SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

ROMA 2014

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni al Security Summit di Roma https://www.securitysummit.it/roma-2014 che si terrà nei giorni 18 e 19 giugno presso l'SGM Conference Center https://www.securitysummit.it/roma-2014/location

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/roma-2014/registrazione-eventi

2. PROGRAMMA DEL 18GIUGNO

09.00 Registrazione

09:30-11:00 - Plenaria - Tavola Rotonda

"Infrastrutture Critiche e cyber defense: stato dell'arte in Italia e in Europa"

Scopo della tavola rotonda è di dibattere del programma europeo per la protezione delle infrastrutture critiche, della direttiva europea sulla sicurezza cibernetica, dell'applicazione del DPCM del gennaio 2013.

Modera: Luisa Franchina.

Partecipano:

- Rita Forsi, Direttore ISCOM, Ministero per lo Sviluppo Economico
- Mario Terranova, Responsabile Ufficio Sicurezza delle infrastrutture e dei centri di servizio, Agenzia per l'Italia Digitale
- Andrea Biraghi, SVP – Director of LoB Cyber Security, CEO E-Security, CEO Cyberlabs - Selex ES
- Gigi Tagliapietra, Presidente Clusit

11.00-11.30 coffee Break e visita all'area espositiva

11:30-13:00 - Tavola Rotonda

"Presentazione del Rapporto Clusit 2014 sulla Sicurezza ICT in Italia"

Oltre alla consueta analisi degli attacchi ed incidenti del 2013 in Italia e nel mondo, il Rapporto 2014 contiene le tendenze del mercato e degli investimenti in Italia e le tendenze del mercato del lavoro.

Tutti i presenti in sala potranno ritirare una copia del rapporto (fino ad esaurimento).

Modera: Gigi Tagliapietra, Presidente Clusit

Intervengono alcuni degli autori del Rapporto: Andrea Zapparoli Manzoni, Davide Del Vecchio e Luca Bechelli

Partecipano:

- Andrea Carmignani, IBM Sales Manager, Responsabile della linea di servizi Enterprise Security per l'Italia
- Cristiano Cafferata, Security Team Sr. Leader in Dell SonicWALL
- Federico Santi, HP Enterprise Security Services, Client Principal Southern Europe

13:.00-14:30 LUNCH-BUFFET e visita all'area espositiva

14:30-16:00 - Percorso Professionale Tecnico

"Cyber Attack e Security Intelligence - Cosa sono i cyber attack, come è possibile rilevarli e come rispondere"

Con l'evoluzione delle tecnologie che favoriscono la mobilità e di conseguenza l'accesso ad una mole quasi incontrollabile di dati, l'Information Security è diventata una priorità fondamentale delle aziende per tutti i progetti IT e non solo. Considerato l'attuale scenario mondiale in cui si ricevono continuamente notizie relative ad attacchi informatici verso aziende ed istituzioni, è importante domandarsi ed informarsi sull' evoluzione delle minacce e dei potenziali danni che queste possono arrecare ai sistemi informatici e ai dati.

Per difendersi è necessario un approccio integrato dei sistemi e dei processi di sicurezza basato sulla Security Intelligence in modo da poter rilevare, fermare e rispondere a un attacco nelle varie fasi in cui viene portato a compimento.

Durante l'intervento verranno analizzate le principali tecniche e metodologie di attacco e verrà mostrato come è possibile la rilevazione tramite l'utilizzo di un moderno sistema di Security Intelligence.

Docenti: Andrea Zapparoli Manzoni e Samuele Battistoni

14:30-16:00 - Percorso Professionale Tecnico

"heartbleed – baco o backdoor ? "

Docente: Cristiano Cafferata

14:30-15:15 - Atelier Tecnologico

"SIEM: casi d'uso e livelli di maturità"

I Security Information and Event Management (SIEM) sono strumenti cruciali per il monitoraggio della sicurezza all'interno delle aziende. Si tratta di tecnologie di security, data management e data analysis al tempo stesso. La realizzazione di una soluzione SIEM è human-intensive e time-consuming e dovrebbe far parte di una strategia di sicurezza globale. Fattori critici di successo sono rappresentati da processi, pratiche, flussi di lavoro, disponibilità di personale competente e dedicato ma soprattutto dalla definizione e implementazione di casi d'uso specifici. HP presenterà alcuni casi d'uso reali per sottolineare l'importanza della comprensione del contesto di business ai fini della corretta percezione del valore di una soluzione SIEM.

Docente: Marco Di Leo

15:15-16:00 - Atelier Tecnologico

"Gli ultimi ritrovati in termini di attacchi alle aziende e furti di dati: vi diciamo chi sono e come combatterli!"

Degli Advanced Persistent Threats (APT) non solo se ne parla ma ad oggi se ne cominciano a contare i danni: è possibile contrastarli ma la difesa deve essere personalizzata e "tagliata su misura" dell'infrastruttura dell'azienda.

Una ricerca del Ponemon Institute ha rilevato che il 67% delle aziende ammette che le proprie soluzioni sicurezza adottate non sono sufficienti a bloccare un attacco mirato. Ma il dato è tragico se consideriamo che il 55% delle aziende non viene nemmeno a conoscenza delle intrusioni subite e, una percentuale bassissima, è in grado di valutare la portata dell'attacco e, ancora più importante, chi lo ha sferrato.

Per contrastare gli attacchi mirati è necessario adottare tecnologie si sicurezza evolute, quelle tradizionali non garantiscono più un adeguato livello di protezione. Di fatto le nuove tecnologie devono essere in grado di gestire la tipologia di attacco, rilevando e analizzando le minacce costanti evolute, ma anche di adattando rapidamente la protezione e reagendo in maniera proattiva ad attacchi specifici.

La tecnologia deve essere in grado di integrare correttamente software, informazioni globali sulle minacce, strumenti e servizi specializzati per offrire nozioni personalizzate sulla minaccia specifica e sui criminali coinvolti. I recenti progressi nella gestione di comando e controllo (C&C) contribuiscono a bloccare i comportamenti sospetti prima ancora che riescano a compromettere l'obiettivo individuato.

Ma non allarmiamoci: oggi sono disponibili specifiche soluzioni preventive e noi ve le racconteremo: vi spiegheremo perchè le soluzioni di sicurezza tradizionali non riescono a combattere queste nuove tipologie di minacce e di attacchi, vi spiegheremo le caratteristiche di queste recenti attività illecite dei cybercriminali e, soprattutto, vi mostreremo le più recenti e efficienti soluzioni ad oggi disponibili sul mercato per combattere questi nuovi crimini informatici.

Relatore: Maurizio Martinozzi

16.00-16:30 - Visita all'area espositiva

16:30-18:00 - Seminario a cura dell'Italian Security Professional Group

"Prevenzione delle minacce e reazione rapida agli attacchi nel nuovo scenario multicanale: situazione attuale, tendenze e soluzioni per Web, Mobile e Social"

La rapida evoluzione delle modalità di interazione con gli utenti finali, che sempre più spesso si realizza tramite piattaforme digitali in una logica di multicanalità (Web, Mobile e Social), presenta una serie di innegabili vantaggi sia per le Aziende che per i Clienti.

In questo scenario emergono però anche una serie importante di problematiche di Security (in senso esteso), che vanno dalla prevenzione degli attacchi sempre più sofisticati dei cyber criminali e degli hacktivist, alle attività anti-frode, ai processi di early warning e di cyber intelligence, alla gestione della reputazione ed al monitoraggio costante della conversazione online in un'ottica di Security, e non solo di Marketing.

Discutiamo di scenari, minacce e soluzioni con un panel di esperti di primo piano, che sono in prima linea del gestire queste tematiche da punti di vista differenti e complementari.

16:30-18:00 - Seminario a cura dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC)

"Pillole di Security - Cosa c'entra WindowsXP con le Infrastrutture Critiche?" Ovvero: l'informatizzazione nelle Infrastrutture Critiche e la fine assistenza di Windows XP e di altri sistemi operativi.

Ad oggi, oltre due mesi dopo l'annuncio dell'End Of Live per WindowsXP da parte di Microsoft, sono ancora molti i sistemi con a bordo questo S.O.: quante sono le Infrastrutture Critiche che funzionano con questa criticità?

Una situazione aggiornata "ufficiale" è impossibile da avere, per comprensibili vincoli di riservatezza da parte delle I.C. più "esposte", mentre altre hanno da tempo intrapreso "bonifiche".

La complicazione da affrontare è la variegata presenza di S.O. che popolano il mondo di SCADA, di controlli remoti su rete, di sale di Controllo e negli uffici stessi e che va dal sempiterno "DOS" a XP passando da NT, 2000, ME, Vista e Windows7: tutti sistemi da abbandonare subito o entro i prossimi 5 anni.

Ma allora è davvero una criticità? La stiamo sottovalutando e abbiamo sbagliato o stiamo sopravalutando il caso. Come è possibile nelle IC difendere i sistemi con XP, in attesa di metterli in sicurezza definitiva? Quali i percorsi virtuosi già intrapresi o da percorrere?

Sono queste solo alcune delle domande e dei temi che verranno approfonditi in questo talkshow che vedrà un Panel con alcuni esponenti dal mondo delle Istituzioni, delle IC e della "remediation".

Moderano: Enzo M. Tieghi e Piergiorgio Foti, Vicepresidenti AIIC

Partecipano:

- Pierluigi Paganini, Member of the Threat Landscape Stakeholder Group presso ENISA
- Raoul Chiesa, Founding Partner & President @ Security Brokers, socio AIIC
- Andrea Guarino, Responsabile Tutela del Patrimonio - ACEA SPA, socio AIIC
- Angelo Luca Barba, Marketing Cyber Security – Selex ES, socio AIIC
- Giorgio Basanisi, Senior Manager Spike Reply, socio AIIC
- Andrea Carcano, CTO & Founder Nozomi Networks, socio AIIC

16:30-18:00 - Seminario a cura dell'Associazione Informatici Professionisti (AIP)

Lo scenario delle professioni e dei professionisti sta subendo una rapida e interessante evoluzione, la legge 4 e il decreto legislativo 13, emanati nel Gennaio del 2013, infatti, possono influire in maniera rapida e positiva sia nel

sistema della attestazione e certificazione professionale, sia nei sistemi formativi a tutti i livelli fino al terzo ciclo.

Il quadro normativo di riferimento è completato dal decreto legislativo 206 del 2007 e dagli standard internazionali di riferimento come: la norma Uni Cei En Iso/Iec 17024:2004 che descrive i requisiti generali per organismi che operano nella certificazione delle persone, la linea guida Cen14:2010 per le attività di normazione sulla qualificazione delle professioni e del personale, l'Eqf (European qualification framework) ed i repertori nazionali di Ateco, CpIstat e Miur che ci forniscono le tassonomie di mestieri e titoli, costituiscono l'infrastruttura normativa su cui abbiamo basato il nostro solido processo di attestazione e certificazione delle persone.

Nell'ambito delle professioni informatiche è stata inoltre recentemente emanata la norma Uni11506 per le attività professionali non regolamentate e riferibili alle figure professionali operanti nel settore ICT che alla luce delle recenti notività legislative è utile al fine del conseguimento di una certificazione di conformità alla norma (UNI 11506), come previsto dall'Articolo 7 comma f.

Il partner individuato da AIP-ITCS per questa certificazione è Kiwa-Cermet, la principale società italiana per la certificazione delle persone e accreditata Accredia secondo lo standard 17024 mentre l'apporto culturale di Clusit e dell'Università degli Studi di Verona è stato determinante per la realizzazione di un comitato di schema di prim'ordine. I primi due profili professionali scelti dei 23 previsti e sono l'ICT Security Specialist e l'ICT Security Manager.

Intervengono:

- Andrea Violetti, su "Certificazione delle competenze: la norma Uni 11506 e i nuovi riferimenti legislativi sulle professioni"
- Alessandro Frillici, su "Colpa in eligendo: le competenze a supporto della responsabilità amministrativa delle persone giuridiche (ex Dlgs 231/01)"
- Alessio Pennasilico, su "ICT security manager, ICT security specialist: due figure professionali di rilievo per la sicurezza informatica"
- Franco Fontana, su "La certificazione delle persone secondo lo standard Uni Cei En Iso/Iec 17024".

Segue:

18.30-20.30 HACKING FILM FESTIVAL

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

3. PROGRAMMA DEL 19 GIUGNO

09:00 Registrazione

09:30-11:00 - Percorso Professionale sulla Gestione della Sicurezza

"Quando il frigorifero inizia ad inviare Phishing, forse andrebbe rivalutata la strategia di security"

Il marketing è geniale nel descrivere scenari futuristici di Internet of Things, Augmented Reality, Always Connected, e claim analoghi. Tanti sono i vantaggi che l'evoluzione tecnologica può portare nella nostra vita e nel nostro lavoro. Troppi sono i rischi ancora ignorati. Ci chiederemo assieme se le nostre reti aziendali sono ancora adatti ad affrontare rischi inusuali, quali fax, frullatori ed utenti :)

Docente: Alessio Pennasilico

09:30-10:15 - Atelier Tecnologico

"Perché incontrare 30 persone prima di assumerne una?" (il problema del gestire le risorse umane nei team che si occupano di Informatica, in particolare in quelli che si occupano di security)

Trovare un nuovo collaboratore per le aziende che si occupano di security è sempre difficilissimo. Per i clienti finali anche la semplice selezione IT è spesso difficoltosa. Discuteremo delle diverse necessità e problemi che si manifestano nel reperire le persone, nello scegliere come gestirle, accennando anche a problemi come quello della formazione, che verrà trattato nell'atelier seguente e delle certificazioni, che verrà trattato il XX. Decidere se avere dipendenti o collaboratori, come valutare le competenze, gli atteggiamenti, l'idoneità al ruolo da ricoprire, come gestire la formazione continua e cosa fare nel caso in cui una risorsa decida di abbandonare l'azienda sono gli spunti che vorremmo discutere con il pubblico.

Relatori: Pamela Pace ed Elena Esposito (WestHouse)

09:30-10:15 - Atelier Tecnologico

"Tanta fatica solo per un bollino, ne vale davvero la pena?"

Il mondo dei Sistemi di Gestione è in continua evoluzione e sviluppo: sempre più spesso viene richiesto alle società di possedere Sistemi di Gestione certificati per poter partecipare a bandi, concorsi e gare. Tale necessità sfocia spesso nella creazione di Sistemi di Gestione talvolta affrettata, a volte senza un'attenta pianificazione e in casi estremi senza considerare la presenza di sistemi di Gestione affini già esistenti in altri rami d'azienda.

Durante l'intervento, partendo dall'esperienza diretta dei relatori, verrà proposto un percorso per la definizione dei Sistemi di Gestione con particolare attenzione a quelli per la Sicurezza delle Informazioni ed evidenziando affinità e divergenze rispetto ai Sistemi di Gestione della Qualità (ISO 9001:2008) che ormai la

maggior parte della aziende possiedono, e ai Sistemi di Gestione per i Servizi IT (ISO 20000:2011).

Verranno inoltre analizzati casi concreti che evidenziano gli aspetti positivi e negativi relativi all'attuazione di Sistemi di Gestione integrati rispetto a Sistemi di Gestione disgiunti.

Sarà effettuata poi un'analisi puntuale sulle modalità di definizione dei perimetri, tematica che genera spesso grande confusione, e in ultimo, analizzando i controlli del capitolo 17 dell'Annex A della ISO/IEC 27001:2013, sarà effettuato un breve confronto con i requisiti della norma ISO 22301:2013 inerente la Continuità Operativa.

Docenti: Alberto Perrone e Paolo Sferlazza

10:15-11:00 - Atelier Tecnologico

"Smettiamo di proteggere i server... iniziamo a proteggere i dati!"

olte le basi dati presenti in ogni organizzazione, poco omogenee, ma soprattutto esposte a grandi rischi. Poter valutare il rischio, misurare la sicurezza delle informazioni e controllare per poter intercettare le anomalie diventa fondamentale.

In questi scenari l'informatica diventa strumento essenziale per poter esercitare il corretto controllo, sia a livelli di compliance che di business requirements, al fine di permettere di prendere le decisioni giuste. Sapendo cosa bisogna decidere.

Docenti: Corrado Giustozzi, Nicola Fusco e Paolo Maria Camussi (Dirigente Internal Audit Fondazione Enasarco)

10:15-11:00 - Atelier Tecnologico

"Connessione globale e riservatezza delle informazioni: nativi digitali e nuove sinapsi"

La connessione globale e la riservatezza delle informazioni: per molti rappresenta un ossimoro. In gioco diverse generazioni, diversi approcci e persino nuove sinapsi.

Cosa cambia per la società e cosa per il business?

Docenti: Armando Leotta e Sabina Di Giuliomaria

11.00-11.30 coffee Break e visita all'area espositiva

11:30-13:00 - Percorso Professionale Tecnico

"New Generation SOC"

La struttura del Security Operations Center (SOC) ha attualmente l'opportunità di essere la pietra angolare su cui costruire ed evolvere la security posture di un'organizzazione. Gli strumenti tipici del SOC, tra cui il SIEM, sono in grado di integrare pressochè la totalità delle sorgenti dati digitali garantendo l'attuazione

non solo di processi reattivi, ma anche proattivi. Il perimetro di raccolta delle informazioni può facilmente espandersi dai classici sistemi di sicurezza perimetrale verso le applicazioni di business e il Big Data. L'analisi evoluta di tale miriade di informazioni – attualmente disseminate e disperse – consente di aumentare la visibilità sui processi di business e disporre di analisi comportamentali, anomalie, serie storiche, etc. L'aumento della conoscenza abilita un superiore livello di Situational Awareness e una maggiore capacità di prendere decisioni informate e contestualizzate.

Docenti: Claudio Telmon, Alfredo Rinaldi, Marco Di Leo

11:30-12:15 - Atelier Tecnologico

"Cosa i Social Network sanno di te che tu non hai condiviso"

Le problematiche di sicurezza legate al mondo dei social network (Linkedin, Facebook, Google+, …) sono sicuramente uno dei temi più trattati e dibattuti di questi ultimi anni.

Cercando di dare il nostro contributo all'argomento, in questa presentazione ci soffermeremo sugli aspetti meno noti e poco conosciuti che influenzano la nostra presenza in rete e la nostra navigazione.

Giocando con la citazione "There are known knowns" di Donald Rumsfeld vedremo i seguenti punti:

•una introduzione alle problematiche note (quello che sappiamo di sapere e/o di non sapere)

•una serie di domande sulle criticità ad oggi ancora non conosciute (quello che non sappiamo di non sapere)

•l'analisi di tutte quelle problematiche che pur essendo davanti ai nostri occhi sono poco o non conosciute (quello che non sappiamo di sapere)

In particolar modo porremo l'attenzione al tracciamento degli utenti concludendo con una descrizione (e suggerimento) di quelli che al momento sono i tools e le soluzioni migliori per difendersi dal "socialeaks".

Docenti: Alessandro Gai e Maurizio Agazzini

11:30-12:15 - Atelier Tecnologicio

"Sourcefire, security for the real world"

Relatore: Stefano Volpi

12:15-13:00 - Atelier Tecnologico

"Una difesa integrata per contrastare attacchi sempre più sofisticati"

Le aziende devono proteggere i loro dati critici in un contesto dove le minacce di tipo Advanced Persistent Threats, attacchi di tipo "zero day", violazioni dei dati e relativo impatto economico sono in continuo aumento. Secondo studi

recenti il costo medio aziendale delle violazioni di dati è aumentato del 15% a livello globale, raggiungendo una media di 3,5 milioni di dollari.

Occorre trovare una soluzione basata sulla Security Intelligence e sull'Analytics che permetta di andare al di là delle difese tradizionali di controllo accessi e firewall tradizionali, permettendo di interrompere gli attacchi sull'intera catena, dall'intrusione (break-in) alla sottrazione dei dati (exfiltrate), aiutando le organizzazioni a prevenire, rilevare e reagire ai cyber-attacchi continui e sofisticati e, in alcuni casi, a eliminare la minaccia prima che si verifichi il danno

Relatore: Domenico Raguseo

12:15-13:00 - Atelier Tecnologico

"Soluzioni DELL SECURITY – le innovative combinazioni dei prodotti DELL "

Docenti: Cristiano Cafferata e Claudio Dell'Ali

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

14:30-16:00 - Percorso Professionale Legale

"I contratti per i servizi cloud: elementi contrattuali e profili inerenti la sicurezza"

Il seminario mira a approfondire le più rilevanti tematiche contrattuali sottese ai contratti per i servizi cloud con un focus specifico sul tema delle obbligazioni a carico dei fornitori inerenti la sicurezza dei dati e delle informazioni. Tra le altre, verranno analizzate le tematiche inerenti le informazioni precontrattuali, le obbligazioni del fornitore, i livelli di servizio, i meccanismi di penalizzazione, i diritti di modifica unilaterale del contratto che i fornitori tipicamente si riservano, le limitazioni di responsabilità. Inoltre, sarà analizzato il tema della sicurezza delle informazioni e dei dati trattati dai fornitori di servizi cloud anche alla luce delle vigenti normative. Durante l'intervento saranno analizzate le indicazioni fornite dal Garante per la protezione dei dati personali e dall'Article 29 data protection workin party in materia di cloud e verranno fornite indicazioni in merito agli approfondimenti che sono in corso da parte del Gruppo di Esperti di contratti di cloud computing della Commissione Europea.

Docente: Gabriele Faggioli, membro del Gruppo di Esperti di contratti di cloud computing della Commissione Europea.

14:30-15:15 - Atelier Tecnologico

"PCI-DSS, terza versione"

La PCI-DSS si rinnova ancora con la recente uscita della sua terza versione. Cosa cambia, da quando ma soprattutto: quali sono le migliori strategie per affrontare la compliance allo standard che impatterà sempre di più chi accetta o gestisce dei pagamenti con carta in Italia? Questo e altro sul tema nel corso di una concentrata sessione tenuta da due QSA.

Docenti: Fabio Guasconi e Francesco Morini

14:30-15:15 - Atelier Tecnologico

"Rischi legati alle identità: quale è la vera minaccia interna?"

Docente: Fabio Ivaldi

15:15-16:00 - Atelier Tecnologico

"Cyberterrorismo: una minaccia credibile?"

Partendo dalle definizioni di cyberweapon e cyber terrorismo, nel corso dell'intervento saranno analizzati i possibili scenari di attacco e di utilizzo di tool e tecnologie cyber ai fini di organizzare e portare a termine attacchi terroristici. Sarà infine proposto un possibile scenario che verrà analizzato secondo metodologie di analisi del rischio statuali.

Docente: Matteo Cavallini

15:15-16:00 - Atelier Tecnologico

"Cinquanta sfumature di cyber"
Oggi tutto è cyber, e chi non è cyber è out. Pochi tuttavia conoscono la reale origine della buzzword del momento, che per quanto sembri modernissima e futuribile ha invece una storia lunga oltre tremila anni. Così, in un viaggio semiserio fra linguistica, scienza e fantascienza, scomoderemo Platone, Wiener e Gibson per approdare infine al mondo di oggi, dove il cyber è definitivamente considerato il quinto dominio del warfare, per commentare quindi la recente iniziativa strategica italiana per la protezione dello spazio cibernetico.

Docente: Corrado Giustozzi

16.00-16.30 Visita all'area espositiva

16:30-18:00 - Percorso Professionale Tecnico

“Alice e Bob nel Paese delle Meraviglie” Information Security, Reputation e la realtà italiana: un’analisi ironica, ma costruttiva dell’IT nostrana e del prossimo futuro. Questo panel, suddiviso in tre sessioni distinte e collegate, vuole generare un dibattito con il pubblico in merito al tema della sicurezza delle informazioni e delle cause del progressivo decadimento della qualità dell'IT pubblica italiana.
Inizieremo in chiave positiva (Alice), analizzando i fattori abilitanti dell'Information Security e focalizzandoci innanzitutto sugli aspetti relativi al "clima aziendale" ed alla c.d. "reputation", grazie all'intervento della Prof.ssa Isabella Corradini.
Nella seconda parte (Bob), l’intervento a due voci di Raoul Chiesa e Carlo Simonelli, proverà a definire - in maniera non proprio accademica, ma attendibile - i motivi per cui, in Italia, questo “Alice in Wonderland” non funziona.
Concluderemo con un dibattito/tavola rotonda, durante il quale il pubblico sarà chiamato ad esporre le proprie esperienze aziendali e personali e ad ipotizzare delle soluzioni ai problemi esposti.

Relatori: Raoul Chiesa, Isabella Corradini, Carlo Simonelli

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

"Bitcoin: cyberinvestigation tra aspetti tecnici e giuridici."

Sono previsti 3 interventi.

"IISFA Cybercop 2014"

Una delle più avvincenti simulazioni di indagini digitali si è da poco conclusa con la premiazione della Relazione Tecnica più esauriente.

Partendo da una denuncia per estorsione scattata su Facebook e richiesta di pagamento tramite bitcoin, cinque squadre si sono sfidate analizzando computer e Telefoni passando attraverso l'analisi di tabulati e log per culminare con l'arresto dell'estortore attraverso la tecnica OSINT.

In questo talk cercheremo di capire come le squadre si sono mosse, come hanno interpretato i vari indizi e cosa ha permesso ad una di primeggiare sulle altre.

Docente: Litiano Piccin

"Bitcoin 2.0 sta superando la sua tempestosa adolescenza?"

Lo davano per morto dopo la caduta di MTGOX e invece fa ancora parlare di sé.

Negli ultimi mesi la potenza di calcolo della rete Bitcoin è triplicata e il suo valore ricomincia a crescere. Combatte ogni giorno con le accuse sempre più pressanti di essere un bene di scambio adatto per le attività criminose in quanto garantirebbe l'anonimato, ma di fatto la blockchain permette a chiunque di seguire e indagare ogni singola transazione. In questo talk vedremo una panoramica sui principali exchangers internazionali italiani.

Docente: Luigi Ranzato

"Bitcoin: aspetti giuridico/economici e fiscali. Il problema del cybericiclaggio"

Bitcoin e le criptovalute rappresentano una sfida estremamente interessante non solo al monopolio monetario ma anche per gli operatori economici e del diritto, perché costituisce un modo originale di rappresentare lo strumento principale usato dall'umanità per pagare un corrispettivo in cambio di un bene o un servizio. Il fenomeno richiede che sia fatta chiarezza sulla natura giuridica e sul trattamento fiscale, anticipando le tendenze. Un intervento del legislatore non è eludibile in ragione del fatto che l'indipendenza da ogni ente centrale e la natura tecnologica imprimono una velocità di diffusione inimmaginabile rispetto agli strumenti tradizionali: i rischi di ingenti trasferimenti di ricchezza in violazione di norme fiscali e penali costituiscono a loro volta fonte di attacchi alla sovranità dei singoli stati nella sua manifestazione principale, quella di creare moneta e di esigere le imposte.

Docente: Antonino Attanasio

4. HACKING FILM FESTIVAL

L' edizione romana dell'Hacking Film Festival, evento culturale "satellite" del Security Summit, sarà dedicata a cortometraggi e filmati indipendenti sul tema dell'hacking e della (in)sicurezza.

Il 18 giugno dalle 18.30 alle 20.00 saranno proiettate opere che illustrano "dall'interno" l'ambiente e il fenomeno hacker, i casi giudiziari più importanti che hanno attraversato il panorama tecnologico underground e le problematiche di sicurezza e vulnerabilità dei sistemi.

Sono quasi tutte 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.

Durante il Festival Alessio Pennasilico, Cristiano Cafferata, Raoul Chiesa e Corrado Giustozzi, insieme ad altri ospiti, coordineranno un breve dibattito sui contenuti e ascolteranno e commenteranno le osservazioni del pubblico.

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.

PROGRAMMAZIONE

18 giugno, 18.30 – 20.00

Proiezione e dibattito:
Underground: The Julian Assange Story di Robert Connolly – Australia 2012.
(Film tv sulla storia del fondatore di WikiLeaks Julian Assange)

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

5. ATTESTATI E CREDITI CPE

Tutte le sessioni, tenute da esperti del mondo accademico e da professionisti del settore, 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 solo a chi ha assistito all'intera sessione e risulta regolarmente registrato.
Gli attestati saranno inviati, per email, solo a chi ne farà richiesta a attestati@clusit.it.
Le richieste possono essere fatte solo a partire dal 20 giugno.

6. GLI SPONSOR

Sponsor Partner


Sponsor Gold


Sponsor Silver

Sponsor Tecnico

Sponsor dell'Hacking Film Festival

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*

Dipartimento di Informatica - Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285

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