SPECIALE

Indice

1. PRESENTAZIONE

Dal 12 al 14 marzo si terrà a Milano la quarta edizione del Security Summit, presso l'Atahotel Executive, Viale don Luigi Sturzo 45 www.atahotels.it/executive.

Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit offre anche momenti di divulgazione, di approfondimento, di formazione e di confronto. Ci saranno 3 sale che lavoreranno in contemporanea per tre giorni, con tanta formazione specialistica differenziata secondo le esigenze ed il profilo di ciascuno. Oltre 80 i docenti e relatori coinvolti nell'edizione milanese del Summit e più di 30 le associazioni e community che hanno collaborato.

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

Segue il programma delle tre giornate, con i dettagli delle varie sessioni.

2. PROGRAMMA DEL 12 MARZO

09:00 Registrazione

09:30-11:00 - Sessione plenaria
Keynote Speakers: Steve Purser, Head of Technical Department, ENISA - European Network and Information Security Agency
"Improving EU Security Through Proactive Community Building"
This presentation will cover the following points:

- **About ENISA**
- **Protecting Critical Information Infrastructure**
- **Input to EU & MS Cyber Security Strategies**
- **Assisting Operational Communities**
- **Security & Data Breach Notification**
- **Data Protection.**

11:30-13:00 - Percorso professionale sulla gestione della sicurezza
"I primi 100 giorni del Responsabile della Sicurezza delle Informazioni nel Made in Italy"
Sei appena stato nominato Responsabile della Sicurezza delle Informazioni. Quali sono le cose da fare nei primi 100 giorni del tuo nuovo incarico? Quelle urgenti? Importanti? Visibili alla Direzione? Ti concentri su quelle che portano un beneficio a breve oppure non ti fai condizionare da questi "tatticismi"? Come ti comporti nei confronti dei tuoi colleghi e dei manager delle altre linee, come gestione esercizio, sviluppo applicazioni, legale? E in ultima analisi quale sono le cose realmente più importanti?
In questa sessione i partner della Oracle Community for Security presentano al pubblico l'ultima delle loro pubblicazioni che sarà scaricabile dal web dopo il convegno. Il taglio è pratico, essenziale ma non banale. Il target è l'impresa italiana del Made in Italy che non può permettersi grandi investimenti in sicurezza ma che di sicurezza ne ha bisogno ora più che mai.
Moderano: Luca Bechelli e Alessandro Vallega
Intervengono: Riccardo Abeti, Bruno Bernardi, Jonathan Brera, Riccardo Canetta, Paolo Capozucca, Roberto Obialero, Giuseppe Russo e Claudio Telmon.

11:30-13:00 - Percorso professionale tecnico
"Cyber Intelligence come principale strumento di contenimento e prevenzione delle minacce"
La massima "la conoscenza è potere" di Bacon non è mai stata così attuale. Nel complesso scenario odierno, che vede da un lato la transizione della nostra intera civiltà dall'analogico al digitale, e dall'altro il dilagare senza freni delle minacce, dal cyber crime all'hacktivism fino allo spionaggio ed alle prime avvisaglie di cyber warfare, i difensori devono rivalutare i modelli di sicurezza tradizionali ed introdurre alcune importanti innovazioni nel loro modus operandi.
La principale di queste innovazioni è la Cyber Threat Intelligence, attività multidisciplinare di estrema importanza e delicatezza, dai molti risvolti (culturali, organizzativi, legali, tecnologici) che è ormai diventata strategica per contenere le minacce esistenti (la maggior parte delle

organizzazioni sono già costantemente sotto attacco) e per prevenire quelle future. Nel corso del seminario tratteremo degli elementi fondamentali necessari per implementare un processo sostenibile di Cyber Threat Intelligence, e di come misurarne l'efficacia nel tempo.
Docenti: Andrea Zapparoli Manzoni e Fabio Panada.

11:30-13:00 - Percorso professionale sulla gestione della sicurezza
"Dall'Access Governance al Fraud Management: un approccio innovativo e globale nella gestione della sicurezza aziendale"
Docenti: Alessio Pennasilico, Paolo Chieregatti, Filippo Giannelli e Giacomo Parravicini.

14:30-16:00 - Tavola Rotonda
"Presentazione del RAPPORTO CLUSIT 2013"
Nel 2012 abbiamo dato vita al primo "Rapporto sulla sicurezza Ict in Italia", seguito da una seconda edizione, in giugno, e da una versione in inglese. L'interesse suscitato (oltre cinquanta articoli su varie testate, alcune decine di migliaia di richieste pervenuteci per richiedere il rapporto e la reiterata segnalazione e citazione da parte dell'ENISA), ci ha incoraggiato a continuare a produrre il Rapporto Clusit, con cadenza annuale e se possibile aggiornamenti nel corso dell'anno.
Oltre alla consueta analisi degli attacchi ed incidenti del 2012 in Italia e nel mondo, il Rapporto 2013 contiene le tendenze del mercato e degli investimenti in Italia e le tendenze del mercato del lavoro. Si fa inoltre il punto sulla tematiche di maggior interesse del momento, già affrontati nel Rapporto 2012 : la sicurezza nel Mobile, nei Socialmedia, nel Cloud. Due Focus On sono dedicati a due temi centrali per l'Agenda Digitale Italiana : la sicurezza in Sanità e l'e-Commerce. Completano i Focus On del Rapporto 2013: il nuovo protocollo IPv6 e una serie di indicazioni su backup e ripristino dei dati. Tutti i presenti in sala potranno ritirare una copia del rapporto.
Modera: Gigi Tagliapietra, Presidente Clusit
Partecipano:

- Paolo Giudice, Segretario Generale Clusit
- Giovanni Todaro, IBM Security Systems Leader
- Alessandro Vallega, Oracle Security Business Development Manager e Responsabile di Oracle Community for Security.

14:30-16:00 - Percorso professionale tecnico
"Cyber Conflicts: dalla Cyber Intelligence alla Cyber Warfare (scenari strategici, tecnici e legali)"
In questo intervento a due voci i relatori affronteranno i differenti temi attinenti il dominio dei Cyber Conflicts (spesso intrinsicamente collegati) quali: Cyber Intelligence, Cyber Weapons, 0days market e brokerage, Information Warfare e Cyber Warfare, fornendo una visione d'insieme dal punto di vista degli aspetti strategici, tecnici e legali.
E' da ritenersi un percorso avanzato, per partecipanti gia' avvezzi alle tematiche in oggetto, e non una sessione introduttiva.
Docenti: Raoul Chiesa e Stefano Mele.

14:30-16:00 - Percorso professionale legale
"Gli eserciti elettronici e i nuovi aspetti della CyberWarfare: tecniche, equilibri politici, aspetti giuridici"
Diversi Stati stanno operando, più o meno in segreto, per costituire un vero e proprio esercito elettronico che un domani servirà per

combattere nuovi tipi di guerre. Non solo: negli ultimi dieci anni si sono già registrati episodi di utilizzo di tecniche di CyberWarfare durante conflitti tradizionali. In questa sessione di studio affronteremo i temi della nozione e dei limiti della CyberWarfare e degli eserciti elettronici in USA, Russia, Cina, Corea del Nord, Corea del Sud, Siria e Iran.
Docente: Giovanni Ziccardi.

16:30-18:00 - Seminario a cura dell'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 (CD Clusit, CD Assintel, OSN)
Partecipano :

- Raoul Chiesa (PSG Enisa, CD Clusit, OSN)
- Enzo Maria Tieghi (CD AIIC, Clusit)
- Eyal Adar (White Cyber Knight)
- Cristiano Cafferata (Dell Sonicwall)
- Maggiore dell'USAF in audio-conference.

16:30-18:00 - Seminario a cura dell'OWASP Italy Chapter
Sono previsti tre interventi.

"Evoluzione e rischi derivanti dai nuovi sistemi di Banking Malware"
Il panorama malware attuale è molto ricco e variegato ed abbiamo soluzioni adatte sia per Pc che per dispositivi Mobile.
Fra le tante tipologie abbiamo il Banking Malware, che costituisce nel presente una delle più diffuse e comuni minacce per i siti web bancari.
Lo scopo del banking malware consiste nel riuscire a fornire all'attaccante il maggior numero possibile d'informazioni sensibili, incluse le stesse credenziali di accesso. Nelle sue forme e varianti più ricercate un banking malware è inoltre in grado di eseguire autonomamente operazioni fraudolente quali ad esempio i bonifici verso beneficiari malevoli spesso anche inconsapevoli! Vedremo come la tecnologia Banking Malware si è evoluta fino ai giorni nostri, giungendo ai sistemi ATS (Automatic Transfer System) in grado di compiere operazioni fraudolente in completa autonomia.
Docente: Giuseppe Bonfà

"Android e mobile security: client side, server side, privacy (do android malware writers dream of electric sheep?)"
Qual'e' lo stato dell'arte della sicurezza "mobile"? App.. HTML5.. BYOD.. Cloud.. TheNextBuzzword.. come interagiscono queste componenti con la privacy degli utenti, la sicurezza dei dati sui dispositivi e sui server e l'entropia mondiale? E le buone vecchie vulnerabilita' nelle applicazioni web?
Esempi e dettagli su piattaforma Android, adatto piu' in generale a chiunque sia interessato alla sicurezza delle applicazioni "mobile".
Docente: Igor Falcomatà

"OWASP Top Ten Mobile and Mobile Threats"
Presentazione del progetto OWASP Top Ten Mobile con esempi, per poi passare al "mondo reale" e parlare di cosa effettivamente sfruttano gli attaccanti dei dispositivi mobile e cosa effettivamente sbagliano gli sviluppatori mostrando alcuni findings rilevanti trovati durante le attività di assessment.
Docente: Gianrico Ingrosso.

16:30-18:00 - Tavola Rotonda
Premio "Innovare la sicurezza delle informazioni" - 8a edizione
Clusit procederà alla presentazione e premiazione delle migliori tesi universitarie del 2012.
Il premio, oltre a incentivare gli studenti a confrontarsi con i temi della Sicurezza Informatica, ha lo scopo di promuovere una collaborazione tra aziende, Università e studenti: un punto di scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro.
Modera: Gigi Tagliapietra, Presidente Clusit
Intervengono:

- **Claudio Telmon, coordinatore Premio Clusit**
- **Massimiliano Macrì, co-responsabile del Premio Clusit**
- **gli studenti premiati, che presenteranno le proprie tesi**
- **Michele Fautrero, @ Mediaservice.net**
- **Davide Varesano, eMaze**
- **Viviana Rosa, BSI Group Italia.**

3. PROGRAMMA DEL 13 MARZO

09:00 Registrazione

09:30-11:00 - Sessione plenaria
Keynote Speaker: Alessandra Falcinelli, Legal Officer, Trust and Security Commissione Europea, Direzione Generale Reti di comunicazione, contenuti e tecnologie (DG CONNEC).
"Trust and security: Dall' Agenda Digitale Europea alla Strategia UE per la sicurezza cibernetica"
Le iniziative della Commissione Europea in tema di sicurezza delle reti e dei sistemi di informazione iniziano nel 2001. Le relative attività si sono basate sulla promozione della cooperazione tra gli Stati Membri e tra il settore pubblico e quello privato in materia di prevenzione, reazione e gestione dei problemi. L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) è stata creata nel 2004 proprio allo scopo di agevolare lo scambio di best practices e di fornire assistenza tecnica e consulenza alla Commissione, agli Stati Membri e al settore privato.
Nel 2009, con la politica su CIIP ("Critical Information Infrastructure Protection") la Commissione ha lanciato iniziative come lo "European Forum for Member States", dedicato alle discussioni politico-tecniche tra gli organi competenti degli Stati Membri e lo "European Public-Private Partnership for Resilience" che offre una piattaforma di discussione tra il settore pubblico e privato.
L'Agenda Digitale Europea, che si muove dalla Strategia 2020 per l'Unione Europea, identifica trust and security tra i requisiti essenziali per l'accesso del cittadino europeo al mondo digitale. Tra il 2010 e il 2012 l'Agenda Digitale ha guidato iniziative come la proposta di revisione del mandato di ENISA, la creazione di un Computer Emergency Response Team per le istituzioni europee (CERT-EU) e le simulazioni di emergenze cyber a livello europeo.
Alcune azioni (per esempio la creazione di una rete di CERT nazionali attraverso l'Unione) non sono ancora state portate a termine e l'Agenda Digitale promette una politica di sicurezza più forte ed incisiva in questo ambito. Per questo la Commissaria Neelie Kroes ha deciso di intensificare le attività della Commissione nel settore sicurezza e ha unito le forze con la Commissaria agli affari interni Cecilia Malmstrom e con la Alta rappresentante Catherine Ashton. La prima comprensiva strategia UE sulla sicurezza cibernetica presentata lo scorso 7 febbraio annuncia azioni in diverse aree –prevenzione e resilienza, lotta al cybercrime, cyberdefence e cooperazione internazionale – e esplora le relative sinergie. Un'azione chiave della strategia è la proposta di direttiva sulla sicurezza delle reti e dei sistemi di informazione presentata dalla Commissione, che richiede che tutti gli Stati membri, i principali operatori internet (come le piattaforme per il commercio elettronico e le reti sociali) e gli imprenditori nel settore delle infrastrutture critiche come energia, trasporti, servizi bancari e assistenza sanitaria si adoperino per garantire un ambiente digitale sicuro e affidabile nell'intera Unione.

11:30-13:00 - Percorso professionale sulla gestione della sicurezza
"La sicurezza del datacenter all'ombra della "nuvola". Come scongiurare il maltempo?"

Il cloud e le tecnologie che supportano il consolidamento dei sistemi abbattono i confini fisici, rendendo ancora più immateriale e fluido il flusso delle informazioni a beneficio di un business che richiede agilità e velocità. Le aziende italiane tuttavia sembrano guardare con prudenza i modelli di servizio cloud pubblici o misti, ed il retaggio di infrastrutture esistenti frena l'evoluzione verso soluzioni radicalmente nuove. In questa "terra di mezzo", l'azienda deve compiere scelte di sicurezza in grado di garantire la protezione di ambienti diversi: il "nuovo legacy" proprio dell'infrastruttura fisica, ed il "vecchio consolidato", che attende di diventare un vero e proprio Cloud. Cosa privilegiare? Quale approccio adottare?
Durante l'intervento saranno esaminate (a partire da esperienze reali) metodologie e tecnologie per la sicurezza dei datacenter aziendali, per individuarne limiti e opportunità, cercando di offrire spunti di riflessione e discussione. Al termine, saranno presentate soluzioni tecnologiche in grado di gestire la sicurezza di un Datacenter virtualizzato ed in evoluzione verso il Cloud.
Docenti: Luca Bechelli e Riccardo Morsicani

11:30-13:00 - Tavola Rotonda
"L'Agenda Digitale per Pubbliche Amministrazioni ed Enti Pubblici Locali e la sicurezza delle informazioni"
Nel corso della tavola rotonda si parlerà di quanto è previsto nell'Agenda Digitale Italiana per le Pubbliche Amministrazioni e gli Enti Pubblici Locali, anche in termini di servizi per cittadini e imprese, con una visione a livello nazionale, regionale e comunale. E, in questo contesto, si parlerà delle problematiche inerenti la sicurezza delle informazioni e dei servizi erogati.
Modera: Danilo Bruschi, Docente Ordinario all'Università degli Studi di Milano e Presidente Onorario del Clusit
Partecipano:

- Giovanni Rellini Lerz, Agenzia per l'Italia Digitale
- Luigi Pellegrini, Direttore Generale Lombardia Informatica
- Walter Castelnovo, Dipartimento E-government, ANCI Lombardia.

11:30-12:15 - Atelier Tecnologico
"La gestione dell'identità nelle aziende globali: l'esperienza Vodafone"
Il fenomeno della centralizzazione dei sistemi e dei centri di competenza nei grandi gruppi internazionali e il rapido diffondersi delle nuove tecnologie (Mobile) e dei nuovi modelli di business (Cloud) apre a queste aziende nuovi scenari complessi sia per quanto riguarda tematiche di Operations (automazione e gestione) che di monitoraggio (supervisione e controllo). L'allargamento delle funzioni aziendali a dipendenti di operating company di altre nazioni introduce nuove sfide soprattutto nel settore della Sicurezza, dove i punti cardine sono legati a tematiche come la gestione del ciclo di vita di utenze di domini terzi o alla gestione del ciclo di vita degli account su sistemi gestiti centralmente dalle funzioni di gruppo, con tutte le relative tematiche di gestione della riconciliazione e reporting. Definita però la soluzione target resta la complessità della gestione del transitorio dovendo garantire l'efficacia dei controlli in essere. Affrontare questi aspetti sia dal punto dei processi che con soluzioni di "Infrastructural Application" può aiutare a gestire la Governance aziendale.
Docenti: Roberto Botta, Andrea Buzzi e Paola Marino

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.
Docenti: Giovanni Abbadessa e Umberto Sansovini

14:30-16:00 - Percorso professionale legale
Sono previsti due interventi.

"Tutela dei contenuti digitali in Internet e responsabilità civili degli ISP e degli aggregatori di contenuti: sviluppi giurisprudenziali"
Il tema della tutela dei contenuti digitali in Internet - sotto il profilo del diritto d'autore e del contrasto alla pirateria digitale, trascurato dall'Agenda Digitale italiana nonostante il ruolo strategico per lo sviluppo e il rilancio dell'industria dei contenuti e in attesa, ormai da anni, di una regolamentazione da parte di AGCom - è quantomai attuale e controverso e deve trovare un necessario punto di equilibrio tra le contrapposte istanze, da un lato, di legittima remunerazione e tutela dell'autore dell'opera dell'ingegno, dall'altro, di tutela del fondamentale diritto della libertà di espressione e di circolazione delle idee. Una lettura sistematica del quadro giuridico correlato non può prescidere, inoltre, in quanto ad essa strettamente correlata, dall'analisi del ruolo svolto dagli intermediari della società dell'informazione (ISP) e dei c.d. aggregatori di contenuti, anche alla luce della recente emersione giurisprudenziale di nuovi criteri per una distinzione tra ISP- meramente passivi e attivi - gravida di conseguenze giuridiche sul piano delle responsabilità civili di tali soggetti.
Docente: Emilio Tosi

"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

14:30-16:00 - Tavola Rotonda
"La sicurezza delle informazioni in Sanità"
Modera: Claudio Caccia, Presidente AISIS (Associazione Italiana Sistemi Informativi in Sanità) e CIO del Gruppo Multimedica
Partecipano:

- Claudio Telmon, del Consiglio Direttivo Clusit, con delega per l'Agenda Digitale in ambito sanitario, che traccerà lo scenario generale delle problematiche di sicurezza in ambito Sanità e della situazione in Italia;
- Fulvio Barbarito, Responsabile dell'Area Sanità in Lombardia Informatica, che illustrà la situazione in Lombardia ed i progetti in corso;
- Matteo Mascarini, Responsabile dell'UGID (Ufficio Gestione Identità Digitali) presso l'Azienda Ospedaliera "Papa Giovanni XXIII", che da anni lavora per ottimizzare i numerosi aspetti connessi alla gestione delle identità virtuali in contesti complessi, e che ci parlerà di un progetto di IDM_SSO come prerequisito alla sicurezza.

14:30-15:15 - Atelier Tecnologico
"Dati aziendali strutturati e non strutturati: proteggere l'informazione e l'infrastruttura di gestione"
La quantità di informazioni necessarie per la gestione del business aziendale è in continua crescita insieme alla rilevanza ed alla criticità di queste informazioni. Al contempo diventano sempre più complessi i modelli di gestione operativa dell'infrastruttura in cui sono custoditi e differenziate le modalità di accesso.
Questa sessione è dedicata all'approfondimento di questi temi, sia per quanto riguarda i dati strutturati, memorizzati nei database e gestiti dalle applicazioni, sia per i dati non strutturati, quali ad esempio quelli trattati con gli strumenti di office, che popolano volumi e cartelle condivisi in rete.
Il tema è affrontato con i contributi di Zeropiu, che si concentra sulla sicurezza dei dati strutturati partendo da un'esperienza realizzata per un grande cliente norvegese su tecnologia Oracle Enterprise User Security, e di SafeNet che presenta alcuni possibili approcci al tema della protezione mediante cifratura della crescente quantità di dati non strutturati di valore presenti nell'infrastruttura aziendale.
Docenti: Andrea Goisis e Simone Mola

15:15-16:00 - Atelier Tecnologico
"Data Security Analitycs"
Le organizzazioni che riservano la dovuta attenzione alle problematiche legate alla sicurezza, si trovano ad essere sommerse da enormi quantità di dati da verificare che devono essere inclusi nelle strategie di Business aziendale per comprendere come la sicurezza favorisca e supporti iniziative di trasformazione innovative.
Vi è quindi l'esigenza di un nuovo approccio olistico che integri Intelligence, Security e Organizzazione aziendale sia per il trattamento di informazioni strettamente legate al business che per i dati "Security Related".

Gli analisti parlano di "Data Security Analitycs", un modello che passa attraverso azioni di

- Database Activity Monitoring
- Operational Intelligence

sia sui dati di "Business" che sui dati "Security Related".
Durante l'Atelier si intende tracciare le linee guida per la progettazione e la realizzazione di un intervento di sicurezza basato sull'analisi dei dati e sull'uso dei risultati come input per migliorare i processi di security integrandoli, a pieno titolo, nel più ampio ambito dei flussi organizzativi aziendali tradizionali.
Docenti: Gaetano Ascenzi, Paolo Capozucca, Paolo Marchei.

16:30-18:00 - Seminario a cura dell'Associazione Italiana Professionisti Security Aziendale (AIPSA)
"La security aziendale, le infrastrutture critiche con particolare attenzione al cyber-spazio".
Intervengono:

- Damiano Toselli, Presidente AIPSA e Security Manager Telecom Italia
- Mauro Masic, Vice presidente AIPSA e Security Manager Magneti Marelli
- Francesco Di Maio, Consigliere AIPSA e Security Manager di ENAV
- Corradino Corradi, Security Manager Vodafone Omnitel N.V.
- Andrea Chittaro, Security Manager Snam spa
- Claudio Pantaleo, socio AIPSA e Consulente.

16:30-18:00 - Seminario a cura del Capitolo Italiano (ISC)²
"Security Services, approccio in-house vs managed security: un'esperienza reale"
La gestione continua dell'information security consente di preservare l'integrità dei beni aziendali, garantisce la compliance con le norme vigenti, aiuta ad evitare possibili danni d'immagine oltre a consentire una concreta continuità delle attività in caso di eventi non previsti. D'altro canto un adeguato livello di sicurezza richiede il giusto mix di tecnologia, personale e processi supportato da una continua attività di intelligence che richiede competenze molto specialistiche. Il mercato attuale offre una vasta gamma di opzioni applicabili nell'adozione di soluzioni per la sicurezza dell'infrastruttura che, fondamentalmente, possono essere ricondotte alle due principali:

- adottare l'usuale modello "compra, installa, implementa e gestisci"
- optare per più innovativi modelli di security as a service che hanno rielaborato il modello di servizio dei Software as a service (SaaS).

In questo complesso panorama, un numero sempre maggiore di organizzazioni sceglie di rivolgersi ai cosiddetti "Managed security services provider (MSSP)" ovvero l'applicazione del modello SaaS (Software as a Service) nell'area dell'Information Security.
I MSSP, infatti, garantiscono la gestione e il monitoraggio delle infrastrutture di sicurezza attraverso strutture attrezzate denominate "security operations centers (SOC) anche in modalità 24x7 (modello economicamente sostenibile solo dalle aziende più grandi) e, di fatto, riducono, se non eliminano del tutto, la necessità di avere in-house risorse qualificate.
Docente: Pierluigi Sartori

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

- **Paolo Giardini e Alessio Pennasilico, che introducono la sessione e presentano i relatori**
- **Raoul Chiesa, su "E-health security: Sicurezza e sanità, matrimonio difficile"**
- **Matteo Flora, su "Social Media Security: osservare la rete per conoscere i propri problemi"**
- **Alessandro Frillici, su "Firme elettroniche e grafometriche alla luce dell'imminente Regolamento europeo".**

4. PROGRAMMA DEL 14 MARZO

09:00 Registrazione

09:30-11:00 - Sessione plenaria
Keynote Speaker: Jim Reavis, Executive Director, Cloud Security Alliance
"The Global Mandate to Secure Cloud Computing"
In this keynote presentation, Cloud Security Alliance Executive Director Jim Reavis provides insight into cloud computing trends from around the world. He will discuss new technological advances in cloud, global interdependence issues and will outline efforts to build security and trust into cloud services. He will also provide an overview of key CSA research projects and their relevance to European interests.

11:30-13:00 - Percorso professionale sulla gestione della sicurezza
"Sicurezza nei Social Media per il Made in Italy"
Alzi la mano chi non ha un account Facebook o LinkedIn. Alzi la mano chi pensa che la sua azienda non abbia intenzione di fare una pagina sui Social Media per "parlare" con i clienti. L'IT lo sa o il marketing sta andando avanti da solo? Qualcuno si è preoccupato della Sicurezza e della Privacy? In questa sessione i partner della Oracle Community for Security presentano al pubblico l'ultima delle loro pubblicazioni che sarà scaricabile dal web dopo il convegno. Il taglio è pratico, essenziale ma non banale. Il target è l'impresa italiana del Made in Italy che non può esimersi dall'usare i Social Media per competere nel mercato globale, ma non può farlo senza conoscerne i rischi e proteggersi adeguatamente.
Modera: Alessandro Vallega
Intervengono: Mauro Alovisio, Bruno Bernardi, Enrico Ferretti, Sergio Fumagalli, Francesca Gatti, Roberto Obialero, Laura Quaroni, Rosario Piazzese, Andrea Zapparoli Manzoni

11:30-13:00 - 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 Paolo Arcagni

11:30-12:15 - 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.
Davide Del Vecchio

12.15-13.00 - Atelier Tecnologico
"Verifica della sicurezza delle applicazioni e minacce del mondo mobile"
Docente: Francesco Faenzi

14:30-16:00 - Percorso professionale legale
"Mobile forensics, acquisizione e analisi forense di tablet, cellulari e smartphone"
Questa sessione si solgerà in due parti.
"Dalla computer forensics alla mobile forensics: gli smartphone come digital evidence"
La scena del crimine digitale è sempre più spesso ricca di evidenze mobili: cellulari, smartphone e tablet, ma anche navigatori, multimedia players, ecc. La corretta identificazione ed il repertamento diventano quindi fasi fondamentali per la preservazione della fonte di prova.
Facciamo il punto della situazione sul trattamento del reperto "mobile" introducendo le best practise nelle tecniche di isolamento ed acquisizione e vediamo sul campo l'acquisizione fisica di un device android.
Docenti: Francesco Picasso e Marco Scarito.
"Mobile Forensics: dove i software commerciali non arrivano"
Abstract: La Mobile Forensics è per sua natura molto più complessa della Disk Forensics, dalle maggiori difficoltà di acquisizione fisica della memoria di dispositivi spesso eterogenei tra loro alla corretta lettura del file system in uso e dei dati che, spesso, sono proprietari e poco documentati. Gli strumenti commerciali vengono in aiuto alle esigenze dell'analista che, basandosi sulle specifiche tecniche rilasciate dal vendor, si fida spesso ciecamente dell'output ottenuto dal software usato. Durante l'intervento verrà affrontato il complesso problema degli automatismi nelle operazioni di estrapolazione di dati di interesse dalle memorie di smartphone, illustrando casi pratici dove i software commerciali danno esiti piuttosto difformi da quelli che emergono con analisi manuali o ad hoc tramite strumenti open source.
Docenti: Paolo Dal Checco e Stefano Fratepietro.

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

14:30-16:00 - Percorso professionale legale
"CLOUD: profili legali e contrattuali"
I servizi cloud pongono una serie di problemi legali e contrattuali che sono stati affrontati anche dal Garante per la protezione dei dati personali e dall'Article 29 Data Protection Working Party. Durante il seminario verranno quindi da un lato affrontate e commentate la maggiori criticità e peculiarità dei contratti di servizi cloud sotto un profilo civilistico e dall'altro illustrate le tutele da prevedere sul piano del trattamento dati personali.
Docente: Gabriele Faggioli

16:30-18:00 - Seminario a cura della Cloud Security Alliance e del suo Capitolo Italiano.
Una Tavola Rotonda organizzata da CSA e CSA Italy con il patrocinio di AFCEA (Armed Forces Communications and Electronics Association)
"Cloud Security for Defence"
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: Gaetano Di Blasio, co-founder e Vice President di Reportec
Partecipano:

- **Jim Reavis, Executive Director di Cloud Security Alliance (CSA)**
- **Gen. Pietro Finocchio, Presidente di AFCEA Capitolo di Roma e Executive Committee Member di AFCEA International**
- **Paolo Campobasso, Finmeccanica Senior Vice President Group e Chief Security Officer**
- **Fabrizio Baiardi, Presidente del corso di laurea magistrale in sicurezza informatica, Università di Pisa**
- **Leandro Aglieri, Presidente Rete di Imprese Cloud4Defence**
- **Enzo Bagnacani, Responsabile in Telecom Italia dello sviluppo delle soluzioni IT Infrastrutturali, Cloud e Tradizionali**
- **Stefano Mele, Coordinatore dell'Osservatorio "InfoWarfare e Tecnologie emergenti" dell'Istituto Italiano di Studi Strategici "Nicolò Machiavelli"**
- **Valerio Vertua, Direttore Area di Ricerca "Legal & Privacy in the Cloud" di CSA Italy**
- **Marco Bavazzano, Consiglio Direttivo ASIS Italia.**

16:30-18:00 - Seminario a cura dell'Associazione Italiana Information Systems Auditors (AIEA)
Sono previsti due interventi.

"COBIT 5 for Info Security in pratica (Self Assessment usando ISO 15504)"
Abstract: una realtà multinazionale vuole misurare in modo omogeneo il livello di IT Security e Compliance di varie realtà locali (spesso PMI) per individuare, pianificare e coordinare interventi correttivi, centrali o periferici, secondo le 7 dimensioni (COBIT5 enablers):

- **Principi e Policy,**
- **Strutture organizzative,**
- **Cultura e comportamenti,**
- **Skills e competenze,**
- **Servizi, infrastrutture ed applicativi per la sicurezza,**
- **Informazioni,**
- **Processi IT**

Verrà sinteticamente presentato e discusso come COBIT5 possa aiutare a individuare gli interlocutori, definire le domande da porre ed elaborare i risultati.
Docente: Alberto Piamonte

"Strumenti metodologici per l'Infosecurity: come far rendere al meglio ciò che abbiamo già pagato!"
Partendo da alcuni casi reali, l'intervento ha l'obiettivo di fornire degli spunti di riflessione pragmatici per capire come strumenti metodologici integrati possano contribuire al processo di efficientamento complessivo delle organizzazioni, anche in contesti di mercato molto difficili come l'attuale che tendono a non far percepire il valore aggiunto di questi approcci/best practices.
Docente: Fabrizio Cirilli.

16:30-18:00 - Seminario a cura dell'Associazione Utilizzatori Sistemi E tecnologie Dell'informazione (AUSED)
"Aggiornamento su Privacy e novità in tema di cybersecurity dall'Europa"
L' intervento verterà sull'analisi di due temi oggetto di ampio dibattito in Europa.
In primo luogo fornirà un aggiornamento sul dibattito in corso al Parlamento europeo sulla proposta di regolamento e sulla revisione della Direttiva 95/46/CE in merito alla protezione dei dati personali. L'obiettivo è di fornire informazioni di prima mano sull'orientamento del Parlamento e degli Stati membri con particolare enfasi sugli aspetti con un potenziale impatto sul settore ICT e sull'innovazione.
In secondo luogo affronterà la tematica del cybersecurity alla luce della recente proposta di direttiva sulla sicurezza delle reti informatiche e le novità introdotte circa l'adozione di misure per la gestione dei rischi e di notifica degli incidenti gravi a livello di sicurezza da parte degli operatori di infrastrutture critiche.
Intervengono: Claudia La Donna, Alberto Savoldelli e Massimo Turchetto

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 31 marzo, 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 di uno stesso Percorso Professionale (Tecnico, Legale o sulla Gestione della Sicurezza) sarà rilasciato un Diploma. Il diploma sarà inviato per email a chi ne farà richiesta a info@clusit.it.

6. HACKING FILM FESTIVAL

Al termine delle due prime giornate del Summit, martedì 12 e mercoledì 13, dalle 18.15 alle 20.15 si terrà la quinta edizione milanese dell'Hacking Film Festival. L'evento culturale "satellite" del Security Summit, sarà come sempre dedicato a dei filmati sul tema dell'hacking e della (in)sicurezza, che serviranno poi di pretesto per un dibattito moderato da Alessio Pennasilico, Cristiano Cafferata, Giovanni Ziccardi e Raoul Chiesa. Tra gli ospiti delle due serate è confermata la presenza del filosofo Lele Rozza.

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 necessario iscriversi inviando una mail a info@clusit.it, precisando se ci si iscrive ad entrambe le serate o a quale delle due.

Al termime, gli spettatori sono invitati a partecipare ad un rinfresco-aperitivo.

12 Marzo 2013 - Ore 18:15 - 20:15

Durante la prima serata saranno proiettati tre brevi filmati.

Il primo è 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.

Il secondo è un filmato realizzato da Matteo Viviani delle Iene, sulla possibilità di recuperare i dati che un utente ha cancellato sul proprio cellulare.

Il terzo è un documentario sugli Hackers realizzato dal National Geografic Channel.

13 Marzo 2013 - Ore 18:15 - 20.15

Nella seconda serata proietteremo il film "23", che tratteggia la storia dell'hacker tedesco Karl Koch, morto in circostanze misteriose nel 1989. Attorno al suo nick "Hagbard" si intersecano numerose vicende: le attività del Chaos Computer Club, la più importante organizzazione europa in tema di hacking, i rapporti delicati tra hacker e criminalità, il fascino della Trilogia degli Illuminati e delle cospirazioni, i contatti con il KGB e le indagini nate negli USA per il furto d'informazioni in sistemi militari. Nonostante il film sia stato molto criticato da amici e parenti più stretti del giovane hacker, il quadro che fornisce è suggestivo e importante testimonianza di un'epoca.

7. GLI SPONSOR DEL SECURITY SUMMIT 2013

Partner

Platinum

Gold

Silver

Hacking Film Festival

Premio Tesi

All'interno dell'Atahotel Executive 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