SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

BARI 2014

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni alla seconda edizione del Security Summit di Bari, che si terrà il 29 maggio presso il Mercure Villa Romanazzi Carducci http://156.54.105.150/congressi.aspx.

La partecipazione al Security Summit e a tutti gli eventi che lo compongono è libera e gratuita, ma è necessario iscriversi online su https://www.securitysummit.it/bari-2014, anche per evitare code e perdite di tempo alla reception del Summit.

2. PROGRAMMA

09.00 Registrazione

9.30-11.00 – SESSIONE PLENARIA

"Presentazione del Rapporto Clusit 2014"

I lavori della seconda edizione del Security Summit di Bari si aprono con la presentazione del Rapporto Clusit 2014, che inizia con una panoramica degli eventi di cyber-crime e incidenti informatici più significativi degli ultimi dodici mesi. Si tratta di un quadro estremamente aggiornato ed esaustivo della situazione globale, con particolare attenzione alla situazione italiana. Abbiamo classificato ed analizzato 1.152 attacchi noti del 2013, suddivisi per tipologia di attaccanti e di vittime e per tipologia di tecniche d'attacco. A questa analisi si è aggiunto quest'anno un nuovo formidabile strumento di rilevazione. Infatti, per la prima volta in Italia, abbiamo avuto a disposizione anche i dati relativi agli incidenti rilevati, aggregati in forma anonima e classificati dal Security Operations Center di FASTWEB, che ha gentilmente acconsentito a condividerli con Clusit.

Il Rapporto contiene anche i risultati di una survey che ha coinvolto ben 438 aziende e che ci ha consentito di analizzare le tendenze del mercato italiano dell'ICT Security, individuando le aree in cui si stanno orientando gli investimenti di aziende e Pubbliche Amministrazioni. Riguardo il mercato del lavoro, lo studio ha evidenziato quali sono le figure professionali più richieste, con l'intento di facilitare le scelte di studenti e professionisti. Si forniscono inoltre importanti approfondimenti su una quantità di temi caldi: Smartphone, Tablet e Social Networks in Azienda; La strategia europea per la cybersecurity; Lo stato della digital forensics in Italia; La sicurezza delle informazioni in azienda ed i controlli interni; Security By Design; La Security vista dal Management; Formazione e Consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni.

Aprono i lavori:

- **Mariella Pappalepore, presidente della Sezione Terziario Innovativo e Comunicazione di Confindustria Bari;**
- **Giuseppe Riccardi, vice presidente della Camera di Commercio di Bari.**

Intervengono:

- **Lino Fornaro, Direttivo Clusit, coordinatore delle attività dell'associazione nel Sud Italia**
- **Alessio Pennasilico, Direttivo e CTS Clusit, coautore del Rapporto Clusit**
- **Stefano Ricca, Responsabile della Divisione Informatica di RICCA**

- Corrado Aaron Visaggio, Docente Dipartimento di Ingegneria, Università degli Studi del Sannio
- Andrea Zapparoli Manzoni, Direttivo Clusit, coautore del Rapporto Clusit 2014

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

11.00-11.30 coffee Break e visita all'area espositiva

11.30-13.00 - Percorso Professionale Tecnico

"Modalità di attacco e tecniche di difesa"

Abstact : Sentiamo sempre più spesso parlare di cybercrime come di rischio imminente, quasi imprescindibile ed improvvisamente si innesca quel meccanismo di autodifesa che ci suggerisce che invece siamo sicuri, che queste paure vengono amplificate da fornitori che hanno interessi specifici, che comunque la probabilità è bassa , che comunque le macchine sono già dotate di firewall e antivirus. Ma siamo veramente di fronte ad un rischio imminente ed imprescindibile ? Perché parlare di cybercrime partendo dalla descrizione di strumenti di difesa ? Proviamo invece a parlare di modalità di attacco , scopriremo che magari siamo stati delle vittime , magari inconsapevoli e che magari avremo potuto evitarle applicando solo delle regole di buon senso, che implicano conoscenza. In questa sessione faremo luce sulle modalità di attacco più diffuse, phishing, cross-site scripting, SQL Injection. Suggeriremo pratiche da adottare e tecnologie adatte a mitigare i rischi.

Docenti: Andrea Zapparoli Manzoni e Domenico Raguseo

11:30-13:00 - Percorso professionale Tecnico

"1-2-3 Stella! Ovvero come trovare il criminale nascosto nella tua rete"

Abstract: I criminali operano ad un ritmo serrato, sviluppando continuamente nuovi attacchi e prendendo di mira in modo accurato le proprie vittime grazie a malware personalizzato.

L'implementazione di soluzioni di sicurezza moderne e dinamiche, nonchè tutte le attività di check-up della security, sono di vitale importanza per la salvaguardia delle aziende da violazioni e perdita di dati. Chi si affida a tecnologie obsolete e/o non controlla quel che davvero avviene nella propria rete ogni giorno, rischia di ospitare inconsapevolmente nella propria infrastruttura minacce che nella migliore delle ipotesi danneggiano gli altri. Nella peggiore, fanno perdere molto denaro all'azienda stessa. Cercheremo di capire le tecniche di attacco e le eventuali contromisure da adottare.

Docenti: Alessio Pennasilico e David Gubiani

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

14:30-15:30 Percorso Professionale Tecnico

"Prendetevi tutto, ma non il mio ….. ! Ovvero quando non avere dati sensibili diventa un problema serio"

Abstract: Riprendendo un famoso spot in cui una modella difende il suo orologio come se fosse un cimelio preziosissimo, facciamo una riflessione su quale sia per noi "il" bene più prezioso da difendere. Tenere bassa la guardia perché si pensa di non avere nulla da difendere (o da perdere) può essere molto pericoloso, specie quando il pericolo c'è ma non si vede. In un mondo ormai interconnesso, dove fenomeni come il BYOD, l'IoT, i social network, l'infomobility, hanno di fatto annullato i confini tradizionali dell'azienda, non si è sviluppata parimenti, un'adeguata consapevolezza delle minacce di questo nuovo contesto. Le PMI, inoltre, ritengono di non essere dei target interessanti per i cyber-attacchi, mentre le statistiche dimostrano il contrario. Rifletteremo insieme sul perché questo accade evidenziando le reali problematiche di security e gli impatti nella quotidianità. Vedremo come è importante dotarsi di strumenti di controllo che ci consentono di evitare brutte sorprese.

Docenti: Lino Fornaro e Giovanni Giovannelli

14:30-15:30 Percorso Professionale sulla Gestione della Sicurezza

" Android Security: Limiti degli attuali meccanismi di detection e possibili linee di evoluzione"

Abstract: L'ampia diffusione di dispositivi mobili Android ed il suo sistema "aperto" lo ha reso, negli ultimi due anni, la piattaforma mobile maggiormente attaccata. La cultura della sicurezza informatica è sicuramente poco diffusa nella popolazione di utenti Android e soprattutto la percezione del rischio è pressoché inesistente (se si esclude una piccola porzione di utilizzatori avanzati). Questo ha portato ad una rapida crescita del numero di malware e ad una conseguente diffusione ad ampio raggio. Si aggiunga che lo spettro di famiglie di malware, classificabili per tipologia di infezione e per payload, si sta allargando in modo estremamente rapido. Il tradizionale meccanismo signature-based di detection dei malware android è chiaramente fallimentare nei riguardi di una grossa porzione di famiglie di malware Android. La ricerca sta producendo numerose metodologie di difesa, non tutte con lo stesso grado di efficacia o, comunque, non tutte efficaci contro lo stesso tipo di malware. Obiettivo di questo intervento è illustrare quali sono le tipologie di malware android presenti attualmente e quali sono le più promettenti metodologie di difesa che potranno costituire lo scenario dell'immediato futuro degli antimalware per android.

Docente: Corrado Aaron Visaggio

15.30-16.00 Visita all'area espositiva

16:00-17:00 Percorso Professionale Legale

"La privacy in Europa: verso il cambiamento"

Abstract: Il diritto alla protezione dei dati personali è fondamentale a livello sia nazionale sia internazionale.

Quanto accade a livello europeo in materia di privacy è importante anche perché il Regolamento che disciplinerà le nuove norme sarà direttamente efficace in tutti gli Stati membri.

La privacy si associa alla sicurezza anche se i due ambiti non sono equivalenti perché la privacy comprende anche la sicurezza, ma non è vero il contrario.

E' necessaria, pertanto, un'analisi adeguata di ogni aspetto connesso alla sicurezza senza prescindere dai rischi e dalla valutazione d'impatto sulla privacy.

E' sempre più importante, alla luce della evoluzione tecnica e normativa internazionale, ragionare in termini di interoperabilità delle risorse e degli strumenti, anche in relazione alla sicurezza, impostando uno standard privacy che utilizzando un approccio metodologico corretto consenta di facilitare la tutela dei dati personali ed ella riservatezza. I consessi internazionali hanno individuato la Privacy by Design come espressione del futuro della privacy; in Europa di discute di data protection by design and by default ed è fondamentale convergere - al di là del nome - verso lo stesso approccio metodologico.

Docenti: Lino Fornaro e Nicola Fabiano

16:00-17:00 Seminario a cura dell'Associazione Informatici Professionisti (AIP)

Sono previsti due interventi:

- **Certificazione delle competenze: la norma Uni 11506 e i nuovi riferimenti legislativi sulle professioni**

Relatore: Rosario Carrisi.

- **ICT security manager, ICT security specialist: due figure professionali di rilievo per la sicurezza informatica**

Relatore: Alessio Pennasilico

Seguono:

17.30-19.30 HACKING FILM FESTIVAL

19.30-20.30 APERITIVO

3. HACKING FILM FESTIVAL

La seconda edizione pugliese 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.

A fine pomeriggio, dalle 17.30 alle 19.30 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.

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

29 maggio, 17.30 – 19.30

- **Manifesto hacker by Marco 1.0**
- **The Disney Trap: How Copyright Steals our Stories**
- **I wouldn't steal…but i do dowloand films**

4. 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 e 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 30 maggio.

5. GLI SPONSOR DEL SECURITY SUMMIT DI BARI

Partner

Platinum

Silver

Sponsor dell'Hacking Film Festival:

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