SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Indice

1. PRESENTAZIONE

Dal 18 al 20 marzo si terrà a Milano la sesta 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/milano-2014/registrazione-eventi.

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

2. PROGRAMMA DEL 18 MARZO

09:00 Registrazione

09:30-11:00 - Sala Rubino- Sessione plenaria

I lavori del Security Summit 2014 saranno aperti da un dirigente dell'Unità Trust and Security, European Commission - DG for Communications Networks, Content and Technology (CONNECT)

"Fostering trust and security in the European Union"

Securing network and information systems in the EU is essential to ensure prosperity and to keep the online economy running. The European Union has been working on a number of fronts to ensure cybersecurity in Europe, from providing the delivery of better internet for kids to implementing the international cooperation on cybersecurity and cybercrime.

The European Union's Digital Agenda sees Internet trust and security as vital to a vibrant digital society, and sets out 14 actions to improve cybersecurity readiness. These include the establishment of a well-functioning network of CERTs (Computer Emergency Response Teams) at national level covering all of Europe; the organisation of cyber-incidents simulations and the support to EU-wide cybersecurity preparedness. Moreover, the policy on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital ICT infrastructure by stimulating and supporting the development of a high level of preparedness, security and resilience capabilities, both at national and at EU level.

The Cybersecurity Strategy for the European Union and the Commission proposal for a Directive on Network and Information Security put forward legal measures and give incentives aiming at making the EU's online environment the most secure in the world. By strengthening preparedness, cross-border cooperation and information exchange, the proposed Directive enables citizens to reap the full benefits the digital environment offers. Moreover, it allows the public and private sector to trust digital networks' services at national and EU level. By setting incentives to foster investments, transparency and user awareness, the strategy will boost competitiveness, growth and jobs in the EU. As network and information systems are globally interconnected, cybersecurity has a global dimension too. The strategy addresses international cooperation as a key priority. Overall, this strategy and legislative proposal will help Europe put its own house in order and increase its international bearing.

These activities on network and information security are supported by the European Network and Information Security Agency, as well as by the Computer Emergency Response Team for the EU institutions (CERT-EU).

11:30-13:00 - Sala Zaffiro - Percorso Professionale sulla Gestione della Sicurezza

"Quando il CIO scende in fabbrica: strategie di protezione ed esempi pratici

Troppo spesso ottimi prodotti per l'automazione industriale vengono messi in crisi da installazioni non adeguate. Per questa ragione sempre più spesso, ove possibile, si stanno eliminando i PC compatibili infilati sotto ad un tavolo ed assemblati dall'installatore a favore di desktop virtuali per garantire resilienza del servizio, la possibilità di fare backup e di utilizzare device più resistenti in fabbrica.

Le necessità di partenza di sicurezza non mutano, ma l'introduzione di tecnologie diverse modificano lo scenario.

Proteggersi da infezioni ed attacchi resta una priorità. Cercheremo di capire di cosa dovrebbe preoccuparsi il CIO diligente, e quale strategia potrebbe discutere assieme al Direttore di fabbrica…

Docenti: Alessio Pennasilico e Maurizio Martinozzi

11:30-13:00 - Sala Rubino - Percorso Professionale Tecnico

"Soluzioni Anti-DDoS"

Gli attacchi informatici sono portati sotto varie forme, modalità e dimensioni e stanno divenendo sempre più una criticità per le grandi aziende ed organizzazioni. Di particolare gravità è il numero crescente di attacchi di tipo Distributed Denial of Services (DDoS), contro i quali le difese perimetrali tradizionali non sono più sufficienti. Diventa quindi necessario ripensare il modello di protezione ed adottare nuove tecnologie in grado di mitigare questo tipo di attacchi assieme alla capacità di integrarle all'interno dei processi di monitoraggio e gestione degli incidenti aziendali.

Docenti: Samuele Battistoni, Rodolfo D'Agostino e Andrea Zapparoli Manzoni

11.30-12.15 - Sala Granato - 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

12.15-13.00 - Sala Granato - Atelier Tecnologico

"Il contributo dei sistemi di Identity nella mitigazione del rischio legato all'esternalizzazione di servizi"

I sistemi di Identity Management hanno modificato radicalmente il loro ruolo all'interno dei processi aziendali. Sono infatti passati dall'essere considerati mere piattaforme tecnologiche nelle mani di strutture IT specialistiche al diventare strumenti consultati periodicamente da strutture di business e di auditing con l'obiettivo di implementare una efficace politica di data governance.

Questo è stato dovuto principalmente a due fattori: la discontinuità tecnologica in atto (es. Cloud, Mobile, Social) e le normative specifiche emesse dalle Autorità relativamente al controllare responsabilmente l'accesso ai dati. Tale esigenza di controllo viene ulteriormente esasperata dai nuovi modelli di business orientati all'esternalizzazione di processi anche critici nell'ottica dell'efficienza operativa e del controllo dei costi. In questi nuovi scenari i sistemi di Identity Management offrono un ausilio fondamentale nel mantenimento dell'accountability sui dati riducendo in allo stesso tempo il rischio operativo legato a tali operazioni, quindi non limitandosi più alla sola dimensione aziendale ma anche a scenari di federazione tra entità diverse che operano nella stessa catena del valore.

Docenti: Andrea Buzzi e Stefano Vaglietti

14:30-16:00 - Sala Rubino - Tavola Rotonda

"Presentazione del RAPPORTO CLUSIT 2014"

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.

Modera: Gigi Tagliapietra, Presidente Clusit

Partecipano:

- alcuni autori del Rapporto Clusit 2014
- Andrea Carmignani, IBM Sales Manager, Responsabile della linea di servizi Enterprise Security per l'Italia
- Domenico Garbarino, Oracle Italia Sales Director Security Solutions
- Gastone Nencini, Trend Micro Italy Country Manager
- Federico Santi, HP Enterprise Security Services, Client Principal Southern Europe

14:30-16:00 - Sala Zaffiro - 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, legale, Consiglio direttivo CLUSIT, Adjunct Professor MIP-Politecnico di Milano, membro del Gruppo di Esperti di contratti di cloud computing della Commissione Europea.

14.30-15.15 - Sala Granato - Atelier Tecnologico

"Data Security Governance: come conciliare esigenze tecniche, obiettivi di business e vincoli di budget."

Nel contesto attuale l'incremento del volume dei dati gestiti dalle aziende e il diversificarsi dei canali a disposizione per accedervi (da remoto, social network, tramite tablet o smartphone) hanno creato nuove e interessanti opportunità di business, ma allo stesso tempo hanno generato una crescita delle minacce ai requisiti di confidenzialità, integrità e disponibilità delle informazioni.

In tale contesto, Protiviti presenta il proprio approccio alla definizione di un modello strutturato di gestione delle informazioni, volto ad identificare le misure di protezione necessarie a mitigare il rischio di data breach e a gestire gli eventi critici anche nel rispetto delle normative e degli standard emergenti.

Zeropiu presenta un metodo, messo a punto con Oracle Italia, per rilevare lo stato della sicurezza delle basi di dati aziendali ed individuare le priorità d'azione. Saipem, primaria realtà del gruppo Eni, porterà la propria esperienza di applicazione di questo metodo ed una analisi del contributo che ha dato alla strategia aziendale di sicurezza delle informazioni.

Relatori: Andrea Gaglietto, Andrea Goisis e Luca Mazzocchi

15.15-16.00 - Sala Granato - Atelier Tecnologico

"Chi possiede i miei dati e come li protegge? - Identity Management, Personal Data Ownership e Data Breach Prevention Strategy"

Il Regolamento UE sulla violazione dei dati e le nascenti iniziative nazionali ed europee (in Italia l'istituzione dello SPID) stanno definendo

ruoli e le responsabilità nella gestione delle identità digitali e dei dati personali.

Lo scenario di cambiamento rende indispensabile mitigare le minacce. La violazione dei dati, intesa in generale come evento che comporta la compromissione di informazioni rilevanti ai fini di un qualsivoglia tipo di business, riscuote ormai notevole attenzione nell'ambito della sicurezza cibernetica; nell'Atelier si approfondiranno gli scenari attuali e futuri dal punto di vista normativo e tecnologico.

Relatori: Riccardo Canetta e Fabrizio Leoni

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

"La sicurezza della Banca 2.0: scenari, minacce e soluzioni per Home Banking, Mobile e Social".

La rapida evoluzione della Banca, che sempre più affida il proprio front-end a piattaforme digitali in una logica di multicanalità (Web, Mobile e Social), presenta una serie di innegabili vantaggi sia per gli Istituti che per gli utenti finali. In questo scenario emergono però anche una serie importante di problematiche di Security (in senso esteso), che vanno dalla protezione contro gli 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. 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 - Sala Zaffiro - Seminario a cura dell'OWASP Italy Chapter

Sono previsti 3 interventi

- 1° Intervento - "HTTP(S)-Based Clustering for Assisted Cybercrime Investigations"

Negli ultimi anni c'è stato un sensibile aumento del numero di attacchi mirati (APTs). Questo è visto dagli esperti di sicurezza come uno spostamento da un mondo dominato da malware diffuso che infetta indiscriminatamente, ad un approccio più mirato selettivamente con maggiore guadagno. In questo discorso, si introduce un nuovo sistema denominato SPuNge che elabora le informazioni sulle minacce raccolte dalla parte degli utenti per rilevare potenziali attacchi mirati per ulteriori indagini. Noi usiamo una combinazione di clustering e tecniche di correlazione per individuare gruppi di macchine che condividono un comportamento simile rispetto alle risorse dannose che accedono e al settore in cui operano. La nostra valutazione e oltre 20 milioni di installazioni mostrano che SPuNge funziona bene in pratica ed è utile per aiutare gli analisti della sicurezza nelle indagini di criminalità informatica.

Docente: Marco Balduzzi

- 2° Intervento - "Android Apps permissions model (in)security"

I dispositivi Android, nonchè le applicazioni per essi sviluppate, stanno crescendo in modo esponenziale e di conseguenza aumentano i dati personali che gli utenti conservano su tali dispositivi. Android ha fatto del

modello a "permessi" una bandiera della sicurezza del proprio sistema operativo. Quanto però questo modello risulta essere realmente sicuro? Può un'applicazione che non richiede alcun permesso comunicare accedere a dati sensibili ed inviarli ad un handler remoto? Ci si focalizzerà sulla gestione della sicurezza su Android e su come tale modello possa essere in parte bypassato. Verrà quindi mostrato un esempio di applicazione, apparentemente innocua, in grado però di sottrarre alcuni dati presenti sulla memoria.

Docente: Davide Danelon

- 3° Intervento - "Io faccio application security, e tu?"

L'application security è una professione ancora misteriosa, almeno qui in Italia. In questo talk ti racconto i miei ultimi 10 anni di carriera, tra errori e successi e ti spiego perché anche tu nella tua realtà, hai bisogno di fare application security. Oggi non parliamo di quali siano le vulnerabilità più pericolose ma parleremo dell'importanza di introdurre in azienda la cultura della sicurezza nel rilascio e della gestione del software, per evitare di trovarsi col sito defacciato.

Docente: Paolo Perego

16:30-18:00 - Sala Granato - Tavola Rotonda

Premio "Innovare la sicurezza delle informazioni" - 9a edizione

Clusit procederà alla presentazione e premiazione delle migliori tesi universitarie del 2013.

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
- gli studenti premiati, che presenteranno le proprie tesi
- Fabrizio Sensibile, @ Mediaservice.net
- Davide Varesano, eMaze
- Viviana Rosa, BSI Group Italia.

-

3. PROGRAMMA DEL 19 MARZO

09:00 Registrazione

09:30-11:00 - Sala Rubino - Sessione plenaria

In apertura della seconda giornata è prevista una tavola rotonda dal titolo "Security By Design? Il CIO visto con gli occhiali del Project Manager", che intende approfondire il concetto di Security by Design, ovvero del progettare prodotti e servizi informatici pensando alla sicurezza fin dal principio. Secondo gli esperti questo è l'unico modo per rendere possibile una ragionevole iniziativa di contrasto alla criminalità, alle frodi e agli errori che funestano i sistemi informativi. Il dibattito sarà tenuto dall'associazione di riferimento per il Project Management, il PMI (Project Management Institute) tramite i suoi rappresentanti del capitolo Northern Italy.

Partecipano:

- **Walter Ginevri, Presidente del capitolo Northern Italy del PMI e coautore del Focus On "Security By Design" del Rapporto Clusit 2014**
- **Luca Bechelli, CD e Comitato Tecnico Scientifico Clusit**
- **Pierluighi Sartori, Chief Security Officer in Informatica Trentina**
- **Alessandro Vallega, CD Clusit e coautore del Focus On "Security By Design" del Rapporto Clusit 2014.**

11:30-13:00 - Sala Rubino - Percorso Professionale sulla Gestione della Sicurezza

"Parliamo delle frodi del 2020. E di altro."

I due temi, quello della frode e quello della sicurezza, si intersecano in più punti, ma come ben sanno gli addetti ai lavori sono ben lontani dal sovrapporsi completamente. La Oracle Community for Security, dedica questo appuntamento annuale a presentare la sua ultima pubblicazione "Le Frodi nella Rete" (che sarà disponibile dopo la presentazione qui: c4s.clusit.it insieme alle sei precedenti) proprio su questo tema. Lo faremo in una nutrita e dinamica tavola rotonda dove gli esperti di sicurezza e di frodi del gruppo di lavoro racconteranno la loro esperienza e spiegheranno il loro punto di vista. Parliamo di tecnologia ICT usata dai buoni (per il contrasto), dai cattivi (per frodare) e dagli inconsapevoli (che non chiudono le finestre), e quindi di frodi, reati, sicurezza, insicurezza, contromisure e organizzazione. In generale e nelle industry: telecomunicazioni, banche, assicurazioni, gaming, settore pubblico e sanità. Pagamenti online, mobile, carte, proprietà intellettuale e contraffazione... Un appuntamento da non perdere!

Modera: Alessandro Vallega

Partecipano: Riccardo Abeti, Orlando Arena, Luca Bechelli, Giancarlo Butti, Elisabetta Calmasini, Paolo Carcano, Enrico Ferretti, Sergio Fumagalli, Luca Lora Lamia , Simone Maga, Paola Meroni, Mario Monitillo, Nicola Murano, Roberto Obialero, Maurizio Pastore, Claudio Telmon, Enrico Toso.

11:30-13:00 - Sala Zaffiro - 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, Andrea Boggio

11.30-12.15 - Sala Granato - 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.

Vi aspettiamo!

Docente: Maurizio Martinozzi

12.15-13.00 - Sala Granato - Atelier Tecnologico

"Sicurezza delle applicazioni"

Nell'era del system of engagement, dispositivi mobili e smarter phones, vanno a sostituire i desktop.I dipendenti preferiscono sempre più spesso utilizzare dispositivi mobili anche in ufficio e di conseguenza le aziende tendono ad adottare modelli BYOD. Questo fa si che il dipendente abbia sul proprio dispositivo applicazioni aziendali e personali. Gestire la sicurezza delle applicazioni diventa pertanto fondamentale per salvaguardare gli interessi aziendali ma anche quelli personali.

Docente : Salvatore Sollami

14:30-16:00 - Sala Rubino - Percorso Professionale Legale

"La sicurezza dei dati e la privacy nelle recenti evoluzioni normative comunitarie e nazionali."

La costante attività del Garante Privacy e l'emanando Regolamento UE sulla protezione dei dati meritano diverse riflessioni sulla compliance normativa in tema di sicurezza dei dati e privacy.

Nel corso degli ultimi mesi, infatti, il quadro è sensibilmente mutato: dall'obbligo di notifica in caso di sottrazione di dati alle regole in caso di marketing diretto alle misure di sicurezza in caso di intercettazioni. A queste, inoltre, bisogna aggiungere i temi attualmente in discussione in sede europea che riguardano la controversa figura del privacy officer, la privacy e security by design e la privacy e security by default.

Nel corso del seminario verranno analizzati i recenti Provvedimenti dell'Autorità Garante sulle tematiche sopra enucleate e si darà un quadro aggiornato sulle evoluzioni normative attualmente in discussione a Bruxelles e i possibili contrasti che tale normativa potrebbe generare tenuto conto del quadro giuridico attuale del nostro Paese.

Docente: Pierluigi Perri

14.30-15.15 - Sala Zaffiro - 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: Alessio Pennasilico, Angelo Giovannardi, Elena Esposito (Westhouse Italia)

14.30-15.15 - Sala Granato - Atelier Tecnologico

"Sistemi IT insicuri? No grazie… come migliorare la sicurezza di applicazioni Web e sistemi ERP"

Un valore sempre più significativo di dati ed informazioni per gli aspetti strategici, decisionali e di comunicazione, minacce sempre più pericolose e strutturate, nuovi modelli di business e normative richiedono alle organizzazioni un continuo processo di miglioramento dei livelli di sicurezza. Questo impegno è strettamente correlato al controllo ed alla governance delle applicazioni software in tutte le fasi del loro ciclo di vita.

In tal senso, i due interventi dell'atelier evidenzieranno in maniera efficace e pragmatica quali siano le carenze culturali e gli elementi di sicurezza a cui prestare attenzione sin dalle prime fasi evolutive dei sistemi IT, con l'obiettivo di prevenire attacchi informatici, usi impropri o illeciti. In particolare le indicazioni si focalizzeranno sia sugli interventi di carattere organizzativo e tecnologico nel processo di sviluppo SSDLC delle applicazioni web, presentando un caso utente virtuoso di una PA, che sulla corretta configurazione e gestione dei sistemi aziendali più complessi (sistemi ERP), illustrando approcci metodologici, strumenti, in grado di prevenire e correggere le criticità più rilevanti (ma purtroppo più comuni, come sarà dimostrato attraverso l'esposizione di dati statistici reali), provando a rispondere alle seguenti domande:

- Quali interventi adottare, prima di mettere online un'applicazione, per contrastare le minacce e prevenire gli attacchi informatici?

- Come controllare e gestire l'accesso alle applicazioni "online" e ai dati aziendali gestiti negli ERP?

Docenti: Fabio Bucciarelli, Roberto Obialero e Pasquale Vinci

15.15-16.00 - Sala Zaffiro _ Atelier Tecnologico

"Benefici derivanti dall'utilizzo di una metodologia nella formazione del personale che si occupa di sicurezza"

Le esigenze professionali, di chi opera o vorrebbe operare, nel campo della sicurezza IT non sempre sono allineate con i contenuti formativi dei corsi di formazione aziendale. Per anni la formazione in questo settore si è basata su esigenze legate a prodotti o su interpretazioni soggettive dei fondamentali. Nel seminario vedremo come adottare un metodo di lavoro condiviso tra i vari settori della sicurezza che, oltre a portare benefici prettamente operativi, presenta vantaggi legati alla formazione, quali ad esempio percorsi formativi progressivi e condivisione della percezione di sicurezza.

Docente: Fabrizio Sensibile

15.15-16.00 - Sala Granato - Atelier Tecnologico

"Dalla mobile security alla gestione dell'identità digitale."

Il tema della sicurezza sui dispositivi mobili non è più un fenomeno marginale, ma è diventato un problema di prim'ordine esattamente come lo è la sicurezza nelle nostre case o la sicurezza della nostra persona. Esiste una consapevolezza crescente da parte dei professionisti, che in pochi mesi ha profondamente cambiato il mercato: si è passati da un "mercato di offerta", che ha visto i principali attori investire tempo e risorse per portare il tema della sicurezza al giusto livello di attenzione dei decisori, ad un "mercato di domanda" che così si è evoluto grazie alla consapevolezza dei rischi ed all'urgenza di trovare velocemente soluzioni adeguate per le aziende. L'evoluzione delle soluzioni ha poi fatto sì che il concetto stesso di sicurezza per gli apparati mobili, passasse da un ambito limitato alla sicurezza del

dispositivo ad un ambito molto più vasto di gestione complessiva dell'informazione digitale che "transita" sul dispositivo mobile; evolvendo contemporaneamente così dal noto acronimo MDM (Mobile Device Mamangement) al meno usato MSM (Mobile Security Management). E' naturale allora pensare come dalla sicurezza delle informazioni (che rappresenta oggi lo stato dell'arte) si possa (e si debba) a breve passare al concetto di gestione dell'identità digitale, in un mondo (quello tecnologico) che ha ormai superato definitivamente i propri confini fisici.

Docenti: Angelo Bosis e Paolo Capozucca

16:30-18:00 - Sala Rubino - Seminario a cura dell'Associazione Italiana Professionisti Security Aziendale (AIPSA)

16:30-18:00 - Sala Granato - Seminario a cura del Capitolo Italiano (ISC)²

Sono previsti due interventi

Primo intervento - "CMS Hacking"

I CMS sono largamente diffusi poichè consentono di realizzare siti funzionali e sexy in tempi brevi e con costi contenuti. Gabriele Buratti propone un'analisi delle vulnerabilità intrinseche nell'utilizzo di codice di terze parti quale un CMS, dei modi in cui queste vengono sfruttate dai malintenzionati per attacchi su larga scala e di come un Web Application Firewall possa essere un valido strumento per fare Virtual Patching.

Docente: Gabriele Buratti

Secondo intervento - "L'information Security è sotto controllo? Investigare la qualità nella gestione dell'Information Security"

Gli studi e le analisi condotte si sono sempre concentrate sull' utilizzo da parte delle organizzazioni dei controlli applicati alla gestione della sicurezza delle informazioni concentrandosi sulla presenza o assenza di controlli, tralasciando la loro qualità. L'obiettivo è concentrarsi sul controllo della qualità, che varia notevolmente in base alle dimensioni dell'organizzazione e del settore industria, spostando il focus dell'aspetto tecnico che da solo si è rivelato poco economico e con una visione errata di tipo down-top.

Docente: Roberto Periale

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

Agenda

16.30 Andrea Violetti - "Certificazione delle competenze: la norma Uni 11506 e i nuovi riferimenti legislativi sulle professioni"

17.00 Alessandro Frillici - "Colpa in eligendo: le competenze a supporto della responsabilità amministrativa delle persone giuridiche (ex Dlgs 231/01)"

17.30 Alessio Pennasilico - "ICT security manager, ICT security specialist: due figure professionali di rilievo per la sicurezza informatica"

18.00 Franco Fontana - "La certificazione delle persone secondo lo standard Uni Cei En Iso/Iec 17024"

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.

4. PROGRAMMA DEL 20 MARZO

09:00 Registrazione

09:30-11:00 - Sala Rubino- Sessione plenaria

Aprirà i lavori della terza giornata Stefano Quintarelli, socio fondatore di Clusit e Parlamentare, che affronterà un tema delicato e di grande attualità: il "Datagate", scandalo globale per i programmi di intercettazione della National security agency (Nsa) statunitense svelati da Edward Snowden, a seguito del quale l'amministrazione Obama si appresta a varare una riforma per limitare l'azione della Nsa. La riforma divide i membri del Congresso, tra chi teme rischi per la lotta al terrorismo e chi invece considera l'azione dell'intelligence finita in parte fuori controllo.

11:30-13:00 - Sala Rubino - Tavola Rotonda

"Information Security Management in Italia. What's next"

Una tavola rotonda sul tema dell'Information Security Management, durante la quale verranno presentati i principali risultati dell'ultima survey condotta da NEXTVALUE su un panel qualificato di oltre 100 CIO e Direttori IT delle più grandi imprese italiane, sulla necessità di affrontare le nuove problematiche in ambito di sicurezza, di compliance e di governance.

Chairman: Alfredo Gatti, CIOnet Italia, Nextvalue

Partecipano: oltre a Mauro Cicognini, membro del direttivo e del CTS Clusit, i CSO e CISO di alcune grandi aziende italiane.

11:30-12:15 - Sala Zaffiro - Atelier Tecnologico

"Sourcefire, security for the real world"

Docenti: Fabio Panada e Stefano Volpi

11.30-12.15 - Sala Granato - 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

12.15-13.00 - Sala Zaffiro - 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: Andrea Boggio

12.15-13.00 - Sala Granato - Atelier Tecnologico

"Architetture orientate alla disponibilità dell'informazione"

La corretta progettazione di una infrastruttura orientata alla disponibilità dell'informazione è presupposto indispensabile per l'erogazione dei servizi e la corretta gestione dei processi di sicurezza.

Per garantire i livelli di servizio stabiliti è necessario valutare i rischi connessi ai disturbi che gli attacchi odierni rappresentano, per la stabilità delle architetture IT.

Le soluzioni Radware sono progettare per garantire i livelli di disponibiltà in ogni condizione di esercizio, garantendo gli SLA e il controllo degli eventi che possono produrre impatti su servizi e infrastruttura

Docente: Alessandro Tagliarino

14:30-16:00 - Sala Zaffiro - 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 :)

Docenti: Alessio Pennasilico e Cristiano Cafferata

14:30-16:00 - Sala Rubino - Percorso Professionale Legale

"Mobile Forensics e Cloud Forensics: tecniche di acquisizione e case study"

Nel campo della mobile forensics, si è vista negli ultimi anni una proliferazione di strumenti ad alto e basso costo, per operare attività di analisi ed estrazione dati dai cellulari. Come già accennato in interventi passati, l'Open Source sta muovendo i primi passi verso software di interfacciamento e di analisi dei dispositivi mobili. La distribuzione forense DEFT, in particolare, sta cercando di raccogliere ciò che è al momento disponibile per fornire agli investigatori un "contenitore" di

strumenti dedicati al mondo della mobile forensics. La prima parte della sessione verterà sulla presentazione degli strumenti e delle metodologie utilizzabili tramite il sistema DEFT per operare alcuni particolari tipi di acquisizione dati e analisi dei principali sistemi operativi presenti nel mondo degli smartphone.

Analogamente con la migrazione massiva dei dati verso i servizi Cloud, oggi la Digital Forensics deve affrontare nuove sfide e proporre soluzioni innovative. Durante la seconda parte della sessione saranno illustrate le tecniche più attuali, con metodi e strumenti pratici, per acquisizioni di pagine web, account di posta elettronica (Gmail, Hotmail, Yahoo), profili Facebook e servizi Cloud (Amazon S3, Google Drive, Dropbox, SkyDrive) attraverso l'utilizzo delle principali soluzione commerciali e open.

La sessione si concluderà con un case study sulla gestione di un incidente di spionaggio industriale su Cloud e Mobile. L'intervento illustrerà un caso realmente affrontato, ovviamente riadattato e anonimizzato, di sospetto spionaggio industriale. Si mostrerà come, dall'analisi di uno smartphone e di un tablet, sia possibile ricostruire lo scambio di file riservati attraverso sistemi di cloud storage.

Docenti: Paolo Dal Checco, Mattia Epifani e Marco Scarito

14.30-15.15 - Sala Granato - Atelier Tecnologico

"Le nuove norme della famiglia 27000"

A ottobre 2013 sono uscite le nuove versioni della ISO/IEC 27001 e 27002, pietre miliari per la gestione della sicurezza delle informazioni. Gli esperti di UNINFO che hanno partecipato ai lavori vi racconteranno da una prospettiva unica cosa, come e perché è cambiato in queste nuove norme e come si sta evolvendo lo scenario delle norme internazionali relative alla sicurezza delle informazioni.

Docenti: Cesare Gallotti e Fabio Guasconi

15.15-16.00 - Sala Granato - Atelier Tecnologico

"La sicurezza nel mondo delle API"

La ridefinizione del modo in cui i sistemi informativi vengono progettati con le Application Programming Interfaces permette di sfruttare pienamente le grandi e moderne innovazioni, prima tra le quali la consumerizzazione. Internet come la conosciamo con i suoi portali, i siti web e le pagine non esiterà più. Avremo una internet basata sulle apps, i widget e gli store pubblici e aziendali e le aziende potranno realizzare dei nuovi servizi e prodotti oppure lasciare che terzi usino le loro API per creare delle nuove applicazioni e arricchire il proprio business.

Da un punto di vista della sicurezza come si accompagna questa trasformazione?

Docenti: Nino Guarnacci e Paola Marino

16:30-18:00 - Sala Rubino - Percorso Professionale Tecnico

"Democrazia e controllo massivo nell'era post-Datagate"

Le rivelazioni di Snowden hanno tracciato il confine con una nuova era nel mondo dell'intelligence e delle cyber operations.

Questo intervento cercherà di fare chiarezza sul c.d. "Datagate affair" ed analizzerà i recenti avvenimenti di Kiev e di Caracas, per focalizzarsi poi sul concetto di democrazia e controllo massivo delle informazioni nel XXI secolo.

Docente: Raoul Chiesa

16:30-18:00 - Sala Zaffiro - Seminario a cura dell'Associazione Italiana Information Systems Auditors (AIEA)

Sono previste due relazioni.

1a relazione - "15° aggiornamento Circ. n. 263 Bankit: COBIT5® per pianificare ed implementare"

Il 2 luglio 2013 Banca d'Italia ha emanato in via definitiva il 15° aggiornamento della Circolare n. 263 del 26 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" in materia di controlli interni, sistema informativo e continuità operativa delle banche e dei gruppi bancari.

Il Framework COBIT5® ha le caratteristiche che ne suggeriscono l'utilizzo sia per pianificare che per implementare le attività legate alle nuove disposizioni:

• fornire una guida autorevole ed universalmente accettata per la valutazione della reale capacità dei processi, l'individuazione delle carenze (gap) e l'implementazione delle eventuali azioni correttive;

• dare uno schema di riferimento generalizzato, allineato con i principali standards, in grado di fornire una semplice architettura che porti alla realizzazione di soluzioni coerenti ed integrate (contrapposte ad un approccio che preveda varie iniziative scollegate), evitando disallineamenti e duplicazioni anche rispetto ad altre iniziative non direttamente collegate alla direttiva;

• provvedere, per quanto riguarda l'IT, una guida alla comprensione ed implementazione delle funzioni di Governance a Management richieste da BI.

In quest'ambito AIEA ha sviluppato un approccio metodologico originale di COBIT5® Implementation, estendibile a problematiche analoghe, mettendo anche a punto alcuni strumenti di lavoro.

Verranno quindi presentati:

• Metodologia in generale

• Sintesi dei risultati della ricerca

• Considerazioni sui requisiti minimi per l'adozione della metodologia (conoscenze e tempi) e delle iniziative di AIEA rivolte a soddisfarli (Formazione, Workshop tematici, traduzioni di manuali).

Docenti: Fabrizio Bulgarelli, Alessandro Bozzoli e Alberto Piamonte

2a relazione - "La privacy nelle organizzazioni non profit"

Le organizzazioni non-profit (una realtà secondo i dati del censimento del 2011 di oltre 300.000 unità, con 4,7 milioni di volontari, 681mila dipendenti, 270mila lavoratori esterni e 5mila lavoratori temporanei) non godono di particolari privilegi per quanto attiene il rispetto della

normativa privacy e pertanto devono mettere in atto tutti gli adempimenti previsti dalla stessa.

Spesso tali organizzazioni trattano dati sensibili, sanitari, giudiziari, sia dei propri assistiti sia degli stessi soci (dei loro familiari) e volontari.

L'intervento ha l'obiettivo di presentare il quadro normativo nel suo complesso (normative e provvedimenti) e la sua applicabilità alle Organizzazioni non - profit, individuando quali sono le attività di natura formale (ad esempio informativa, consenso...), organizzativa (ad esempio ruoli privacy) e tecnica (ad esempio misure di sicurezza) che devono essere messe in atto per il rispetto di tali normative.

Inoltre saranno evidenziati i rischi specifici rispetto alle altre organizzazioni, quali quelli derivanti dall'uso di strumenti e spazi promiscui (con altre organizzazioni, con i volontari…) o dall'uso non sempre consapevole di strumenti quali i social network (o banalmente della posta elettronica), le difficoltà di un corretto presidio, la carenza di specifica formazione, le possibili soluzioni.

Docente: Giancarlo Butti

16:30-18:00 - Sala Granato - Seminario a cura dell'Associazione Utilizzatori Sistemi E tecnologie Dell'informazione (AUSED)

"Evoluzione della Business Continuity e ruolo del Disaster Recovery negli ambienti Cloud"

L'evento cercherà di approfondire i temi della Business Continuity e del Disaster Recovery nell'era delle soluzioni mobile e Cloud attraverso gli "occhi" del BC-Manager e del ruolo che ricopre.

Avere i nostri dati nella "Struttura" e non più "on premise" rappresenta, per la mentalità corrente, un salto di qualità nel concepire i criteri di sicurezza di notevole significato.

Un po' di teoria ed una caso Utente significativo.

La strada è tracciata, la tecnologia è sempre più all'altezza e il mercato si sta riposizionando in quest'ottica.

Agenda

16:30 Introduzione a cura di AUSED

16:40 Relazione di Corradino Corradi di Vodafone e Consigliere BC MANAGER dal titolo:

"Il roulo del BC e DR Manager nell'era della mobilità e del cloud computing"

A seguire: "Business Case ENI"

Relazione di: Michele Fabbri di ENI dal titolo:

"L'esperienza ENI nella creazione del green data center"

18,00 Dibattito e Chiusura lavori

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.

La registrazione è possibile solo online sul portale 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 a tre sessioni appartenenti ad uno stesso Percorso Professionale (Tecnico, Legale, sulla Gestione della Sicurezza), sarà rilasciato un Diploma. I diplomi saranno inviati, per email, solo a chi ne farà richiesta a attestati@clusit.it.

6. HACKING FILM FESTIVAL

La sesta edizione 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.

Al termine delle due prime giornate, martedì 18 e mercoledì 19, dalle 18.15 alle 20.15 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, Giovanni Ziccardi, Lele Rozza e Raoul Chiesa, 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.

Al termine, gli spettatori sono invitati a partecipare ad un aperitivo offerto dalla cantina TERRE DELLA CUSTODIA.

La partecipazione è gratuita.

7. GLI SPONSOR DEL SECURITY SUMMIT 2013

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.

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