SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

ROMA 2013

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni al Security Summit di Roma, che si terrà nei giorni 5 e 6 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/user/register

2. PROGRAMMA DEL 5 GIUGNO

09.00 Registrazione - Welcome Coffee

09:45-12:30 - AUDITORIUM - CONVEGNO DI APERTURA - TAVOLA ROTONDA

"La sicurezza ICT e le proposte per l'Agenda Digitale e l'innovazione in Italia"

Il convegno di apertura del Summit sarà costituito da una Tavola Rotonda sul tema della protezione delle informazioni e della sicurezza della rete in una società che va verso una digitalizzazione globale e servizi di e-government sempre più estesi: quali sono le principali minacce e quali le iniziative ed i consigli di istituzioni ed operatori del settore per proteggere le aziende e gli utenti finali.

Si inizierà con la presentazione del Rapporto Clusit 2013, passando quindi alle iniziative dell'Agenda Digitale e più in generale a quali sono le priorità per 2013 e 2014.

La Tavola Rotonda, moderata da Gigi Tagliapietra, vedrà la partecipazione, oltre che di alcuni esperti del settore, dei vertici delle Istituzioni italiane di riferimento su Agenda Digitale, Contrasto al Cyber Crime, Protezione dei Dati Personali.
Abbiamo invitato:

- **Agostino Ragosa, Direttore Generale dell'Agenzia per l'Italia Digitale**
- **Antonio Apruzzese, Direttore della Polizia Postale e delle Comunicazioni**
- **Antonello Soro, Presidente dell'Autorità Garante per la protezione dei dati personali**
- **Stefano Parisi, Presidente di Confindustria Digitale**

Tutti i partecipanti potranno ritirare una copia del Rapporto Clusit 2013 sulla sicurezza ICT in Italia (fino ad esaurimento)

12.30-14.00 LUNCH-BUFFET e visita all'area espositiva

14:00-15:30 - PERCORSO PROFESSIONALE TECNICO

"Test di sicurezza in ambienti Smart Grid e SCADA"

I sistemi Supervisory Control Data Acquisition (SCADA), ampiamenti utilizzati sia nel settore delle Utility che in ambiente industriale, sono da sempre considerati critici a dalla loro affidabilità dipende non solo la correttezza del controllo di processo, ma spesso anche l'erogazione di servizi vitali per le persone. La criticità e al tempo stesso la "fragilità" che caratterizza questi sistemi e architetture li rende un facile bersaglio per

organizzazioni di "cyber" criminali e script kiddies. In questo contesto è fondamentale poter "misurare" lo stato di sicurezza attraverso test specifici per questi ambienti che coprano sia la sfera tecnologia che di processo, per poi entrare nella parte più ostica: la soluzione compatibile con i requisiti funzionali. Dopo una panoramica sulle tipiche minacce e vulnerabilità, in questa sessione analizzeremo anche tematiche di analisi e gestione del rischio e andremo a fondo su come i test di sicurezza di tipo penetration test debbano essere adattati in questo ambito di applicazione.

Docenti: Alessandro Gai e Simone Riccetti

14:00-15:30 - PERCORSO PROFESSIONALE TECNICO

"Quando inizi ad accettare l'impossibile, rischi di scoprire la verità (sulla sicurezza delle applicazioni in the cloud)"

A quale layer proteggi le tue informazioni in the Cloud? A quali livelli puoi accedere? Che tu sia un Cloud Provider, un utilizzatore, o un'organizzazione che ha un proprio private cloud, di certo vuoi garantire la confidenzialità, l'integrità e la disponibilità delle informazioni gestite. A seconda della soluzione adottata puoi o non puoi adottare alcuni accorgimenti. Come districarsi dunque, al fine di fronteggiare il maggior numero di minacce possibile? Cercheremo di esporre i rischi, alcune soluzioni e la loro fattibilità nei diversi contesti...

Docenti: Alessio Pennasilico e Fabrizio Fiorucci

14:00-15:30 - PERCORSO PROFESSIONALE SULLA GESTIONE DELLA SICUREZZA

"Dall'Access Governance al Fraud Management: un approccio innovativo e globale nella gestione della sicurezza aziendale"

Docenti: Andrea Zapparoli Manzoni, Paolo Chieregatti, Filippo Giannelli

15.30-16.00 Visita all'area espositiva

16:00-17:30 - TAVOLA ROTONDA

Una tavola rotonda a cura della AFCEA (Armed Forces Communications and Electronics Association) Rome Chapter e CDTI di Roma, con il patrocinio del Cloud Security Alliance Italy Chapter.

"Cyber Defence over Clouds: a feasible marriage?"

Il Cloud Computing è considerato ormai un processo irreversibile di innovazione dell'ICT il cui mercato procede con un ritmo di crescita decisamente superiore al mercato ICT tradizionale, che in questi ultimi anni ha evidenziato anzi trend negativi. Nel settore della Difesa, in particolare negli USA, sono già stati avviati studi e valutazioni preliminari

sull'adozione di questo nuovo paradigma, portando in alcuni casi sia all'elaborazione di strategie sull'adozione (DoD - Cloud Computing Strategy) sia all'avviamento di progetti cloud per la razionalizzazione ed efficientamento delle infrastrutture ICT preesistenti (DISA).

Nella tavola rotonda verranno discusse le opportunità, i rischi e le strategie di adozione del paradigma cloud computing nella Difesa Italiana.

Nella prima parte del confronto, si discuteranno le opportunità di utilizzare il cloud in particolare nell'ambito delle infrastrutture e servizi ICT a supporto dell'Amministrazione. Successivamente verranno analizzati i requisiti di sicurezza cloud richiesti per l'implementazione e la distribuzione di servizi XaaS nel contesto Difesa. Il dibattito si concluderà con lo stato dell'offerta e metodi di valutazione dei Cloud Provider per la Difesa.

Modera: Lucilla Mancini, co-founder e responsabile comunicazione e marketing CSA

Partecipano:

- Gen. Pietro Finocchio, Presidente di AFCEA Capitolo di Roma e Executive Committee Member di AFCEA International
- Alberto Manfredi, Presidente di CSA Italy
- Leandro Aglieri, Presidente Rete di Imprese Cloud4Defence
- Amm. Edoardo Compiani, Comandante del C4 Difesa (TBC)
- Alessandro Musumeci, CIO Ferrovie dello Stato e Presidente del CDTI di Roma
- Simone Battiferri, Executive Vice President Business, Telecom Italia (TBC)
- Andrea Rigoni, Director General of Global Cyber Security Center Poste
- Luigi Lupoli, Responsabile Business Development Selex ES
- Carlo Maria Medaglia, Professore Associato Facoltà di Ingegneria dell'Informazione, Informatica e Statistica "Sapienza" Università di Roma e Direttore Scientifico del CATTID

16:00-17:30 - PERCORSO PROFESSIONALE TECNICO

"Digital Forensics e Criminal Profiling: analisi di casi pratici"

Questa presentazione "a 3 voci" vuole porre l'attenzione su alcuni aspetti spesso poco trattati quando si analizzano casi di reati informatici, o reati nei quali il "mezzo informatico" (e di TLC) contiene la c.d. "digital evidence": il comportamento informatico dei soggetti indagati e/o per i quali è stata predisposta dall'Autorita' Giudiziaria un'acquisizione e conseguente analisi forense degli strumenti informatici.

I tre relatori non vogliono però fermarsi qui ed, uscendo dal contesto prettamente giudiziario, vogliono fornire idee e spunti di riflessione alle aziende ed ai professionisti della sicurezza informatica: il tuo sistema operativo, i tuoi file ed i tuoi modelli organizzativi sono il tuo "human-hash"!

Docenti: Raoul Chiesa, Isabella Corradini, Selene Giupponi

16:00-17:30 - PERCORSO PROFESSIONALE LEGALE

"Privacy: fra novità e giurisprudenza"

Le novità legislative in arrivo a livello di UE sono di grande importanza e potrebbero sensibilmente modificare il panorama giuridico esistente ed è quindi importante iniziare a conoscerle anche al fine, ove possibile, di organizzarsi per il loro recepimento. Nel frattempo, la giurisprudenza in materia di controllo sui lavoratori si evolve ed è interessante un'analisi delle recenti pronunce dei magistrati.

Docente: Gabriele Faggioli

Seguono:

18.00-20.00 HACKING FILM FESTIVAL

20.00-21.00 APERITIVO

3. PROGRAMMA DEL 7 GIUGNO

09:00 Registrazione

09:30-11:00 - PERCORSO PROFESSIONALE TECNICO

"L'utente poco saggio pensa che gli informatici lo boicottino. Come far usare cloud e mobile in azienda, senza farsi odiare e senza mettere a rischio i dati?"

I servizi in the cloud sono meravigliosi: belli, semplici, utili e gratuiti. Troppo spesso, quindi, in azienda si assiste al proliferare di strumenti per uso personale utilizzati dagli utenti, all'insaputa dei Sistemi Informativi, che provocano una emorragia di dati aziendali verso l'esterno, senza alcun controllo.

E' possibile mitigare questa situazione? Cosa si potrebbe fare per tutelare le informazioni senza abbassare il livello di servizio e senza provocare una rivolta armata degli utenti?

Vedremo come l'uso di alcune tecnologie di mercato permetta di gestire correttamente il traffico, i servizi, i dispositivi mobili, il cloud, l'accesso, continuando a garantire almeno i livelli minimi di sicurezza...

Docenti: Alessio Pennasilico e Cristiano Cafferata

09:30-10:15 - ATELIER TECNOLOGICO

"Security Operations Center"

L'intervento descriverà com'è organizzato un SOC che eroga servizi di sicurezza gestita. Quali sono i servizi che vengono tipicamente erogati e quali sono i fattori da prendere in considerazione quando si deve scegliere un provider di servizi.

Docente: Davide Del Vecchio

09:30-10:15 - ATELIER TECNOLOGICO

"Certificazioni e profili professionali relativi alla sicurezza informatica: Iniziative normative in ambito nazionale ed internazionale; nuovo quaderno CLUSIT"

E' sempre più chiaro quanto i professionisti che lavorano nell'ambito dell'informatica siano uno dei pilastri della società moderna e si illustrerà come sia l'Europa sia l'Italia si stanno attivando con iniziative normative e legislative per iniziare a regolamentare questo campo. Chi si occupa di sicurezza informatica, a cui spesso è richiesto di provare la propria professionalità anche attraverso molteplici certificazioni professionali verrà inevitabilmente coinvolto in questo processo, a cui esiste tuttavia ancora una possibilità di partecipare attivamente.

Le stesse certificazioni professionali sulla sicurezza informatica saranno inoltre oggetto dell'imminente aggiornamento del quaderno CLUSIT, che sarà anche presentato in anteprima nel corso dell'intervento.

Docente: Fabio Guasconi.

10:15-11:00 - TAVOLA ROTONDA

"Editoria e Sicurezza informatica: cosa sta succedendo in Italia?"

La tavola rotonda vuole fornire uno spazio di dialogo e confronto tra il mondo dell'editoria italiana e quello dell'Information Security.

Partendo dalla positiva collaborazione tra l'editore Hoepli ed il GdL "Cyber World" presso il CASD/OSN, vogliamo capire quale è l'interesse e quali i motivi del connubio tra editoria ed InfoSec.

Modera: Raoul Chiesa

Intervengono:

- Giovanni Hoepli, Hoepli Editore
- Anna La Rosa, Project Officer dell'Osservatorio per la Sicurezza Nazionale (OSN) e Coordinatrice del GdL "Cyber World" presso il CASD/OSN, Min. Difesa
- Giorgio Tosi Beleffi, Ministero dello Sviluppo Economico
- Gen. B. A. Giuseppe Romania, Vice Direttore e Capo Dipartimento di Scienza Tecnica, Economia e Politica Industriale presso il Centro Militare di Studi Strategici del CASD

10:15-11:00 - ATELIER TECNOLOGICO

"La gestione dei dati di traffico telefonico e telematico da parte delle Telco: norme privacy, prescrizioni del Garante, misure di sicurezza"

Nella prima parte dell'Atelier verranno illustrate le norme che regolano il trattamento dei dati di traffico telefonico e telematico da parte delle aziende di telecomunicazioni, in particolare: 1) Quadro normativo europeo ed italiano 2) Norme ed obblighi relativi alla conservazione dei dati per finalità di fatturazione e di giustizia 3) Evasione delle richieste di dati relativi al traffico, soggetti legittimati a richiederli e relative disposizioni 4) Misure di sicurezza specifiche per dati relativi al traffico prescritte dal Garante per la protezione dei dati personali.

Nella seconda parte saranno affrontate le problematiche di carattere tecnico relative alle misure di sicurezza cui sono interessati gli operatori di telecomunicazione.

Docente: Stefano Tagliabue

11.00-11.30 coffee Break e visita all'area espositiva

11:30-13:00 - PERCORSO PROFESSIONALE SULLA GESTIONE DELLA SICUREZZA

"Abbiamo speso bene e dove serviva, per proteggere i nostri dati? Dove e perché: due parole, un percorso, dalla sicurezza dei dati a quella dell'organizzazione"

I dati non sono tutti uguali, e non é lo stesso il valore che questi hanno per l'organizzazione, sia essa una azienda o una Pubblica Amministrazione; spesso però sembra più semplice, o necessario, gestire infrastrutture e servizi senza tenere conto di questo aspetto. Si corre pertanto il rischio di perdere di vista le reali esigenze di protezione e di non disporre di razionali per valutare o quantificare gli investimenti in sicurezza, futuri o passati. Prendiamo una pausa e vediamo come affrontare la questione.

Docenti: Luca Bechelli e Claudio Pantaleo

11:30-12:15 - ATELIER TECNOLOGICO

"Security & Compliance Governance Process Outourcing"

Analisi delle possibilità di esternalizzare attività e operatività di un processo di security & compliance, metodologie di riferimento, piattaforme tecnologiche abilitanti e perimetri di responsabilità

Docente: Francesco Faenzi

11:30-12:15 - ATELIER TECNOLOGICO

"Electronic Signature in Mobile Transaction"

Technical solution I.CA MobileSign is designed for use in all electronic systems that require client authentication or authorization of the transaction without the need to be equipped with additional hardware equipment, such as in connection with banking and business systems, insurance companies and other entities. In the electronic banking systems is a substitute for authorization device (OTP) and SMS. For banking applications in a smartphone enables electronic signature of payment transactions or contracts. In commercial or insurance systems it can be used for electronic signing of various agreements, commitments and requirements or to access protected information.

Docenti: Lenka Capousková e Katerina Jarosová

12:15-13:00 - ATELIER TECNOLOGICO

"Sicurezza & Big Data: la Security Intelligence aiuta le aziende a difendersi dai cyber-attacchi"

Attacchi evoluti, frodi diffuse e uso pervasivo di social media, mobile computing e cloud computing stanno cambiando radicalmente il panorama della sicurezza: cresce la necessità delle aziende di gestire i Big Data e cambia anche il modo di proteggere i dati aziendali. Per aiutare a rilevare le minacce insidiose che possono nascondersi in moli sempre maggiori di dati, sono necessarie funzionalità di correlazione in tempo reale per insight continui con elementi di business analytics personalizzati per enormi quantità di dati sia strutturati (come security device alert, log di sistema operativo, transazioni DNS e flussi di rete) e non strutturati (come e-mail, contenuti dei social media e transazioni di business): un approccio che permette alle aziende di avvalersi delle funzionalità di analisi dei Big Data per prevenire e rilevare sia le minacce esterne sia i rischi interni.

Docente: Giovanni Abbadessa

12:15-13:00 - ATELIER TECNOLOGICO

"Security Governance: focus sui principali controlli critici"

La Governance della sicurezza informativa attraverso l'adozione di controlli critici di sicurezza. Approcci, aspettative e best practice.

Docenti: Sabina Di Giuliomaria e Armando Leotta

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

14:30-16:00 - PERCORSO PROFESSIONALE TECNICO

"Basta hacker in TV! Lamento pubblico con chi mi può capire"

La sicurezza informatica è diventata così "trendy" da occupare spazi sempre più importanti in serie TV e film Hollywoodiani. Purtroppo questo si traduce in convinzioni ed aspettative fuorvianti, quando non totalmente erronee, da parte del pubblico non tecnico. Quale sede migliore del Security Summit per lamentarsi, con chi comprende l'argomento e la gravità di quanto accade?

Vedremo qualche vero attacco e come esso sia spesso affrontabilissimo, o poco mitigabile in altri casi, da parte di una azienda reale che non ha consulenti informatici con la pistola e che sanno schivare i proiettili.

Cercheremo poi di comprendere quanto un attacco possa essere comprensibile ed investigabile in un contesto lavorativo reale in Italia, rispetto a quanto viene spesso rappresentato. Ingresso sconsigliato ai cyborg ed a chi proviene dal futuro.

Docente: Alessio Pennasilico

14:30-15:15 - ATELIER TECNOLOGICO

"I sette vizi capitali di PCI-DSS"

Sempre più società si trovano ad imbattersi nello standard PCI DSS che regolamenta il trattamento dei dati delle carte di debito e credito. Nonostante lo standard non sia di recente pubblicazione (l'edizione 3.0 è ormai alle porte), nelle realtà aziendali ci si imbatte ancora costantemente in dubbi, perplessità e falsi miti, riguardo la sua attuazione: compliance o certificazione? Self Assessment Questionnaire o Report on Compliance? L'impianto documentale da produrre è quello specificato nel solo capitolo 12? Come si sceglie il perimetro sul quale applicare i requisiti? Quali sono le attività periodiche che è necessario effettuare?

In questa grande confusione, capita spesso di tralasciare aspetti importanti, come ad esempio la sicurezza organizzativa e fisica, incentrandosi per lo più sugli aspetti tecnologici.

Durante l'intervento, che dà per assodata una conoscenza di base dello standard, saranno trattati problemi pratici relativi all'attuazione dello standard PCI DSS, attraverso la presentazione di scenari concreti ispirati dall'esperienza sul campo dei relatori. Saranno infine presentate alcune soluzioni per il superamento delle problematiche esposte, andando a scoprire e sfatare i falsi miti che caratterizzano lo standard.

L'intervento vuole mappare, provocatoriamente, sui sette vizi capitali le singolarità che si incontrano nella quotidiana applicazione di PCI DSS.

Docenti: Alberto Perrone, Paolo Sferlazza

14:30-15:15 - ATELIER TECNOLOGICO

"HoSè (Hospital's Security): Tecnologie informatiche per la sicurezza in ambito sanitario-ospedaliero"

Nelle strutture sanitarie è importante che pazienti, medici, operatori sanitari, terapie, strumenti, indumenti e interventi siano correttamente identificati al fine di evitare trattamenti non idonei, somministrazioni di farmaci non adeguati, operazioni chirurgiche non necessarie o in siti errati, e altro ancora. Nel corso dell'Atelier saranno mostrate le tecnologie che consentono di implementare processi di tracciabilità per garantire incolumità fisica al paziente e assicurare alla struttura sanitaria risparmi in termini di risorse umane ed economiche nel rispetto della privacy, dalla steganografia all'impiego degli RFID. Verranno esaminati vantaggi e criticità dei possibili sviluppi e scenari applicativi futuri.

Docente: Giuseppe Mastronardi

15:15-16:00 - ATELIER TECNOLOGICO

"La strategia europea per la cyber security".

Infine anche l'Europa si è dotata di una strategia per il contrasto al cyber crime. Arrivare tra gli ultimi può essere tuttavia vantaggioso se così facendo si ha potuto beneficiare dell'esperienza degli altri.

Nell'intervento verrà illustrata l'impostazione della strategia europea, discutendone in particolare l'approccio che si differenzia da quello adottato da altri Paesi."

Docente: Corrado Giustozzi

15:15-16:00 - ATELIER TECNOLOGICO

"La computer forensics come strumento di supporto delle strutture di auditing nelle indagini interne aziendali"

Nata come disciplina scientifica per eseguire indagini e accertamenti tecnici su sistemi informatici ed elettronici a fini giudiziari, la computer forensics sta assumendo un ruolo rilevante nel supporto degli uffici di auditing aziendale. Gli uffici, a cui sono affidate le attività di vigilanza e controllo, si trovano sempre più spesso a confrontarsi con malversazioni, usi impropri, illeciti e reati condotti usando strumenti informatici aziendali. Si rendono quindi necessari accertamenti tecnici informatici sui sistemi sospetti. Naturalmente il problema non può essere approcciato con i soli metodi degli accertamenti interni tipici delle funzioni di auditing, perché privi dei requisiti minimi di legittimità dell'acquisizione della prova informatica. Si rende quindi necessario adottare strumenti e procedure di "information forensics" per cristallizzare i reperti informatici e le prove dando legittimità e valore legale ai dati estratti.

Docente: Alessandro Fiorenzi

16.00-16.30 Visita all'area espositiva

16:30-18:00 - SEMINARIO Italian Security Professional Group

"Cyber Warfare, tutti in prima linea: privati, aziende, Governi, eserciti, infrastrutture critiche. Siamo pronti?"

La tematica Cyber Warfare, che fino al 2011 era considerata ancora una fonte di rischio piuttosto remota, nel 2012 è diventata un serio problema internazionale, ed è considerata della massima gravità dagli addetti ai lavori, mentre Governi ed organizzazioni sovranazionali come la NATO stanno investendo miliardi in questo ambito. Per la natura di questo tipo di conflitto, tutti sono in prima linea, e tutti sono a rischio.

I principali attori sulla scena internazionale stanno sviluppando importanti capacità di cyber-offense con finalità di deterrenza, ed alcuni minacciano persino di ricorrere a misure cinetiche nel caso di cyber attacchi, in un crescendo di dichiarazioni che sanciscono l'inizio di un'era di "cyber guerra fredda" della quale è difficile ipotizzare gli sviluppi, ma che sicuramente nei prossimi anni è destinata a modificare gli equilibri geopolitici mondiali. Siamo pronti a sostenere gli impatti di questo sviluppo rapidissimo delle minacce? Cerchiamo di fare il punto della situazione insieme ad un panel internazionale di esperti di Cyber

Warfare, vendor di sicurezza, hacker, esperti di infrastrutture critiche e consulenti in materia di Cyber Defense.

Modera: Andrea Zapparoli Manzoni

Intervengono: Raoul Chiesa, Corrado Giustozzi, Stefano Mele, Massimiliano Rijllo, Enzo Maria Tieghi.

16:30-18:00 - SEMINARIO AIIC (Associazione Italiana esperti in Infrastrutture Critiche)

"Infrastrutture Critiche e Cybersecurity"

La proposta di direttiva europea, il decreto italiano, l'impatto sulle infrastrutture critiche

Modera: Bruno Carbone, Consigliere AIIC

16:30-18:00 - SEMINARIO IISFA (International Information Systems Forensics Association)

Sono previsti 3 interventi.

"Bitlodine: analisi e intelligence di Bitcoin"

Bitcoin è una crypto-currency completamente decentralizzata, a inflazione programmata e limitata nel tempo, che si pone come obiettivo quello di diventare l'equivalente digitale del contante, impossibile da controllare e manipolare da banche o istituzioni. Inizialmente confinato a una ristrettissima cerchia di crypto-geeks, libertari e crypto-anarchici, Bitcoin ha recentemente ottenuto popolarità mainstream, in virtù della sua volatilità di prezzo, e come potenziale occasione di diversificazione di investimento in un contesto economico instabile. La decentralizzazione e, allo stesso tempo, il fatto che ogni transazione sia visibile pubblicamente, rende Bitcoin ideale per alcuni usi, come il gioco d'azzardo con garanzia crittografica, precedentemente di difficile implementazione. Grazie alle sue apparenti caratteristiche di anonimato, Bitcoin è adottato da Silk Road, mercato non regolato del "deep web", famoso per la vendita di droghe e documenti falsi. In questo intervento verrà descritto l'ecosistema Bitcoin, e presentato un tool, Bitlodine, sviluppato dal relatore come lavoro di tesi per un master a Chicago. Bitlodine effettua analisi sulle transazioni del network Bitcoin per estrarre informazioni potenzialmente utili a proposito dell'identità e caratteristiche dei partecipanti. Si mostreranno esempi d'uso del tool nel mondo reale, dimostrando che l'indirizzo che ha mosso più denaro nel 2012 appartiene proprio a Silk Road.

Docente: Michele Spagnuolo

"Cybercop 2013"

Presentazione della simulazione Cybercop 2013, svoltasi durante l'ultimo IISFA Forum a Napoli il 25 maggio 2013.

Docente: Giuseppe Specchio

"Storage Forensics"

La crescente necessità di gestione di grandi quantità di dati digitali richiede infrastrutture e competenze più avanzate rispetto a quelle tradizionali. Nell'ottica forense questo costringe l'analista ad operare rispettando le politiche di Business aziendale e nello stesso tempo ad acquisire quanto richiesto nella maniera più corretta possibile.

Docente: Litiano Piccin

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 si terrà il 5 giugno dalle 18:00 alle 20:00.

Le pellicole saranno presentate e commentate da: Alessio Pennasilico, Corrado Giustozzi, Cristiano Cafferata, Lele Rozza e Raoul Chiesa.
L'Hacking Film Festival è realizzato in collaborazione con la Facoltà di Informatica Giuridica dell'Università degli Studi di Milano.
Si ringrazia il prof. Giovanni Ziccardi, responsabile scientifico del Festival.

La partecipazione è gratuita, ma è richiesta l'iscrizione via mail a info@clusit.it.

Al termine, gli spettatori sono invitati a partecipare ad un aperitivo

PROGRAMMA

Per questa quarta edizione romana del Festival, saranno proiettati dei brevi filmati, con lo scopo di promuovere un dibattito tra gli animatori del Festival ed il pubblico su temi caldi relativi alla sicurezza delle informazioni. Si comincerà con uno spot belga sulla criticità dei propri dati personali messi on-line da cittadini ed utenti. Della durata di circa 2 minuti, è stato voluto da associazioni legate alla sicurezza delle informazioni in Belgio. E' un progetto durato diversi mesi, costato circa 500.000 €, avente lo scopo di sensibilizzare i cittadini in merito alle informazioni personali che forniscono spontaneamente on-line.

5. ATTESTATI E CREDITI CPE

Tutte le sessioni, tranne quelle organizzate e gestite autonomamente dalle associazioni (Seminari Associazioni), prevedono il rilascio di Attestati di Presenza 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 sarà rilasciato solo a chi ha assistito all'intera sessione e risulta regolarmente registrato. Gli attestati saranno emessi al termine del Security Summit e inviati per email. In caso di mancata ricezione entro il 20 giugno, gli attestati possono essere richiesti a info@clusit.it.

La registrazione è possibile solo online sul portale www.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 l'eventuale materiale didattico.

A chi avrà assistito, secondo le regole di cui sopra, a tre sessioni appartenenti ai Percorsi Professionali sarà rilasciato un Diploma. Il diploma sarà inviato per email a chi ne farà richiesta a info@clusit.it.

6. GLI SPONSOR DEL SECURITY SUMMIT ROMA 2013

Partner

IBM

Platinum

SonicWALL

F5

Westcon Security

Gold

Attachmate

CERTIFICATION AUTHORITY

LUTECH

NetIQ

Silver

Albaist

FASTWEB un passo avanti

iDIALOGHI

mediaservice.net

SecurityBrokers

SentiNet

websense

Sponsor dell'Hacking Film Festival

SonicWALL

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: 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