SPECIALE

ROMA

Indice

1. PRESENTAZIONE
2. PROGRAMMA DEL 10 GIUGNO
3. PROGRAMMA DEL 11 GIUGNO
4. ATTESTATI E CREDITI CPE
5. GLI SPONSOR DEL SECURITY SUMMIT

1. PRESENTAZIONE

Sono aperte le iscrizioni al Security Summit di Roma, che si terrà nei giorni 10 e 11 giugno presso l'SGM Conference Center
www.sgmconferencecenter.it

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

Per chi vuole rivivere in parte il Summit di Milano in marzo, ricordiamo che sU https://www.securitysummit.it/page/video sono disponibili i video degli interventi dei keynote: Gadi Evron e Piotr Oleszkiewicz. Sono pure disponibili i video delle principali Tavole Rotonde e degli Atelier Tecnologici, e alcune Videointerviste.

Nella pagina http://milano.securitysummit.it/photo troverete diverse foto realizzate nei tre giorni del summit.

Sul gruppo SECURITY SUMMIT su Facebook
www.facebook.com/group.php?gid=64807913680, troverete una più vasta raccolta di foto. Sempre su Facebook, potete porre delle domande ai docenti del summit di Roma. Come abbiamo già fatto a Milano, queste domande saranno catalogate e raggruppate per argomento e poste dal Clusit a docenti e relatori, di cui pubblicheremo le risposte.

2. PROGRAMMA DEL 10 GIUGNO

09:00 Registrazione

10:00-13:00 MANIFESTAZIONE DI APERTURA

In apertura del Summit è prevista una sessione plenaria d'eccezione: un incontro con i rappresentanti del Governo, delle Autority, del sistema Confindustria e delle Imprese. Una tavola rotonda dal titolo «Sicurezza delle informazioni e della rete: nuove sfide per le istituzioni e le imprese», nella quale si dibatterà di protezione delle informazioni e di sicurezza della rete in una società che va verso una digitalizzazione globale e servizi di e-government sempre più estesi: quale è la situazione odierna e quali i piani progettuali perchè la sicurezza ICT sia parte integrante del processo di innovazione tecnologica nel nostro Paese.

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

14:00-18:00 SEMINARIO CLUSIT

Le novità nel campo degli standard per la sicurezza IT

Docenti:

- Fabio Guasconi "Prospettiva ISO/IEC sulla sicurezza ICT"
- Jean Paul Ballerini "PCI Compliance: dallo Standard all'implementazione"
- Anthony Cecil Wright "La Business Continuity, la norma BS25999, lo schema di certificazione BCI"
- Andrea Praitano "La sicurezza secondo ITIL"
- Rita Forsi, direttore dell'ISCOM - Istituto Superiore delle Comunicazioni e Tecnologie dell'Informazione
- Giacinto D'Ammicco "Lo Schema nazionale di certificazione coordinato da OCSI"
- Franco Guida "Uso efficiente dei Common Criteria"
- Murizio Tosti e Stefano Maurini"Network unidirezionale a differente classifica"
- Stefano Ramacciotti "I Common Criteria 3.1 ad un anno di distanza dalla loro entrata in vigore"

14:30-17:30 CONVEGNO organizzato dall'Ospedale Pediatrico Bambino Gesù
La sicurezza informatica in sanità

Moderatore: Massimiliano Raponi, Direttore Sanitario Ospedale Pediatrico Bambino Gesù

Interventi:

- "Sicurezza e privacy: misure minime e misure adeguate"
  Pierfrancesco Ghedini, Direttore Sistemi Informativi e Biotecnologie AUSL Modena e Presidente AISIS - Associazione Italiana Sistemi Informativi Sanitari
- "L'importanza del fattore umano: informazione, formazione, coinvolgimento e collaborazione"
  Andrea Oliani, AO Verona
- Verso un ospedale "senza carta"
  Elio Soldano, Responsabile Sistemi Informativi ULSS 9 di Treviso
- "Interazione tra sistema informatico aziendale, apparati biomedicali e reti"
  Giulio Siccardi, Dirigente Responsabile Servizio Sistemi Informativi e Telematici, Direzione Tecnologie e Infrastruttura Ospedale Pediatrico Bambino Gesù
- Presentazione di uno studio per la Commissione Europea sull'utilizzo delle tecnologie RFID in Sanità
  Lorenzo Valeri, RAND Europe

Educazione Continua in Medicina ECM: Per il Convegno è stata avviata, presso il Ministero della Salute, la procedura prevista per l'accreditamento per le figure professionali di: Medico-Chirurgo, Infermiere e Infermiere Pediatrico.

14:30-15:30 ATELIER TECNOLOGICO a cura di Cisco
Quale futuro per la Sicurezza Informatica nella Pubblica Amministrazione?

Una tavola rotonda fra esperti del settore e visionari: Quali tendenze per la sicurezza informatica nel futuro? Quali tecnologie, competenze ed informazioni da considerare per difendere efficacemente un sistema informativo, dati, cose e persone? Una tavola rotonda tra esperti e ricercatori per mettere a confronto diversi punti di vista sulle tendenze, soluzioni (alcune esistenti, altre che stanno prendendo forma) che ci accompagneranno nei prossimi anni e che permetteranno l'evoluzione dei servizi informatici anche nella Pubblica Amministrazione.

14:30-16:00 PERCORSO PROFESSIONALE TECNICO: 1a sessione
Social Engineering e intrusione fisica

Gli attacchi fisici all'infrastruttura sono sempre più efficaci, hacking via firewire, dischi rigidi esterni, trojan, chiavette usb permettono di creare nuove forme di intrusione che, con un piccolo aiuto mutuato dalla psicologia, possono avere effetti devastanti.
Docente: Raoul Chiesa

16:30-18:00 PERCORSO PROFESSIONALE LEGALE: 1a sessione
La responsabilità amministrativa delle persone giuridiche nei delitti informatici

Docente: Gabriele Faggioli

3. PROGRAMMA DEL 11 GIUGNO

09:00 Registrazione

09:00-13:00 SEMINARIO CLUSIT
SCADA & DCS Security Tutto quello che vorreste sapere sulla protezione di reti e sistemi di controllo ed automazione e non avete mai osato chiedere

Docenti:

- Raoul Chiesa
- Fabio Guasconi
- Alessio Pennasilico
- Enzo M. Tieghi

9:30-11:00 TAVOLA ROTONDA
Sicurezza delle Infrastrutture Critiche

Chairman: Luisa Franchina, direttore generale Protezione Civile

Partecipano:

- Daniele Perucchini, FUB, Responsabile Area Procedure critiche per la P.A. e le organizzazioni complesse
- Michael Thornton, Joint Research Center, Traceability and Vulnerability Unit
- Salvatore Tucci, Università Tor Vergata, presidente AIIC

9:30-11:00 PERCORSO PROFESSIONALE TECNICO: 2a sessione
Evoluzione del Malware, Botnet e underground economy

Docente: Luigi Mancini

10:00-11:00 ATELIER TECNOLOGICO a cura di TREND MICRO
La nuova frontiera della sicurezza informatica: come, dove e a che livelli difendersi dalle nuove minacce

Internet è oramai una potente piattaforma che ha cambiato il nostro modo di fare business e il nostro modo di comunicare. Offre una crescente base di utenti, infinite informazioni disponibili, e con la continua evoluzione di nuove tecnologie, nuove vulnerabilità e nuove debolezze sfruttabili. In qualsiasi momento si navighi sul Web o si faccia clic su un URL incorporati in un e-mail, mettiamo noi stessi e gli altri a rischio di minacce Web-based. Oggi l'orizzonte delle minacce è caratterizzato da cyber criminali guidati da profitti, che hanno tratto vantaggio dall'evoluzione di Internet per creare una potente economia sommersa.

Le soluzioni di sicurezza di ieri non sono in grado di proteggere dalle minacce di oggi. Le soluzioni di sicurezza oggi hanno bisogno di affrontare due sfide fondamentali:

- Un cambiamento radicale nel panorama delle minacce, che ha prodotto più complesse tipologie di minacce;
- L'esplosione del numero di minacce, che ha dato l'avvio ad un modello a un problema di quantità di pattern download.

Nella prima parte di questo Atelier, dopo una breve introduzione sul fenomeno delle botnet, e sull'elevato numero di malware che sono sistematicamente diffusi anche attraverso le reti botnet (webthreats), si parlerà dell'evoluzione delle minacce e sarà presentata una proiezione dell'incremento malware da qui al 2015. Si parlerà di un nuovo approccio al malware, evidenziando come si possano ridurre i tempi di reazione nei confronti dei nuovi malware, con presentazione di casi concreti.

Docente: Gastone Nencini

11:30-13:00 TAVOLA ROTONDA
Identità, sicurezza e privacy al tempo dei Social Network

Chairman: Gigi Tagliapietra, presidente Clusit

Partecipano:

- Mafe De Baggis
- Nicola Mattina
- Alessio Pennasilico, esperto di security
- Stefano Quintarelli

11:30-12:30 ATELIER TECNOLOGICO a cura di MCAFEE
Un approccio integrato e unificato per la protezione della rete

L'estensione della rete aziendale contribuisce ad aumentare i rischi. Visitatori e dipendenti in viaggio possono collegarsi a sistemi non conformi senza policy di sicurezza. I sistemi non conformi, infetti o con configurazione errate rappresentano un rischio per la sicurezza e aggiungono costi dovuti al downtime e al ripristino dei sistemi e della rete. Anche un solo host infetto in rete può causare danni alla banda di rete o infezioni ad altri sistemi conformi, così come attacchi mirati o un utilizzo non consentito delle risorse aziendali possono causare danni rilevanti in termini di dati ed informazioni aziendali sottratti in maniera fraudolenta. Una corretta strategia di controllo degli accessi alla rete, gestita centralmente, permette di proteggere le aree ad alto rischio in rete – tramite identificazione, quarantena e remediation dei sistemi infetti – con il miglioramento dell'infrastruttura di rete esistente e una conseguente riduzione dei costi.

Nella prima parte dell'atelier, sarà illustrato un approccio integrato alla sicurezza di rete utilizzando soluzioni per la protezione di email e contenuti web, UTM, prevenzione delle intrusioni e User Behavior Analysis, in conformità con le policy di sicurezza.

Nella seconda parte il focus sarà su un nuovo modo di approccio al NAC (Network Access Control) attraverso l'unificazione della protezione di endpoint e rete con controllo accessi e auditing delle policy, il tutto amministrato da un'unica console di gestione.

Docenti:

- Pier Carlo Devoti
- Marcello Romeo

11:30 PERCORSO PROFESSIONALE LEGALE: 2a sessione
Data retention. Limiti e obblighi di legge

Docente: Stefano Aterno

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

14:30-17:30 CONVEGNO
Tutte le novità sulla sicurezza digitale nella Pubblica Amministrazione

Chaiman: Giovanni Manca, Responsabile Ufficio sicurezza del CNIPA

Interventi:

- "Privacy: l'impatto delle recenti disposizioni del Garante sulla P.A."
  Cosimo Comella, Autorità Garante per la protezione dei dati personali
- "Fascicolo Sanitario Elettronico e Dossier Sanitario"
  Stefano Lotti, Technical Program Manager INVITALIA
- "Identità Digitale: Interoperabilità a livello Europeo"
  Giovanni Manca, Responsabile Ufficio sicurezza del CNIPA
- "Nuove regole sull'Identità Digitale"
  Corrado Giustozzi
- "Biometria e nuovi passaporti: collaborazione tra Ministero degli Interni, Polizia di Stato e CNIPA"
  Alessandro Alessandroni, Responsabile Ufficio Osservatorio del mercato del CNIPA
- "Nuove regole sulla firma digitale"
  Stefano Arbia, CNIPA

14:30-16:00 TAVOLA ROTONDA
Le attività delle Istituzioni Europee a supporto della sicurezza informatica e delle reti

Chairman: Lorenzo Valeri, delegato Clusit per i rapporti con la Commissione Europea

Con la partecipazione dell'ENISA, dell'Autorità Europea Garante per la Privacy e dell'UNICRI.

14:30-16:00 PERCORSO PROFESSIONALE TECNICO: 3a sessione
Information Forensics nel "nuovo" panorama tecnico e normativo italiano

Docente: Gerardo Costabile

16:30-18:00 PERCORSO PROFESSIONALE LEGALE: 3a sessione
Il trattamento dei dati personali e le misure di sicurezza. Lo stato dell'arte normativo

Docente: Mario Mazzeo

Il programma è in continuo aggiornamento su www.securitysummit.it

4. ATTESTATI E CREDITI CPE

Le sessioni che prevedono il rilascio di Attestati di Presenza e l'attribuzione di Crediti CPE sono:

- i Percorsi Professionali (tecnico, legale o "gestione della sicurezza");
- gli Atelier Tecnologici;
- i Seminari Tecnici Clusit Education.

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

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

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

Le registrazioni potranno essere accettate anche direttamente alla Reception del Security Summit, ma non potrà essere garantita la disponibilità del posto in sala, né l'eventuale materiale didattico.

A chi avrà assistito, secondo le regole di cui sopra, a tutte e tre le sessioni di uno stesso percorso Professionale sarà rilasciato un Diploma.

8. GLI SPONSOR DEL SECURITY SUMMIT

elenco parziale

Sponsor Partner:

Sponsor Gold:

Sponsor Silver:

Partner e sponsor di Clusit Education:

All'interno del 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.

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