.

All'indirizzo www.clusit.it/download è disponibile sia il quaderno (con consultazione riservata ai soci) che l'abstract (in consultazione libera).

Dopo 90 giorni dalla pubblicazione la consultazione sarà libera per tutti.

5. SICUREZZA AZIENDALE CON IL SOLE 24 ORE

A seguito di un accordo con Mediaplanet Italia, Clusit sarà il partner editoriale e redazionale dello speciale **Sicurezza Aziendale**, un supplemento distribuito con *Il Sole 24 Ore* il prossimo 2 luglio (prendete nota della data!!).

Lo speciale **Sicurezza Aziendale**, tramite articoli, interviste e business cases, affronterà i seguenti temi:

- IT Security (Network, Processi e Accessi, Firewalls, Antivirus, Vulnerability Assets)
- Business Recovery & Continuity
- Strategie e Risk Management
- Assicurazioni Aziendali
- Protezione dei beni, informazioni e accesso (Sistemi di sorveglianza)
- Certificazioni di Sicurezza.

6. EVENTI SICUREZZA

5-6 giugno 2007, Roma - **INFOSECURITY Roma**

www.infosecurity.it/IT/roadshow/programma.aspx

6 giugno 2007, Roma - Seminario CLUSIT

Il Social Engineering e la sua applicazione nel penetration testing professionale

https://edu.clusit.it/scheda_seminario.php?id=8

14 giugno 2007, Milano - Seminario CLUSIT

Computer forensic: aggiornamenti

https://edu.clusit.it/scheda_seminario.php?id=9

20 giugno 2007, Roma - Seminario CLUSIT

Computer forensic: aggiornamenti

https://edu.clusit.it/scheda_seminario.php?id=10

21-22 giugno 2007, Castel San Pietro Terme (BO)

Primo Forum Internazionale sull'identificazione digitale

www.clusit.it/eventi/070621_digidal.pdf

26 giugno 2007, Segrate (MI) - **La Security nei sistemi di controllo ed automazione, nelle reti ed infrastrutture**

www.anipla.it/FILE_ANIPLA/FILE_MENU/File_Archivio/PROG/2007/gds_26-06-07.pdf

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO - cell. 347.2319285

* associazione senza fini di lucro, costituita il 4 luglio 2000

© 2007 Clusit - Vietata la riproduzione

Clausola di esclusione della responsabilità e informazioni relative al

Copyright: www.clusit.it/disclaimer.htm