SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

ROMA

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni al Security Summit di Roma, che si terrà nei giorni 8 e 9 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 DELL'8 GIUGNO

09.00 Registrazione - Welcome Coffee

09.45-12.30 MANIFESTAZIONE DI APERTURA - SALA AUDITORIUM

"Le nuove frontiere dell'Ict Security"

Il convegno di apertura, di grande spessore istituzionale, vedrà come ospite d'onore il **Prof. Udo Helmbrecht, Direttore Esecutivo dell'ENISA** (l'Agenzia Europea per la sicurezza delle reti e delle informazioni), che porterà la visione europea su Cloud Computing, Social networks, Botnet & Malware, Mobile Security e Critical National Infrastructures. Seguirà una tavola rotonda in cui si dibatterà di Cloud Security e Mobile Security, ma anche di Partnership tra Pubblico e Privato e di come sensibilizzare l'utente finale, il cittadino.

Alla TR, moderata da Gigi Tagliapietra, partecipano: Udo Helmbrecht (ENISA), Rita Forsi (ISCOM, Ministero per lo Sviluppo Economico), Jean Paul Ballerini (IBM), Gastone Nencini(Trend Micro), Alessandro Vallega (Oracle).

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

14.00-15.30 PERCORSO PROFESSIONALE TECNICO - SALA AUDITORIUM

"Attacchi alle infrastrutture virtuali: come proteggere le informazioni e difendersi nei nuovi ambienti tecnologici beneficiando al massimo dei vantaggi"

Abstract: L'evoluzione delle infrastrutture coincide con l'evoluzione delle minacce. L'installazione delle protezioni sul perimetro protegge ancora i miei dati? Quali nuove tecnologie posso utilizzare per difendermi? E quali soluzioni mi permettono di sfruttare al massimo i benefici delle nuove tecnologie? Quali strumenti ho a disposizione per fortificare la difesa dei miei asset aziendali? Proteggere il perimetro basta ancora? Che nuove minacce mettono a rischio le informazioni? Attacchi a L2, attacchi a L7, virtualizzazione, Cloud, dipendenti infedeli, media rimovibili, enormi interessi economici, come districarsi in mezzo a tutto ciò?

Docenti: Alessio Pennasilico e Gastone Nencini

14.00-15.30 PERCORSO PROFESSIONALE GESTIONE DELLA SICUREZZA - SALA LUCIA

"ROSI - Return On Security Investment: Esperienze a confronto"

Abstract: Viene presentata la seconda versione del documento ROSI liberamente disponibile http://rosi.clusit.it e frutto del lavoro di Clusit, AIEA, Oracle, Deloitte, Ernst & Young, KPMG e PriceWaterhouseCoopers, che fornisce un aiuto a persone in posizione di responsabilità nell'ICT per

definire gli investimenti più opportuni nell'ambito della sicurezza delle informazioni.

Questa edizione incorpora il contributo di numerosi altri autori, alcuni dei quali chiamati a darne testimonianza, in particolare rispetto all'approccio denominato "bottom-up" e basato sui "pattern".

Intervengono: Mauro Cicognini, Stefano Saibene, Riccardo Scalici, Enzo M. Tieghi, Giuseppe Russo, Andrea Zapparoli Manzoni.

14.00-14.45 ATELIER TECNOLOGICO - SALA TIMOTEO

"Dal log management in ambienti eterogenei al monitoraggio degli accessi privilegiati, soluzioni Balabit per un "controllo rinforzato""

Abstract: L'attenzione alla tutela e all'integrità dei dati gestiti dai sistemi informativi è sensibilmente aumentata negli ultimi tempi anche grazie a leggi, regolamenti e standard industriali recenti. Ai sistemi informativi è richiesta una sempre maggiore garanzia nella protezione e nella verificabilità del dato. Da qui nasce l'esigenza di un maggiore controllo sugli eventi di sistema e sulle attività degli operatori con

particolari privilegi, il tutto a supporto della continuità operativa e dell'analisi forense. Durante l'incontro presenteremo casi reali e le nostre soluzioni per rispondere a queste problematiche.

Relatori: Gaetano Gargiulo e Vanni Galesso

14.45-15.30 ATELIER TECNOLOGICO - SALA TIMOTEO

"La gestione delle identità federate nel cloud"

Abstract: La sicurezza può a volte rappresentare un deterrente per l'adozione del cloud con implicazioni diverse a seconda degli ambienti e dei settori di mercato. Ad esempio, le imprese che hanno strumenti di collaborazione e di posta elettronica nel cloud devono pensare al controllo degli accessi e delle policy, mentre quelle che si occupano di assistenza sanitaria devono preoccuparsi dell'isolamento dei dati e della crittografia.

La gestione delle identità centrata sull'utente fornisce una soluzione di gestione delle transazioni di identità che permette ai singoli utenti di avere il controllo sulle informazioni comunicate per identificarsi.

Questi aspetti diventano particolarmente importanti a fronte dell'esigenza di accedere a svariate applicazioni e servizi in ambito cloud.

Relatore: Fabrizio Patriarca, IBM Security Client Technical Professional

15.30-16.00 Visita all'area espositiva

16:00-17:30 PERCORSO PROFESSIONALE TECNICO - SALA AUDITORIUM

"Cloud Security: l'elemento decisivo"

Abstract: "Partendo dalla definizione del NIST si mettono in evidenza le caratteristiche maggiormente rilevanti dal punto di vista della sicurezza (Multi-tenancy, resource pooling, elasticity). In questo contesto si tratteggiano gli elementi rilevanti nell'analisi dei rischi associati al cloud computing. Si passano quindi in rassegna 5 Rischi tra i più rilevanti (Lock-in, mancato rispetto normativa privacy, subforniture, compromissione della sicurezza dei dati, compromissione della rete). Si introducono quindi i lavori della Cloud Security Alliance e l'approccio di sicurezza proposto.

L'intervento di Matteo Cavallini si chiude con la notizia che Consip pubblicherà entro giugno un Quaderno dal titolo "Cloud Security: una sfida per il futuro". Esempio di una sfida per il futuro.

Docenti: Matteo Cavallini e Ugo Piazzalunga

16.00-17.30 PERCORSO PROFESSIONALE GESTIONE DELLA SICUREZZA - SALA LUCIA

"Data Leakage Prevention"

Abstract: In questo seminario, i relatori trattano il tema della Data Leakage Prevention guidando il pubblico in una discussione in grado di indirizzare i punti più importanti dei progetti e degli approcci di prevenzione e di comprenderne le motivazioni che portano alla decisione di investimento.

Ad esempio:

- La perdita dei dati è frequente? Qual'è l'entità dei danni che si riscontra in caso di perdita dei dati?
- Che tipo di dati si perdono e si rubano, e per quali motivi? In quali settori industriali o contesti capita più frequentemente?
- Come faccio a valutare l'investimento in sicurezza rispetto al beneficio della mancata o ridotta perdita probabile? Come faccio a dimostrare la necessità economica dell'investimento al management?
- La complessità dei sistemi informatici è tale che è impossibile portare ad un livello adeguato di sicurezza tutti i sistemi in breve tempo. Con quali criteri e come approccio un progetto per fasi o priorità? Che costi hanno tali progetti?
- Che tipo di approccio tecnologico è utile per proteggere quali informazioni? Il controllo deve essere sul perimetro o a diversi livelli, "a cipolla", su tutta l'infrastruttura?
- Chi devo coinvolgere nel progetto DLP oltre l'IT? L'Organizzazione? Il Legale? Il responsabile di linea di business?

- Chi è lo sponsor di un progetto DLP di successo? A cosa si deve rinunciare per la riservatezza?
- Come controllo la riservatezza dei dati e documenti che sono lecitamente usciti dai confini dell'azienda ma nonostante ciò devono ancora essere protetti? E come controllo le modifiche nel tempo dei privilegi di accesso a documenti che sono già usciti dal perimentro?
- Come devo considerare le tecnologie di "mobility"? Autorizzo l'uso di nuovi device, ipad, iphone, tablet, ecc. personali e aziendali ai miei dipendenti e come li proteggo?
- E il Cloud? Un progetto di classificazione dei dati e l'analisi del rischio mi aiuta a valutare l'adozione di soluzioni SaaS nel public cloud?
- Che cosa fanno le altre aziende del mio settore merceologico in relazione a questi temi?
- Quali altre sfide ci presenterà la tecnologia negli anni a venire?

Modera : Mauro Cicognini

Intervengono: Lucilla Mancini, Federico Santi, Francesco Severi, Andrea Zapparoli Manzoni.

16:00-17:30 PERCORSO PROFESSIONALE GESTIONE DELLA SICUREZZA - SALA SCOLASTICA

"Il rischio informatico nelle piccole imprese"

Abstract: La gestione del rischio informatico nella piccola impresa deve tenere conto delle particolarità di questa tipologia di imprese. Molti standard e best practice sono concepiti per aziende più grandi. Anche se in teoria possono essere adattati ad aziende di qualsiasi dimensione, questa strada comporta uno sforzo che spesso non è commisurato ai vantaggi. Può essere invece utile un approccio più pragmatico, pur senza perdere di vista i principi che guidano la gestione del rischio informatico. Saranno anche affrontate le problematiche di rischio specifiche per le piccole imprese, legate alle nuove offerte di outsourcing, come ad esempio il cloud computing.

Docente: Claudio Telmon

Seguono:

18.00-20.00 HACKING FILM FESTIVAL

20.00-21.00 APERITIVO

3. PROGRAMMA DEL 9 GIUGNO

09:00 Registrazione

09.30-11.00 PERCORSO PROFESSIONALE GESTIONE DELLA SICUREZZA - SALA AUDITORIUM

"La sicurezza dei pagamenti e delle carte di credito (PCI-DSS)"

Abstract: Oltre ad una breve introduzione alla norma PCI-DSS che rappresenta lo stato dell'arte per la protezione dei dati delle carte, in questo seminario i relatori spiegano perché sia importante proteggersi, come lo fanno gli interessati in Italia e all'estero, che difficoltà si incontrano, che caratteristiche ha un progetto di successo e quali tecnologie siano oggi disponibili nel mercato, nell'intento di condividere le "lessons learned" e le migliori pratiche e fornire un punto di partenza a valle del quale intraprendere un percorso di investimento e di compliance in maniera informata.

Intervengono: Alberto Perrone, Enrico Ferretti, Andrea Longhi, Paolo Marchei, Stefano Saibene, Alessandro Vallega.

09:30-11:00 PERCORSO PROFESSIONALE LEGALE - SALA LUCIA

"I servizi "cloud": problemi legali e contrattuali"

Abstract: I servizi "cloud" pongono una serie di problematiche legali e contrattuali di grande rilevanza. Il trattamento dei dati personali, le misure di sicurezza, le garanzie del fornitore, i livelli di servizio e le responsabilità in caso di problematiche sono solo alcuni dei temi che devono essere valutati nella scelta. Inoltre, il carattere potenzialmente internazionale dell'organizzazione del fornitore rende necessaria una valutazione sugli adempimenti, le tutele e le precauzioni che occorre prendere in considerazione anche alla luce delle vigenti normative italiane e estere.

Docente: Gabriele Faggioli

09.30-11.00 PERCORSO PROFESSIONALE TECNICO - SALA SCOLASTICA

"I requisiti di sicurezza per i moduli crittografici e la validazione degli algoritmi crittografici secondo lo standard FIPS 140-2"

Abstract: La pubblicazione FIPS PUB 140-2 (Federal Information Processing Standard Publication) intitolata: "Requisiti di sicurezza per i moduli crittografici", è uno standard di sicurezza impiegato in campo informatico e utilizzato per validare moduli crittografici. Adottato da U.S.A, Canada, Gran Bretagna, Francia e Germania, è ormai divenuto lo standard de facto per la crittografia, ed è molto probabile che assurga, nel prossimo futuro, a standard internazionale. In particolare, USA e Canada lo impongono già per settori particolari come le istituzioni finanziarie e sanitarie e, generalmente, nelle infrastrutture critiche e nella Homeland Security.

Questo standard richiede che laboratori specializzati convalidino un determinato modulo hardware, software, firmware ben definito ai sensi del predetto standard dopo opportune attività di valutazione. Le prove di convalida per la corretta implementazione degli algoritmi di crittografia e componenti di algoritmi approvati dal FIPS e raccomandati dal NIST sono effettuate con il Cryptographic Algorithm Validation Program (CAVP) che è un prerequisito per il Cryptographic Module Validation Program (CMVP), un programma congiunto, USA-Canada, di accreditamento di sicurezza per i moduli di crittografia.

Docente: Stefano Ramacciotti

11.00-11.30 coffee Break e visita all'area espositiva

11.30-13.00 PERCORSO PROFESSIONALE TECNICO - SALA AUDITORIUM

"Il processo di Application security dal modello tradizionale al Cloud"

Abstract: L'introduzione degli aspetti di sicurezza in tutte le fasi del ciclo di sviluppo del software sta cambiando il modo di concepire, progettare e utilizzare le applicazioni. Sebbene esistano diverse best practice di Secure Engineering, la loro integrazione nel ciclo di sviluppo adottato dalle organizzazioni è una delle maggiori sfide con cui dobbiamo confrontarci, soprattutto nella nuova era del Cloud.

Docenti: Alessandro Gai, Simone Riccetti

11.30-13.00 PERCORSO PROFESSIONALE LEGALE - SALA LUCIA

"La classificazione delle informazioni, elemento chiave per la protezione delle informazioni in azienda"

Abstract: Il tema della protezione delle informazioni, che a tutti gli effetti costituisce uno dei componenti del patrimonio aziendale, si fa sempre più attuale. Proteggere adeguatamente le proprie informazioni, infatti, oltre a prevenire l'indebita conoscenza delle stesse da parte della concorrenza, costituisce un parametro fondamentale per attribuire delle responsabilità giuridicamente rilevanti in capo a chi non tratta adeguatamente tali informazioni, oltre ad essere elemento di valutazione per la quantificazione del danno. Un'efficiente protezione delle informazioni, tuttavia, oltre ai possibili espedienti tecnico/informatici di sicurezza, deve passare necessariamente attraverso una gestione delle stesse mediante classificazione, così da garantire un'adeguata protezione parametrata all'importanza delle stesse, ferma restando la necessità di valutare e rispettare i limiti normativi vigenti in tema di controlli sui lavoratori sia in chiave preventiva che reattiva.

Docenti: Gabriele Faggioli e Gary McConnell

11.30-12.15 ATELIER TECNOLOGICO - SALA TIMOTEO

"Un approccio alla sicurezza entitlement-centered"

Abstract: La deperimetrizzazione delle aziende ha reso le aziende più moderne entitlement-based. L'industria della sicurezza informatica ha intercettato questo cambiamento e a meno di strumenti che consentono di gestire quest'evoluzione, le aziende continueranno a gravare sui propri clienti con costi d'integrazione e con oneri di conformita' legislative. L'Entitlement è un linguaggio comune che puo' aiutare a cambiare il modo in cui l'identità è usata come base per un approccio olistico per la definizione delle politiche di sicurezza e di gestione dei rischi in azienda.

Relatore: Domenico Catalano, Senior Sales Consultant Oracle

12:15-13:00 ATELIER TECNOLOGICO - SALA TIMOTEO

"Dalla virtualizzazione al Cloud Computing: le nuove esigenze di sicurezza legate all'evoluzione dei datacenter"

Abstract: Dopo una panoramica iniziale sulle problematiche di sicurezza legate all'evoluzione dei datacenter, si entrerà nel dettaglio nel presentare una soluzione, la prima e ad oggi unica al mondo, per la sicurezza degli ambienti virtualizzati.

Relatori: Maurizio Martinozzi, Manager - Sales Engineering, Trend Micro

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

14:30-16:00 PERCORSO PROFESSIONALE TECNICO - SALA AUDITORIUM

"Metodologia per la simulazione degli attacchi e per l' analisi delle minacce contro le applicazioni e infrastrutture critiche"

Abstract: Questa presentazione introduce una nuova metodologia per l'analisi degli attacchi e delle vulnerabilita' delle applicazione web critiche come online banking. Il principale obbiettivo della analisi è la minimizzazione dei rischi per il buisiness, che consistono nella perdita di dati sensibili a danno degli utenti e nelle frodi ai danni delle aziende che forniscono servizi commerciali e finanziari su internet. La nuova metodologia per la simulazione degli attacchi e per l'analisi delle minacce si chiama P.A.S.T.A. (Process for Attack Simulation e Threat Analysis).

Seguendo le varie fasi della metodologia, e' possibile determinare la strategia piu efficace per la neutralizzazione del rischio dalle minacce di

attacchi di malware come Zeus e botnets. L'impatto di questi attacchi e' enorme ed e' stimato per gli Stati Uniti in circa 10 milioni di dollari per settimana. Questi attacchi sono diretti principalmente verso applicazioni di on-line banking e perseguono l'acquisizione non autorizzata di dati sensibili come passwords, dati di conto bancari e di carte di credito,

nonche' permettono l'alterazione delle transazioni finanziarie on-line come bonifici e transferimenti di denaro per commettere frodi. In questa presentazione verranno usati i diversi stadi della metodologia per l'analisi dei vettori di attacco disponibili nei tool di attacco e di diffusione di bankign trojan malware come Zeus. La nuova metodologia di analisi P.A.S.T.A si basa anche sul contributo di dati di "intelligence" dei crimini informatici da cui si ricavano i scenari di attacco e i vari tipi di vettori usati. Questi vettori di attacco consistono in particolare in attacchi di (Denial of Service) interruzzione/degrade del servizio, Man the Middle (MiTB) o compromissione dei dati in transferimento e Man in The Browser (MiTB) o compromissione del browser. Questo tipo di informazioni critiche e' essenziale per l'attuazione di contromisure efficaci per la mitigazione dei rischi di banking malware che includono per esempio controlli di prevenzione, indentificazione e monitoraggio degli attachi a diversi livelli dell'applicazione e dell'infrastruttura.

La presentazione mette in evidenza come gli attacchi di MiTB cercano di iniettare HTML nel browser per raccogliere dati delle carta di credito e carte di debito così come per alterare i dati durante le transazioni di on-line banking per trasmettere i pagamenti a conti fraudolenti i cossiddetti Money Muli (Muli del denaro).

Questa presentazione mira ad educare i responsabili della gestione dei rischi informatici e di frodi finanziarie fornendo esempi di come sia possible controllare e gestire questi rischi usando il nuovo processo per l'analisi delle minacce e la simulazione degli attacchi (P.A.S.T.A). I particolari di come sia possible usare questo processo per l'analisi di minacce contro applicazioni on-line è anche trattata nel libro di prossima pubblicazione: Application Threat Modeling pubblicato da Wiley & Sons che e' incorporato nel tool di analysis "Threat Modeler". L'obbiettivo della presentazione e' dotare i professionisti di sicurezza informatica ai vari livelli di responsabilita' di strumenti di riferimento per la gestione dei rischi informatici per applicazioni e infrastrutture critiche web e consentire una decisione strategica dell' applicazione delle contromisure per la mitigazione dei rischi di malware. Gli esempi trattati consistono nella autenticazione e verifica su canale esterno "Out Of Band Authentication" (OOBA), le password d'uso temporaneo "One Time Password" (OTP) e nei controlli per l'identificazione e correlazione degli eventi di attacco.

Docente: Marco Morana

14:30-16:00 TAVOLA ROTONDA - SALA LUCIA

"Dematerializzazione e sicurezza ict a seguito delle nuove regole per la Pubblica Amministrazione (Correttivo al Codice dell'Amministrazione Digitale – CAD, Dlgs 30.12.2010 n.235)"

Modera: Giovanni Manca

Intervengono :

- Giovanni Manca "CAD: obblighi e opportunità nella pubblica amministrazione"

- Giovanni Rellini "Continuità operativa e Disaster Recovery nella pubblica amministrazione"
- Corrado Giustozzi "Esigenze di sicurezza nella PA: diverse prospettive tra Codice dell'Amministrazione Digitale e Codice della Privacy"

Pur non facendo parte di un Percorso Professionale, anche questa sessione consentirà l'attribuzione di crediti CPE

14:30-16:00 PERCORSO PROFESSIONALE TECNICO - SALA SCOLASTICA

"Rischi ed opportunità nell'utilizzo degli Smartphones"

Abstract: Gli smartphone stanno prendendo sempre piu' piede e sono utilizzati in contesti personali, di business e sociali. Nel contempo, aumentano con cadenza quasi quotidiana gli attacchi e gli abusi verso il mondo Mobile, con la peculiarita' propria di questi ultimi anni di utilizzare proprio l'handset come "Vettore di Attacco". Questa presentazione fornira' una panoramica storica degli attacchi verso questi dispositivi, per focalizzarsi poi sui rischi e sulle opportunita' proprie dei rischi e del mercato odierno.

Docente: Raoul Chiesa. Con la partecipazione di Alessio L.R. Pennasilico

16.00-16.30 Visita all'area espositiva

16:30-18:00 SEMINARIO a cura Dell' Italian Security Professionals Group - SALA AUDITORIUM

"Botnet delenda est"

Modera: Matteo Cavallini

Un seminario sotto forma di Tavola rotonda con interventi di Matteo Cavallini, Claudio Guarnieri e Feliciano Intini.

AGENDA

- "Un caso reale di Botnet Investigation, un modello crimininale vincente e i suoi punti deboli"
  Ormai siamo tutti generalmente istruiti su cosa sia una Botnet, ma entriamo in un caso specifico e reale cercando di comprendere le caratteristiche di un'infrastruttura funzionante e perchè i big player della security hanno fallito.
- "Rustock e Coreflood due casi di successo nella lotta alle Botnet"
  I dettagli delle due operazioni che hanno fatto più scalpore in questo inizio d'anno, con una serie di riflessioni comuni sulle implicazioni che ci possono essere nei casi di takedown e takeover.
- "Anti-botnet Center italiano, una proposta che potrebbe farci fare un grande passo avanti"

La proposta di costituire un antibotnet Center italiano nelle sue linee essenziali. Le criticità, le implicazioni, i vantaggi e le prospettive.

- Open discussion finale

16:30-18:00 SEMINARIO a cura di IISFA (International Information Systems Forensics Association) - SALA LUCIA

"Digital Forensics & Investigation"

Chairman: Gerardo Costabile, Presidente IISFA Italian Chapter

Intervengono:

- Francesco Scarpa, IISFA Board "Link Analysis e frodi informatiche nel settore bancario e finanziario: case study"
- Mattia Epifani, CIFI - RE@LITY NET "Ipad Forensics"
- Massimiliano Graziani, CIFI - IISFA Board "IISFA Cybercop Challenge 2011"

16:30-18:00 SEMINARIO a cura di AIIC (Associazione Italiana esperti in Infrastrutture Critiche) - SALA SCOLASTICA

"La SCADA Security nell'era di STUXNET"

Abstract: Questa sessione mira a fare il punto su come si è modificata la cyber security nel mondo SCADA a valle di StuxNet e di come questa deve evolvere al fine di garantire un adeguato livello di protezione e sicurezza a questi sistemi vitali per la nazione.

Intervengono:

- Roberto Setola, Segretario AIIC "StuxNet, antefatto e lesson learned"
- Giancarlo Caroti, Terna "La cyber security di un sistema SCADA, l'esperienza del mondo elettrico"
- Tommaso Palumbo, Polizia di Stato "Le strategie messe in campo dal CNAIPIC"
- Andrea Rigoni, GC-SEC Global Cyber Security Center e membro del CD della AIIC "Le attività di cyber scada security a livello internazionale"

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 seconda edizione romana si terrà l'8 giugno dalle 18:00 alle 20:00 e sarà seguito da un aperitivo. Sono in programma 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, Francesco Loriga, Alessio Pennasilico e Pierluigi Perri.

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.

PROGRAMMA

Una serata dedicata a brevi filmati, con lo scopo di discuterne i contenuti con il pubblico.

I temi affrontati abbracceranno la cultura hacker, il tema del copyright, del diritto d'autore, della diffusione della conoscenza:
tutti temi cari all'underground telematico fin dalle sue origini.

Verranno proiettati diversi filmati, come Metamondo, un cortometraggio realizzato in Italia, Disney Trap (inglese sottotitolato in italiano) sul diritto d'autore. A tal proposito verrà fatta anche una comparazione tra il filmato che le major inseriscono in tutti i DVD per tutelare le opere cinematografiche, con la risposta che Internet ha prodotto. Termineremo con un filmato sul TrustedComputing realizzato negli States, ma modificato in Italia per trasformare audio e contenuti nella nostra lingua, un filmato che si concentra sul tema della fiducia, tema che giornalmente le aziende affrontano nel decidere come gestire i loro dati, uno degli asset più importanti.

La Scaletta dei filmati che verranno proiettati:

1. **Manifesto hacker by Marco 1.0**
2. **The Disney Trap: How Copyright Steals our Stories**
3. **La pirateria è un REATO**

4. **I wouldn't steal... but i do download films**
5. **TCPA - Trusted Computing Platform Alliance (versione adattata da no1984.org)**

La partecipazione è gratuita, ma è richiesta l'iscrizione, per la quale basta inviare una mail a info@clusit.it

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

Al termine delle proiezioni ci sarà un rinfresco-aperitivo.

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, legali e sulla gestione della sicurezza), gli Atelier Tecnologici e la tavola rotonda "Dematerializzazione e sicurezza ict a seguito delle nuove regole per la Pubblica Amministrazione (Correttivo al Codice dell'Amministrazione Digitale – CAD, Dlgs 30.12.2010 n.235)".

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.

6. GLI SPONSOR DEL SECURITY SUMMIT

Partner

IBM

TREND MICRO

Oracle Community For Security

ORACLE

BSC CONSULTING

BUSINESSe

Deloitte.

present

Platinum

SafeNet

SONICWALL

Silver

Albast

BalaBit IT Security

BARCLAY TECHNOLOGIES

Check Point

Clever consulting

Intelligent Computer Solutions

ITWAY

KASPERSKY

Lantech

McAfee

mediaservice.net

NETGEAR

STONESOFT Network Security

Symantec.

TITUS

websense

Sponsor dell'Hacking Film Festival:

Oracle Community For Security

SONICWALL

Partner e sponsor di Clusit Education:

(ISC)² CEFRIEL BUSINESSe CISCO CRAG Partners enterasys ORACLE

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