SPECIALE

ROMA

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni al **Security Summit di Roma**, che si terrà nei giorni 9 e 10 giugno presso l'**SGM Conference Center** www.sgmconferencecenter.it

La partecipazione al Security Summit e a tutti gli eventi che lo compongono è libera e gratuita, con il solo obbligo di iscriversi online su https://www.securitysummit.it

Per chi vuole rivivere in parte il Summit di Milano in marzo, ricordiamo che sU http://milano.securitysummit.it/page/video sono disponibili i video degli interventi dei keynote: Mark Abene, Pascal Lointier e Sharon Conheady. Sono pure disponibili alcune Videointerviste.

Sul gruppo SECURITY SUMMIT su Facebook www.facebook.com/group.php?gid=64807913680, troverete una vasta raccolta di foto.

Gli atti delle sessioni formative e degli atelier e convegni di Milano sono disponibili su http://milano.securitysummit.it/page/atti_milano_2010.

2. PROGRAMMA DEL 9 GIUGNO

09.00 Registrazione - Welcome Coffee

09.45-12.45 MANIFESTAZIONE DI APERTURA

In apertura del Summit è prevista una tavola rotonda d'eccezione dal titolo «Sicurezza delle informazioni e della rete: nuove sfide per le istituzioni e le imprese».

Nel corso della tavola rotonda, cui parteciperanno rappresentanti del Governo, delle Istituzioni di riferimento e delle Imprese, e che vedrà come ospite d'onore Udo Helmbrecht, il nuovo direttore dell'ENISA (l'Agenzia Europea per la Sicurezza delle reti e delle informazioni), verrà affrontato il tema della protezione delle informazioni e della sicurezza della rete: quale è la situazione odierna e quali i piani progettuali perchè la sicurezza ICT sia parte integrante del processo di innovazione tecnologica nel nostro Paese?

Abbiamo invitato :

- Paolo Romani, Vice Ministro, per l'apertura dei lavori
- Udo Helmbrecht, nuovo direttore dell'ENISA, ospite d'onore della manifestazione
- Rita Forsi, Direttore dell'ISCOM, Direttore Generale Ministero per lo Sviluppo Economico
- Francesco Pizzetti, presidente dell'Autorità Garante per la protezione dei dati personali
- Antonio Apruzzese, direttore della Polizia Postale e delle Comunicazioni
- Gigi Tagliapietra, presidente Clusit, moderatore della tavola rotonda.

Interverranno anche:

- Marco Bresciani, Partner Accenture Technology Consulting, global offering lead per i servizi di Security Strategy e Risk Management
- Kristin Lovejoy, VicePresident IBM Global Security Strategy
- Cesare Ottaviani, Business Unit Security Director CA
- Alessandro Vallega, coordinatore della Oracle Community for Security

13.00-14.30 LUNCH-BUFFET e visita all'area espositiva

14.30-16.30 PERCORSO PROFESSIONALE TECNICO: 1a sessione

"La tutela delle informazioni classificate e l'evoluzione dei Common criteria"

Nel corso della presente sessione sarà fornita agli astanti una introduzione ai Common Criteria contestualizzati nello Schema Nazionale per la tutela delle informazioni classificate di cui al DPCM 11 Aprile 2002. Dopo un excursus storico del perché e di come si è giunti ai Common Criteria sarà fornito un quadro di situazione relativo al citato Schema Nazionale e una descrizione dello Standard ISO 15408. Concluderà la presentazione una breve descrizione di come si è evoluto lo standard nelle diverse versioni a fronte dell'adozione di nuove tecnologie e nuove esigenze di sicurezza.

Docenti : Stefano Ramacciotti, Luciano Porcelli.

14.30-16.30 TAVOLA ROTONDA

Cybersecurity vs Infrastrutture Critiche Nazionali: come difendersi e prevenire i possibili impatti

La tavola rotonda è finalizzata alla individuazione di come si sta procedendo in materia di protezione delle infrastrutture critiche nazionali sia in ambito internazionale che nazionale, e cosa dovrà necessariamente essere attuato per prevenire i possibili impatti derivanti da minacce naturali e intenzionali (es.: spionaggio industriale, terrorismo, criminalità organizzata). Verranno quindi analizzate le modalità con cui Enti, Imprese, strutture nevralgiche nazionali e loro partner, pianificando ed attuando idonee e preventive contromisure di CyberSecurity, possano contribuire a difendere asset nazionali e potenziali obiettivi sensibili, mitigando il rischio di subire danni con ricadute sul sistema sociale ed economico/produttivo dell'intero paese.

Coordinano la TR: Raoul Chiesa e Michele Bianco

14.30-16.30 TAVOLA ROTONDA a cura di ANSSAIF

L'uso degli strumenti di socialnetworking in azienda: opportunità e rischi

14.30-15.15 ATELIER TECNOLOGICO a cura dell'Oracle Community For Security

- **Frodi Interne: dalla raccolta degli eventi alla gestione dell'incidente**

Per una opportuna gestione delle criticità di sicurezza, è necessario che gli eventi prodotti dalle differenti piattaforme siano monitorati ed analizzati. Il sistema FRAUD GATE l'osservatore ideale: un sistema fornito di un motore a regole dinamiche per caricare ed elaborare i dati correlandoli con altri e per assegnare loro l'esatto scoring delle criticità rilevale. Il FRAUD GATE visualizza grafici dinamici ed evidenzia le segnalazioni differenziandole in base alla criticità: il primo punto per l'evidenza di un incidente e la relativa gestione passando tramite piani di mitigazione, investigazione ed Information Forensics."

Docente: Wilmana Malatesta (Visiant Security)

- **Le nuove frontiere della sicurezza: evoluzione da infrastruttura a dati e applicazioni, Owasp Top Ten - new release**

Spesso ci domandiamo: i nostri pc sono sicuri rispetto agli hacker? Se uso il conto corrente on line, mi possono depredare? Sono dubbi legittimi, ma è solo la punta dell'iceberg.Infatti appare palese che, mentre la nostra infrastruttura digitale diventa sempre più complessa ed interconnessa, le sfide legate ad una adeguata sicurezza applicativa aumentano esponenzialmente. L'Open Web Application Security Project (OWASP) è un'organizzazione mondiale no profit, che si pone come obiettivo il miglioramento continuo della sicurezza delle applicazioni software. La sua missione è proprio quella di evidenziare sfide e criticità legate ai temi della sicurezza applicativa, in modo da permettere a imprese e organizzazioni di prendere decisioni efficaci e adottare soluzioni concrete per contrastarne i rischi.

Docente: Lucilla Mancini (Business-e)

15.30-16.30 ATELIER TECNOLOGICO a cura di IBM

Cloud Security Computing

Il Cloud Computing si sta affermando come un nuovo modello di consumo che attrae sempre più aziende.

Il principio alla base del Cloud è che risorse di computing come processore e memoria così come risorse di storage sono erogate on demand e mantenute solo finché necessarie. Questo nuovo paradigma se da un lato sta trasformando il modo di lavorare dell l'IT grazie a due concetti quali scalabilità senza bisogno d'infrastruttura interna e accesso globale, dall'altro porta degli impatti non trascurabili sulla sicurezza e sulle metodologie e tecnologie sinora utilizzate,richiedendo sempre più una visione della sicurezza interdisciplinare ed integrata. L'intervento descrive alcuni degli impatti più significativi che il cloud ha introdotto nella sicurezza e nelle infrastrutture odierne fornendo una overview dei possibili approcci metodologici e delle soluzioni ad oggi disponibili per mitigare eventuali esposizioni.

Docenti: Andrea Carmignani, Cesare Radaelli

Seguono:

17.30-19.30 HACKING FILM FESTIVAL

19.30-20.30 APERITIVO con degustazione di birre artigianali

3. PROGRAMMA DEL 10 GIUGNO

09:00 Registrazione

09.30-11.00

PERCORSO PROFESSIONALE TECNICO: 2a sessione

Il Content Security dall'ambiente fisico al virtuale : come approcciare le nuove sfide ?

Docenti: Alessio Pennasilico, Gastone Nencini

9.30-11.00 TAVOLA ROTONDA

Il ritorno degli investimenti in sicurezza informatica (ROSI)

Ancora oggi, i CISO e i CSO delle aziende fanno leva in particolare sulla gestione dei rischi e sulla necessità di adempiere ad obblighi normativi, per giustificare la richiesta di investimenti in sicurezza dei sistemi informativi. Il ritorno dell'investimento è raramente preso in considerazione, a causa della difficile dimostrabilità dello stesso e della complessità della materia. Eppure, sono sempre più le Direzioni Generali delle aziende che chiedono, e spesso pretendono, una giustificazione quantitativa del ritorno dell'investimento. E in momenti di crisi economica, e quindi di maggior attenzione all'allocazione dei budget, il management delle aziende, in mancanza di tale giustificazione quantitativa, tende a non intraprendere nuovi progetti in ambito sicurezza informatica. Nel corso di questa sessione si daranno indicazioni utili per le aziende per il calcolo del ROSI all'inteno dei propri progetti di sicurezza. Non si pretende di fornire uno strumento preciso, ma almeno una serie di indicazioni sulla metodologia da utilizzare e sui fattori da prendere in considerazione per calcolare il ROSI.

Partecipano: Mauro Cicognini, Pierluigi Lonero, Andrea Longhi, Alberto Piamonte, Alessandro Vallega.

9.30-11.00 TAVOLA ROTONDA per la PA (ma non solo)

Impatti della direttiva europea relativa ai servizi nel mercato interno (123/2006 sull'Identità Digitale)

La Direttiva Europea relativa ai servizi nel mercato interno (N. 123/2006) recentemente recepita in tutti gli Stati Membri dell' UE. introduce interessanti nuovi scenari sull'identità digitale. Oltre a questo la Direttiva stessa richiede agli Stati che ci sia interoperabilità "cross-border". Quest'ultimo aspetto richiede che l'identità digitale sia gestita in termini di attribuzione delle credenziali a un soggetto, gestione delle medesime credenziali, controllo della gestione delle credenziali da parte di un terzo. Inoltre deve essere definito il profilo del documento informatico oggetto delle transazioni e il suo valore legale "europeo" nell'ambito del

procedimento. Nella tavola rotonda in oggetto, il tema viene approfondito dal punto di vista generale, da quella della sicurezza ICT, della protezione dei dati personali. Infine viene descritto lo stato dell'arte europeo, al massimo livello di aggiornamento, mediante la testimonianza diretta di DigitPA che partecipa al tavolo di esperti insediato dall'UE per consentire una reale applicazione della Direttiva.

Moderatore : Giovanni Manca

Intervengono :

- Giovanni Manca "Introduzione ed aspetti generali"
- Corrado Giustozzi "Quali sono i nuovi scenari e gli impatti sulla sicurezza ICT"
- Cosimo Comella "Il punto di vista del Garante della privacy"
- Stefano Arbia "La testimonianza di DigitPA (ex CNIPA) su come applicare la Direttiva"

11.00-11.30 coffee Break e visita all'area espositiva

11.30-13.15 PERCORSO PROFESSIONALE TECNICO: 3a sessione

Web Application Security: a 2.0 attacker's perspective

Nel seminario verrà analizzata l'evoluzione delle web application dalla comparsa del termine "web 2.0" ad oggi, capendo quali sono i nuovi vettori, le tecniche e gli strumenti di attacco.

Verranno approfonditi in particolare attacchi di tipo XSS (sempre attuali e sempre più pericolosi), il phishing, i nuovi "worm 2.0", gli attacchi drive-by download e la tecnica x-Morphic.

Dopo aver descritto l'evoluzione del "mercato" underground e aver visto alcune tecnologie di protezione si cercherà di rispondere alla domanda "quali informazioni si possono recuperare dal mio browser", scoprendo come la risposta a questa domanda possa portare alla tracciabilità del browser e a nuove problematiche sulla privacy.

Infine verrà fatta un'analisi delle problematiche legate ai social network e alla sicurezza delle informazioni personali e aziendali.

Il programma per punti:

- web 2.0 e nuovi vettori d'attacco (dal 2004 a oggi)
- evoluzione degli attacchi XSS e nuove tecniche di utilizzo: XSS proxy / XSS fingerprinting / XSS tunneling / XSS browser exploitation with Metasploit (demo dei tool BeEF e XSS Shell)
- evoluzione del phishing: dal whaling al SEO poisoning o al phishing nei social network (il mercato underground della pubblicità sulle fanpage di facebook)

- worm 2.0, l'evoluzione dei worm e gli attacchi anti automation (anti capctha e logical attacks)
- evoluzione del "mercato" underground del malware e delle minaccie
- attacchi tipo drive-by download, tecnica x-Morphic e relative tecnologie di protezione
- quali informazioni si possono recuperare dal mio browser?
- Problematiche sulla privacy legate all'unicità e alla conseguente tracciabilità dei browser.
- social network e la sicurezza delle informazioni (le api di facebook)
- il social penetration test (che cosa è) e conclusioni

Docenti: Alessandro Gai, Simone Riccetti

11.30-13.15 PERCORSO PROFESSIONALE TECNICO: 4a sessione

Data Loss Prevention: Cos'è, quando serve, i vantaggi, come scegliere e introdurre le soluzioni DLP in azienda

Obiettivo del seminario è fare chiarezza sulla famiglia di tecnologie DLP, per chiarire quali siano gli elementi di novità e le peculiarità rispetto agli strumenti di sicurezza già presenti in azienda. A partire da una serie di scenari di riferimento, saranno identificati gli ambiti nei quali la Data Loss Prevention può offrire un reale innalzamento del livello di sicurezza e verso quali tipologie di minacce e rischi si contrappone. Sempre sulla traccia degli scenari di partenza, sarà dedicata buona parte del seminario alla descrizione dei requisiti che l'azienda deve soddisfare per trarre, dalle soluzioni DLP, reale efficacia: tali requisiti saranno inseriti nell'ambito di un processo ideale di definizione degli obiettivi di sicurezza rispetto ai quali tali soluzioni possono offrire delle valide risposte e, conseguentemente, i criteri per disegnare, a partire dal contesto in essere, la soluzione tecnologica di cui l'azienda ha realmente bisogno. Infine, saranno discussi gli impatti in termini operativi, di processo e tecnologici che derivano dall'integrazione di tali tecnologie in azienda, sulla base di quanto è attualmente disponibile sul mercato. Il seminario sarà svolto in collaborazione con l'azienda Crag Partners che, sulla base degli scenari di riferimento, presenterà al termine il proprio framework consulenziale e di prodotti basati su tecnologia RSA.

Docenti: Luca Bechelli, Roberto Pachì

11.30-13.15 TAVOLA ROTONDA

Il furto di informazioni: impatti legali e organizzativi e tecnologie a supporto

Obiettivo della tavola rotonda è illustrare ai partecipanti (IT Manager e CIO) lo stato dell'arte dell'IT Security all'interno delle aziende, quali sono

le principali minacce per il business come il furto o la fuoriuscita non autorizzata di informazioni aziendali riservate, qual è il trend futuro e qual è la risposta di Sophos a queste problematiche.

Moderatore: Laura Ciarallo, giornalista professionista, dal 1996 assunta nella redazione del TG5 dove svolge attualmente le mansioni di vice-caporedattore della redazione economica.

Partecipano:

- Angelo Jannone, professore presso l'Università di Roma "La Sapienza",consulente di Corporate Governance, Security & Compliance e direttore operativo di Commetodi S.p.A, che tratterà gli impatti legali e organizzativi del furto di informazioni aziendali
- Marco Fagiolo, Responsabile della Delivery dei Servizi ICT e ICT Security Manager di Finmeccanica Corporate, che spiegherà come il gruppo Finmeccanica sta affrontando il tema della sicurezza delle informazioni, attivando in maniera preventiva la tecnologia NAC di Sophos
- Mark Harris, VP SophosLabs Sophos, illustrerà l'attività svolta dai SophosLabs
- Walter Narisoni, Sale Engineer Manager South Europe Coordinator Sophos Italia, che illustrerà, a completamento dell'intervento di Mark Harris, quali sono le tecnologie oggi a disposizione per contrastare il fenomeno del furto di informazioni.

13.15-14.45 LUNCH-BUFFET e visita all'area espositiva

14.45-16.45 PERCORSO PROFESSIONALE TECNICO: 5a sessione

Mobile security, il telefono una naturale estensione della propria vita digitale

Docenti: Alessio Pennasilico, Fabio Pietrosanti, Paolo Colombo

14.45-15.45 ATELIER TECNOLOGICO a cura di Clusit e Oracle

PCI-DSS: la norma e la tecnologia

1. Introduzione
   - Frodi e SSC
   - Soggetti coinvolti
   - Carte e processi
2. PCI-DSS
   - Famiglia di standard
   - Applicabilita`
   - Conformita`
   - Requisiti
   - Audit e scansione

- Statistiche e sanzioni
- Materiale a disposizione
- Rapporto con altri standard
- Snapshot del Mercato
- Pro e Contro

3. Alcune Soluzioni tecnologiche per la PCI-DSS
   - Cifratura dati in transito e nel database
   - Separazione dei ruoli
   - Accesso ai dati per classificazione degli utenti
   - Funzionalita` di auditing
   - Mascheramento dei dati
   - Gestione delle identita` e controllo accessi
   - Gestione della sicurezza dei documenti

Docenti: Fabio Guasconi, Alfredo Valenza

14.45-15.45 ATELIER TECNOLOGICO a cura dell'Oracle Community For Security

➢ **Log-management per il Rischio e la Compliance**

Il log-management è una parte sempre più importante nella gestione delle informazioni tecnologiche e di business all'interno dell'azienda. Ogni apparato, software e applicazione genera log che identifica in modo preciso chi li utilizza, quello che fanno e quando lo fanno. Inoltre i log registrano le attività dei sistemi e rende queste informazioni preziose per la risoluzione dei problemi IT. Ma per gli IT manager la sfida è la collezione, la normalizzazione, l'aggregazione delle informazioni provenienti dalle differenti fonti log per creare analisi significative e reportistiche utili. I software di gestione dei log sono diventati molto più interessante per i manager nel settore IT negli ultimi anni perché hanno compreso come un processo di raggiungimento e mantenimento della compliance porti una reale riduzione dei rischi.

Docente: Fabio Pierri (Xech)

➢ **L'Identity & Access Management (IAM) fa paura?**

Nonostante indagini di mercato a livello europeo abbiano evidenziato come i progetti in ambito Identity & Access Management abbiano ormai raggiunto un ottimo grado di maturità, molte aziende hanno ancora paura di affrontare adeguatamente problematiche di gestione delle identità e degli accessi ai servizi. Per rispondere alle paure più classiche che insorgono quando si approccia un progetto IAM e fugarle, è necessario mettere in luce i punti deboli di un'infrastruttura sia organizzativa che tecnologica mediante un approccio di Identity Assurance. Identity Management, Web Access Control, Enterprise-Single Sign-On, Strong Authentication, Privileged User Management, Identity Log Management sono solo alcuni dei temi che quasi tutte le societa' di medie e grandi dimensioni devono affrontare, tanto che gia' si parla della next big-thing "Cloud Security". L'Identity Assurance può essere considerata come l'area tematica sotto la quale ricadono quelle che fino a qualche anno fa erano problematiche affrontate singolarmente, spinti da esigenze diverse, dal supporto all'operations sino alla compliance. L'integrazione sempre più profonda di queste aree

progettuali ha raggiunto un livello di maturità tale da consentire un approccio strutturato e strategico alla tematica.

Docente: Andrea Buzzi (Value Team)

15.45-16.45 ATELIER TECNOLOGICO a cura dell'Oracle Community For Security

Il cloud computing: nuovo paradigma e nuovi rischi?

Il cloud computing sarà uno dei modelli di erogazione di servizi informatici con maggiore diffusione nei prossimi anni. Il suo successo sarà determinato principalmente dal fatto che esso si basa su un paradigma incentrato sul servizio erogato agli utenti, che rende trasparenti gli aspetti tecnologici e fisici sottostanti, consentendo all'utilizzatore di concentrarsi sugli aspetti di servizio più che sui dettagli tecnici. Tali caratteristiche, se da un lato rendono particolarmente accattivante il modello, dall'altro, se non opportunamente governate, espongono le aziende ad una serie di rischi, soprattutto in termini di sicurezza delle informazioni e di continuità operativa. L'intervento partirà da un'analisi dei principali modelli di business ed operativi sui quali si basa il cloud computing, per poi identificare i principali rischi ad essi associati, proporre un modello per il loro governo e infine spiegare come far leva sulle infrastrutture esistenti di Identity and Access Management, estendere la Service Oriented Security facendo uso degli standard, per realizzare od utilizzare un cloud sicuro.

Docenti: Valentino Squilloni (Spike Reply) e Domenico Catalano (Oracle/SUN)

15.45-17.45 TAVOLA ROTONDA a cura di IISFA

Computer forensics e digital investigation: aspetti tecnici e giuridici

Partecipano:

- Gerardo Costabile, Presidente IISFA Italia - Responsabile Sicurezza Logica Poste Italiane, moderatore della tavola rotonda

Apertura dei lavori e presentazione dell'IISFA Survey 2010 - Lo stato dell'arte della computer forensics in Italia

- Massimiliano Graziani, IISFA Board - Computer forensics expert

Cybercop 2008-2010: l'esperienza evolutiva del "gaming" a supporto della formazione e della cultura nella computer forensics

- Litiano Piccin, consulente tecnico - computer forensics expert - IISFA Member

Iphone forensics: tecniche di analisi e di indagine

- Mario Ianulardo, Avvocato in Napoli, Docente all'Università di Salerno

Alibi informatico e aspetti giuridici: casistica italiana ed internazionale

- Stefano Aterno, Avvocato in Roma, Docente all'Università "La Sapienza" di Roma, Vicepresidente IISFA Italia

Computer forensics e Corte di Cassazione: le prime sentenze

17.00-19.00 TAVOLA ROTONDA

Italian Security Professional Group: approfondimento e discussione sul CyberCrime

La criminalità informatica rappresenta oggi una minaccia non solo per singole aziende ed istituzioni ma per interi sistemi economici e politici.

Gli interessi in gioco sono enormi e paragonabili a quelli dei mercati "classici" della criminalità.

Con questo seminario interattivo cercheremo di sfatare alcuni falsi miti sul CyberCrime, discuteremo di possibili soluzioni e scenari futuri.

Introduce e modera: Paolo Colombo, Owner Italian Security Professional

Intervengono:

- Claudio Guarnieri, Ricercatore Indipendente Honeynet Project
- Raoul Chiesa, Permanent Stakeholders' Group ENISA
- Marco Pacchiardo Senior Security Consultant British Telecom

Agenda:

Cybercrime, definizione e progenie

- Cyberwarfare, Cyberespionage
- Esempi reali: South Korea 2009,Operation Aurora, Shadowcrew/Albert Gonzalez

Underground Market

- Ecosistema commerciale del CyberCrime
- Business Case
- Figure professionali coinvolte

Cyberlaundering

- Riciclaggio online
- Strumenti di pagamento anonimi
- Strumenti del CyberCrime
- Botnet e DYI Kit
- Botnet Tracking

Q&A

Il programma è in continuo aggiornamento su https://www.securitysummit.it/

4. HACKING FILM FESTIVAL

E' l'evento culturale "satellite" del Security Summit dedicato ai lungometraggi e documentari indipendenti sul tema dell'hacking e della (in)sicurezza, che per questa prima edizione romana si terrà il 9 giugno dalle 17.30 alle 19.30 e sarà seguito da un aperitivo con degustazione di birre artigianali. Sono in programma tre diversi cortometraggi, opere girate con mezzi modesti e con budget amatoriali ma che sono in grado di illustrare con un realismo non comune tutte le complesse sfaccettature sociali, politiche, giuridiche e tecnologiche di un mondo complesso come quello dell'hacking. Le pellicole saranno presentate e commentate da: Raoul Chiesa, Corrado Giustozzi e Alessio Pennasilico. Al termine delle proiezioni è previsto un collegamento telefonico con Mark Abene, meglio noto come "Phiber Optik", vera e propria leggenda dell'hacking e del phreaking negli anni '90 e co-protagonista in uno dei documentari che verranno proiettati.

L'Hacking Film Festival è realizzato in collaborazione con il Dipartimento di Informatica e Comunicazione dell' Università degli Studi di Milano e la Facoltà di Informatica Giuridica.

Si ringrazia il prof. Giovanni Ziccardi, responsabile scientifico del Festival.

La partecipazione è gratuita previa iscrizione obbligatoria, via mail.

Maggiori informazioni e iscrizioni su
https://www.securitysummit.it/page/hackingfilmfestival.

PROGRAMMA:

Sapere Aude 1784 di mfp&ila, CCC2007, 2007 (durata 10 minuti, in italiano)

Uno "Short emotional trip", come lo definiscono gli Autori: 10 minuti di musica a rappresentare 5 giorni di "recursive knowledge". Un giornalista-radio polacco parla del CCC 2007 (Chaos Computer Club Camp) come l'esempio vivente che "una societa' aperta, ideale" sia possibile...
www.olografix.org/sapereaude

Unauthorized Access di Annaliza Savage, 1994 (versione di 15 minuti, con sottotitoli in italiano)

Opera prima di Annaliza Savage ed uno dei primissimi documentari sull'hacking, il phreaking ed il trashing nella prima metà degli anni '90. I MOD & LOD, Kevin Poulsen... tanti i protagonisti di questo indimenticabile documentario, girato tra gli USA, l'Olanda e la Germania...quando il blue-boxing era ancora una realtà.
http://carnal0wnage.blogspot.com/2009/10/annaliza-savage-unauthorized-access.html
www.imdb.com/name/nm0767244

Hackers: Outlaws and Angels, 2002 (durata 46 minuti, in inglese)

Questo documentario, della Discovery Channel Production, svela le battaglie quotidiane tra i "bad guys" e gli hacker che si oppongono, formando i professionisti dell'IT ed il Law Enforcement, controllando il cyberspazio alla ricerca di segno di infowar imminenti. Interviste quindi ai protagonisti di questa "guerra invisibile", tra cui il DoD USA, il NYPD, i detective della Kroll Associates, il team dell'X-Force e svariati hacker e cracker conosciuti nel settore.
www.youtube.com/results?search_query=Hackers%3A+Outlaws+and+Angels+&search_type=&aq=f
www.youtube.com/watch?v=14h-ksuHpbA
http://movies.nytimes.com/movie/278330/Hackers-Outlaws-and-Angels/overview

Al termine delle proiezioni ci sarà un aperitivo con degustazione di birre artigianali.

5. ATTESTATI E CREDITI CPE

Le sessioni che prevedono il rilascio di Attestati di Presenza e l'attribuzione di Crediti CPE sono: i Percorsi Professionali tecnici e gli Atelier Tecnologici.

Tutte queste sessioni sono tenute da esperti del mondo accademico e da professionisti del settore e danno diritto a crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua.

L'Attestato di Partecipazione viene rilasciato al termine di ciascuna sessione solo a chi ha assistito all'intera sessione/atelier/seminario e risulta regolarmente registrato.

La registrazione è possibile solo online sul portale http://securitysummit.it/ e non sono accettate altre modalità di registrazione come email o fax.

Le registrazioni potranno essere accettate anche direttamente alla Reception del Security Summit, ma non potrà essere garantita la disponibilità del posto in sala, né la consegna immediata dell'attestato.

6. GLI SPONSOR DEL SECURITY SUMMIT

Sponsor Partner:

Sponsor Platinum:

Sponsor Silver:

Sponsor dell'Hacking Film Festival:

All'interno dell'SGM Conference Center è previsto uno spazio espositivo a disposizione delle aziende sponsor, in cui incontrare i partecipanti al Security Summit, illustrare i loro prodotti, svolgere dimostrazioni e presentazioni.

Per chi lo desidera, è possibile fissare in anticipo degli incontri, della durata di circa 20 minuti. Per maggiori informazioni e per prenotarsi: https://www.securitysummit.it/page/spazio_espositivo.

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