SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Indice

1. PRESENTAZIONE
2. PROGRAMMA DEL 17 MARZO
3. PROGRAMMA DEL 18 MARZO
4. PROGRAMMA DEL 19 MARZO
5. ATTESTATI E CREDITI CPE
6. HACKING FILM FESTIVAL
7. GLI SPONSOR DEL SECURITY SUMMIT

1. PRESENTAZIONE

Dal 17 al 190 marzo si terrà a Milano la settima 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 90 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-2015/registrazione-eventi.

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

2. PROGRAMMA DEL 17 MARZO

09:00 Registrazione

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

Presentazione del Rapporto Clusit 2015

I lavori del Security Summit si apriranno con la presentazione del Rapporto Clusit 2015.

Oltre alla consueta analisi degli attacchi ed incidenti del 2014 in Italia, in Europa e nel mondo, il Rapporto 2015 contiene un contributo inedito di Poste Italiane e della Polizia Postale e delle Comunicazioni ed un altro del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza.

Completano il Rapporto nove Focus On: Internet of (Hacked) Things; M-Commerce; Bitcoin, aspetti tecnici e legali della criptovaluta; Doppia autenticazione per l'accesso ai servizi di posta elettronica; Lo stato della sicurezza dei siti web della pubblica amministrazione; Il Regolamento generale sulla protezione dei dati: novità per i cittadini, le imprese e le istituzioni; Cloud e sicurezza: profili legali; Return on Security Investment; L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario.

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

Partecipano:

- Gigi Tagliapietra, Presidente Onorario Clusit, moderatore
- alcuni degli autori del Rapporto: Andrea Zapparoli Manzoni, Davide Del Vecchio, Paolo Bufarini
- Gastone Nencini, Trend Micro, Country Manager Italia
- Federico Santi, HP Enterprise Services, Client Principal – Southern Europe
- Alessandro Vallega, Oracle, Security Business Development Manager
- Stefano Volpi, Cisco, Area Sales Manager, Global Security Sales Organization (GSSO)

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

Essere oggi l'azienda mobile del domani: mobili e con la testa tra le nuvole, ma sicuri

Le opportunità offerte delle tecnologie mobili stanno cambiando il modo di lavorare delle persone. Le aziende governano o subiscono tale processo con la consapevolezza dei potenziali vantaggi, ma anche con una certa preoccupazione

rispetto agli impatti sulla sicurezza ICT, che è vista come un fattore abilitante per il cambiamento.

La Oracle Community for Security dedica questo appuntamento annuale a presentare la sua ultima pubblicazione (che sarà disponibile dopo la presentazione su http://c4s.clusit.it insieme alle sette precedenti), con lo scopo di dare voce ai numerosi interrogativi e provare a dare delle risposte: cosa significa essere "azienda mobile"? Come si rapporta dal punto di vista della sicurezza tale cambiamento all'interno di altri trend altrettanto dirompenti, come il Cloud? Quali sono gli aspetti di insicurezza o le opportunità di sicurezza di cui tenere conto? Quali misure posso adottare?

Lo faremo in una nutrita e dinamica tavola rotonda dove gli esperti di sicurezza e di tecnologie mobili del gruppo di lavoro racconteranno la loro esperienza e spiegheranno il loro punto di vista. Un appuntamento da non perdere!

Modera: Luca Bechelli

Partecipano: Riccardo Abeti, Mauro Alovisio, Fabio Bucciarelli, Andrea Mariotti, Roberto Obialero, Rosario Piazzese, Alessandro Vallega

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

(Cybercrime*Cryptolocker + Spie*APT)/ Datacenter * Hybrid cloud = AIUTOOOOO!

Cerchiamo di governare infrastrutture sempre più complesse e distribuite, esposte a minacce sempre più numerose e talvolta complesse, avendo sempre meno tempo e budget. Affinché questo scenario non diventi la ricetta per un incidente molto grave è opportuno cercare di razionalizzare processi e controlli, fino agli strumenti tecnologici, al fine poter avere il controllo della strategia di security e della sua efficacia, e non esserne succubi.

Docenti: Alessio Pennasilico e Maurizio Martinozzi

11.30-12.15 - Sala Granato - Atelier Tecnologico

SOC e Sicurezza gestita: rilevamento e risposta al Malware Evasivo

L'ultima evoluzione delle APT (...) sfrutta malware "evasivo" di crescente sofisticazione, in grado di eludere i sistemi di sicurezza più avanzati. In particolare, questo tipo di malware usa una serie di tecniche per determinare se si trova all'interno di un sistema di analisi anziché nel normale ambiente di lavoro dell'utente. In tal caso, il malware nasconde i propri comportamenti aggressivi, riuscendo così a raggirare completamente il rilevamento da parte del sistema di analisi, o perlomeno a limitare la quantità di informazioni che riesce ad estrarre.

Saranno illustrate le più recenti soluzioni, sia tecnologiche sia organizzative, per gestire e individuare questi attacchi. In particolare si mostrerà come i Managed Security Services di ultima generazione, dotati di una tecnologia innovativa, possano contrastare efficacemente questo tipo di minacce. La presentazione

mostrerà infine le tecniche di evasione omunemente adottate dal malware, come il il fingerprinting dei sistemi di analisi, l'uso di codice bloccante e le tecniche di rilevamento della presenza di un operatore umano.

Relatori: Marco Ceccon e Marco Cova

12.15-13.00 - Sala Granato - Atelier Tecnologico

Sistemi di gestione: ne vale davvero la pena! L'esperienza di Snam Rete Gas

Il raggiungimento della certificazione di un Sistema di Gestione, in coerenza con le diverse normative ISO, non deve essere visto solo come finalizzato all'ottenimento di un bollino imposto da esigenze specifiche, quali ad esempio il soddisfacimento di un requisito di un bando di gara o l'aggiunta di un elemento qualificante all'interno di un albo fornitori.

In alcuni casi l'esigenza di creare, formalizzare, e vivere un Sistema di Gestione nasce anche da una visione strategica interna all'azienda e volta a gestire al meglio i processi di business, ottenendo così vantaggi in termini di efficienza, efficacia e massimizzando il ritorno dell'investimento. Il Sistema di Gestione diventa così un valore aggiunto per l'organizzazione e non un elemento di costo o, peggio ancora, un insieme di formalismi.

Durante la presentazione interverrà il dott. Andrea Chittaro, Chief Security Officer di Snam, la società italiana leader in Europa nella realizzazione e gestione integrata delle infrastrutture del gas naturale, in qualità di promotore dell'adozione dei Sistemi di Gestione per la Sicurezza delle Informazioni (ISO/IEC 27001:2013) e della Continuità Operativa (ISO 22301:2012) per l'unità Sistemi di Processo Gas di Snam Rete Gas, la società interamente controllata da Snam che gestisce il trasporto del gas naturale lungo gli oltre 32.000 km della rete nazionale.

Nata all'inizio del 2012, l'unità Sistemi di Processo Gas ha iniziato a confrontarsi prima con il Sistema di Gestione Qualità, instaurato e certificato nel corso del 2013, per poi raggiungere l'anno successivo la certificazione ISO/IEC 27001:2013. Attualmente sta instaurando un Business Continuity Management System secondo quanto previsto dallo standard ISO 22301:2012.

Relatori: Andrea Chittaro e Paolo Sferlazza

14:30-16:00 – Sala Rubino – Percorso Professionale sulla Gestione della Sicurezza

Governare il Mobile in azienda: Tavola Rotonda con i protagonisti

Come indirizzare i requisiti di sicurezza, di conformità e di controllo dei costi per gestire al meglio le crescenti flotte aziendali di device mobili?

In questa sessione discuteremo delle migliori practice e dei principali problemi indirizzati dalle aziende che hanno già trasformato i propri processi di business in mobilità. Nell'intervento si parlerà di come governare le nuove tecnologie Mobile verso un approccio "MobileFirst" e dell'importanza di adottare una

piattaforma di MDM avanzata (EMM) come fondamento verso un nuovo ecosistema di soluzioni mobile verticali e innovative.

Docenti: Andrea Zapparoli Manzoni, Riccardo Canetta, Gary McConnel

14:30-15:15 – Sala Zaffiro – Atelier Tecnologico

Sei sicuro di non essere stato attaccato?

In questa sessione verrà dimostrato dal vivo un malware attack per discutere e dimostrare poi concretamente come un'azienda può difendersi oggi dagli attacchi sia in un'ottica di prevenzione che di rimedio.

Relatori: Marco Mazzoleni e Andrea Allievi

14.30-15.15 – Sala Granato – Atelier Tecnologico

SPID: l'opportunità per promuovere la Digital Trasformation nelle aziende private Italiane

SPID (Sistema Pubblico di Identità Digitale), la nuova infrastruttura nazionale per l'accesso unificato a servizi online della pubblica amministrazione, offre una grande opportunità al mercato privato. Considerando l'obbligo normativo, per le pubbliche amministrazioni, di offrire accesso ai servizi anche tramite il sistema SPID, per il mercato privato questa è un'opportunità per ridisegnare i propri sistemi di accesso e mettere le identità digitali al centro della loro trasformazione digitale. Integrarsi con l'infrastruttura SPID richiede la partecipazione ad una federazione SAML2.0, standard OASIS consolidato da ormai 10 anni (Marzo 2005); ma oggi l'opportunità vera è quella di dotarsi di un'infrastruttura di gestione degli accessi che sia in grado di rispondere alle principali sfide della trasformazione digitale cui sono chiamate le aziende per aprirsi ai nuovi consumatori digitali: esperienza utente sicura e unificata per enterprise, cloud e mobile, autenticazione forte e multilivello, audit & governance, controllo delle frodi e protezione della reputazione, omni-canalità, … Condividendo le esperienze di clienti nazionali ed internazionali Oracle e Alfa Group vi proietteranno nel mondo di chi ha già abbracciato la sfida della gestione delle identità a supporto della trasformazione digitale.

Relatori: Angelo Bosis e Matteo Galimberti

15.15-16.00 – Sala Zaffiro – Atelier Tecnologico

Aspetti di sicurezza di sistemi SCADA e Smart Metering

I sistemi SCADA e Smart Metering rappresentano una componente centrale nel governo delle infrastrutture industriali e gran parte delle infrastrutture critiche.

Un loro malfunzionamento può avere importanti ripercussioni sia sulla sicurezza e la disponibilità di servizi strategici quali l'energia i trasporti e la sanità, sia sui processi di business.

L'intervento si propone quindi di fornire una panoramica sulle caratteristiche tecnologiche principali di tali infrastrutture, rivolgendo una particolare

attenzione agli aspetti di sicurezza e sui profili di rischio, fornendo degli esempi tratti da esperienze concrete.

L'intervento affronterà inoltre i temi della normativa e della regolamentazione esistente o in via di sviluppo per queste aree, indicando infine delle linee di sviluppo efficaci per aumentare l'affidabilità e la protezione di tali sistemi.

Relatore: Danilo Benedetti

15:15-16:00 – Sala Granato – Atelier Tecnologico

Security Analytics attraverso i Machine Data, ovvero la gestione delle minacce note e non

La presentazione spiega agli esperti di Security come l'innovazione portata dall"Operational Intelligence" venga ulteriormente ampliata e valorizzata nei casi di Security Intelligence & Analytics grazie allo sfruttamento in Tempo Reale dei Machine Data (il segmento dei BIGDATA a più alta crescita, con la più estesa varietà e a maggior valore) creando un nuovo standard che va oltre i limiti dei SIEM tradizionali.

Relatore: Stefano Radaelli

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

Intelligence in "Cyberwar" scenarios – aka the continuous feeling that we are missing out something... :(

L'importanza dell'Intelligence globale e locale nel percorso dall'alerting ad una *reale* comprensione dell'attacco, passando attraverso la sua contestualizzazione.

Un esempio pratico di come un evento apparentemente banale possa condurci a gruppi di attacco ben organizzati e focalizzati.

Docenti: Raoul Chiesa e Daniele Nicita

16:30-18:00 – Sala Zaffiro – Seminario a cura dell'OWASP Italy Chapter

Sono previsti tre interventi:

Il 1° a cura di Egidio Romano
Con PHP Object Injection ci si riferisce ad una classe di vulnerabilità che può affliggere quelle applicazioni PHP che utilizzano la funzione "unserialize" in modo insicuro. Attraverso questo genere di vulnerabilità un potenziale attaccante potrebbe essere in grado di "iniettare" uno o più oggetti all'interno dello scope dell'applicazione.

Gli attributi di tali oggetti possono essere modificati arbitrariamente dall'attaccante, e ciò potrebbe causare un comportamento inaspettato del flusso di esecuzione dell'applicazione, che potrebbe consentire all'attaccante di eseguire diverse tipologie di attacchi, o nei casi più gravi di eseguire codice PHP arbitrario.

Il 2° a cura di Marco Balduzzi
In questo intervento presenteremo una nuova tecnica di cybersquatting da noi battezzata soundsquatting. Il soundsquatting consiste nell'utilizzare un set di parole omofone, ovvero di differente origine ma ugual suono, per dirottare inavvertitamente un utente verso un sito diverso da quello desiderato, normalmente gestito dall'attaccante e malizioso. Un esempio è dato da whether (se) e weather (meteo).

Utilizzando un tool da noi sviluppato, mostreremo in che modo il soundsquatting viene attualmente utilizzato per fini illeciti tra cui advertisting, scamming, phising e malvertising.

Il 3° a cura di Matteo Meucci
"La nuova OWASP Testing Guide v4, come non usarla per testare le applicazioni web!"

Presentazione della nuova Testing Guide v4. Quali sono le novità e casi di studio sulla corretta adozione dello standard.

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

Premio "Innovare la sicurezza delle informazioni" – 10a edizione

Clusit procederà alla presentazione e premiazione delle migliori tesi universitarie del 2014.

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: Claudio Telmon, coordinatore del Premio Clusit

Intervengono:

- gli studenti premiati, che presenteranno le proprie tesi: Andrea Braschi, Giuseppe Cascavilla, Andrea Continella, Claudio Guarisco, Flavio Lombardi
- Domenico Cavaliere, Presidente Emaze
- Fabrizio Sensibile, Senior Security Consultant, @ Mediaservice.net
- Viviana Rosa, Head of Training And Marketing, BSI Group

3. PROGRAMMA DEL 18 MARZO

09:00 Registrazione

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

Incontro con il Garante per la protezione dei dati personali

In apertura della seconda giornata è previsto un incontro con l'On. Antonello Soro, Presidente dell'Autorità Garante per la protezione dei dati personali.

La sessione, moderata da Gabriele Faggioli, Presidente Clusit, vedrà la partecipazione attiva del pubblico del Summit che avrà la possibilità, sia nel corso della sessione che già il giorno prima, di porre direttamente al Garante tutte le domande di interesse. Le domande saranno selezionate ed accorpate da un team del Clusit e l'On Soro risponderà direttamente ai presenti in sala.

11:30-13:00 – Sala Rubino – Percorso Professionale Legale

Una sola privacy per tutta l'UE. Il nuovo regolamento europeo sulla privacy: stato dell'arte, temi chiave, criticità ed opportunità.

Obbligo di rendere pubblici i furti di dati, privacy by design e by default, privacy impact assessment alla base dell'analisi dei rischi, privacy officer obbligatorio e ridisegno dei ruoli: questi alcuni dei concetti con cui le aziende saranno obbligate a fare i conti quando il nuovo regolamento europeo sulla protezione dei dati personali sarà approvato definitivamente. Regolamento non direttiva. Una differenza che significa validità in tutta l'UE del nuovo testo, senza bisogno di complessi iter legislativi nazionali per il recepimento.

La Oracle Community for Security ha guardato a questa rilevante riforma da un'ottica professionale con l'obiettivo di individuare i cambiamenti più significativi che le aziende europee dovranno affrontare. Non solo, però. L'analisi del testo ha evidenziato le similitudini tra i contenuti del Regolamento e il mainstream culturale che in questi anni di intensa e progressiva digitalizzazione dell'economia e delle relazioni sociali ha dato origine a standard di sicurezza, normative e provvedimenti a tutela di interessi diversi (utenti dell'e-commerce, delle carte di credito, dell'internet banking, …), tutti di fronte a rischi in continua evoluzione rispetto al passato.

Conoscere in anticipo il nuovo Regolamento sulla privacy è dunque un contributo interessante per orientare le scelte di investimento in sicurezza che la digital transformation impone, concretamente, di fare da subito.

Partecipano: Giancarlo Butti, Enrico Ferretti, Sergio Fumagalli, Andrea Longhi, Andrea Reghelin, Guglielmo Troiano, Alessandro Vallega

11:30-13:00 – Sala Zaffiro – Percorso Professionale Tecnico

Meglio prevenire che curare? L'approccio hacker ed i cyber attack

La gestione della sicurezza dei dati aziendali è sempre più complessa, i rischi sempre maggiori, come emerge da diversi report, tra cui quello Clusit e quello Cisco. Per questa ragione l'approccio classico basato sulla difesa perimetrale non

è più sufficiente, in un'epoca di reti vaste e diffuse, dove anche il datacenter esterno ha assunto un ruolo primario nella gestione dei dati aziendali più riservati. Cercheremo di analizzare assieme alcuni scenari, per comprendere da cosa è necessario difendersi, cercando di comprendere quali strategie possano essere le più efficaci per garantire la necessaria riservatezza, integrità e disponibilità dei dati. Perché curare soltanto non ci tutela a sufficienza e prevenire soltanto rischia di non permettere di gestire imprevisti che accadranno per certo.

Docenti: Alessio Pennasilico, Stefano Volpi, Marco Mazzoleni

11.30-13.00 – Sala Granato – Percorso Professionale sulla Gestione della Sicurezza

Dall'Information Security alla CyberSecurity, e ritorno (Come migliorare la sicurezza dell'azienda attraverso un efficace governo degli incidenti)

A fronte dell'escalation delle minacce informatiche degli ultimi tempi, i modelli di gestione della sicurezza devono cambiare? In che modo?

A partire da casi reali e da esperienze sul campo, parleremo di risposta agli incidenti, di come essa possa supportare il governo della sicurezza, di CyberSecurity e di Information Security e di come i due ambiti possano operare in modo coordinato per il miglioramento della protezione delle aziende.

Docenti: Luca Bechelli, Marco Di Leo, Fabio Vernacotola

14:30-16:00 – Sala Rubino – Percorso Tecnico

Soluzioni di sicurezza capaci di collaborare tra loro: nuove strategie per alzare le difese

Con l'ascesa di minacce sempre più sofisticate è quasi impossibile per i prodotti che offrono un solo livello di protezione garantire sicurezza efficace. È quindi necessario sviluppare una nuova generazione di soluzioni di sicurezza capaci di collaborare fra loro e di condividere informazioni.

Docenti: Andrea Zapparoli Manzoni e Walter Narisoni

14.30-15.15 – Sala Zaffiro – Atelier Tecnologico

CryptoLocker la punta dell'iceberg, impariamo a difenderci dagli attacchi mirati

Prendendo spunto (insegnamento) dal Ransomware CryptoLocker, la sessione esamina la tematica degli attacchi mirati e le soluzioni tecnologiche sviluppate da Trend Micro per difendersi.

Relatore: Patrick Gada

14.30-15.15 – Sala Granato – Atelier Tecnologico

Aziende senza frontiere ma sicure: confermata l'importanza dei sistemi convergenti

Introduzione su punti di forza e portfolio offerta a valore di Riverbed, evidenziando la leadership dell'azienda nell'Application Performance Infrastructure.

Approfondimenti sull'importanza del nuovo modello convergente che garantisce consolidamento, prestazioni e sicurezza di dati e applicazioni nel data center.

Aspetti tecnici ed esempi concreti di aziende che hanno già implementato SteelFusion, una soluzione che consente alle organizzazioni di ottenere il meglio da entrambi i mondi: centralizzando i dati, eliminando il downtime delle filiali e riducendo il TCO.

Relatori: Valter Villa e Pietro Felisi

15.15-16.00 – Sala Zaffiro _ Atelier Tecnologico

Skills 4 Security: antani?

Nuove figure professionali definite da standard, dalle norme, dal mercato, i corsi e le certificazioni sulla sicurezza informatica. Come orientarsi oggi e domani in questo scenario in forte evoluzione, mettendosi nei panni sia delle aziende che dei professionisti.

Relatori: Francesco Morini, Alberto Perrone, Roberto De Sortis

15.15-16.00 – Sala Granato – Atelier Tecnologico

ICS Security Assessment: metodologia ed esperienze pratiche

Da alcuni anni le cosiddette "Infrastrutture Critiche" ed, in particolare, i sistemi di controllo industriale (ICS – Industrial Control System) sono oggetto di un numero sempre più crescente di minacce ed attacchi sofisticati e complessi. La sensibilità sulle tematiche di ICS Security sta quindi aumentando e, di conseguenza, incrementano gli investimenti per la protezione di tali infrastrutture al fine di ridurre il livello di rischio.

Risulta quindi fondamentale valutare il livello di sicurezza attualmente presente all'interno dei siti produttivi attraverso una metodologia ripetibile ed efficace.

L'intervento si pone l'obiettivo di presentare la metodologia di assessment e le relative esperienze pratiche maturate per alcune delle principali realtà Oil & Gas che hanno consentito di identificare le aree di miglioramento rispetto alle principali best practice e standard di settore (es. NIST, ISO, CERT, etc) e di definire un piano di intervento compatibile con le regole e le prassi proprie dei contesti industriali critici.

Relatori: Alan Ferrario, Andrea Lombardini, Alessandro Marzi

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

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

Governance e sicurezza delle informazioni nella sanità pubblica

Docenti: Filomena Polito, Corrado Giustozzi, Alessandro Frillici

16:30-17:15 – Sala Granato – Atelier Tecnologico

Mobile, Big Data, Social Platforms, Cloud: la sicurezza IT al centro della Terza Piattaforma

Con il progressivo affermarsi di un nuovo ecosistema industriale basato su Mobile, Big Data, Social Platforms, Cloud – ovvero lo scenario che IDC chiama Terza Piattaforma che si intreccia con gli Innovation Accelerators (IoT, Robotics, 3D Printing, Cognitive Systems etc..) – una parte sempre più importante dell'economia verrà canalizzata attraverso i nuovi modelli economico-sociali che stanno prendendo forma oggi attraverso le innumerevoli iniziative che nascono in tutte le parti del mondo. Al centro di queste evoluzioni sostanziali che coinvolgono sia il settore che il mercato, la sicurezza IT giocherà sempre più il ruolo centrale di tecnologia abilitante che consente lo sviluppo di nuove imprese e nuova occupazione. Nel corso del suo intervento, IDC evidenzierà le tendenze di tali trasformazioni indicando le direzioni di investimento nazionali e internazionali e si soffermerà nel delineare le nuove aspettative che si vanno sviluppando attorno al ruolo e alla figura del Responsabile della Sicurezza.

Relatore: Fabio Rizzotto

4. PROGRAMMA DEL 19 MARZO

09:00 Registrazione

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

L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario

Aprirà i lavori della terza giornata una tavola rotonda moderata da Alberto Grisoni, Direttore di AZIENDA BANCA.

Scaduti i termini per l'adeguamento alla direttiva, a che punto sono le banche rispetto alle misure di sicurezza? Abbiamo invitato 5 banche per domandare loro che impatti ha avuto la direttiva e cosa stanno facendo per ottemperare ai requisiti richiesti.

Interviene: Romano Stasi, Segretario Generale del Consorzio ABILab

Partecipano alla tavola rotonda:

- Stefano Arduini, Cedacri SpA, Responsabile Internal Auditing, Certificazioni
- John Ramaioli, Banca Popolare di Milano, Responsabile Sicurezza e Business Continuity
- Pablito Rosa, Istituto Centrale Banche Popolari Italiane (ICBPI)
- Claudio Telmon, Clusit, Comitato Direttivo e Comitato Tecnico Scientifico
- Enrico Luigi Toso, DB Consorzio (gruppo Deutsche Bank), ICT Regulatory Risk and Control Specialist

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

(in)Sicurezza (im)Mobile: come non cadere nelle mani dei criminali dopo essere sopravvissuti alla ressa per acquistare l'ultimo nuovo smartphone

Il telefono che ho in tasca è più potente del PC che avevo sul tavolo qualche anno fa. I device si evolvono, abbiamo sempre l'ultimo modello in tasca, ma raramente ci preoccupiamo delle minacce. Perchè anche i rischi e gli attacchi evolvono.

Come affrontare questo scenario, in un contesto in cui questi telefoni "smart" conservano sempre più spesso dati aziendali, spesso su dispositivi personali?

Quale è il ruolo di questi dispositivi rispetto ad APT, malware, ransomware e tecniche varie che oggi costituiscono il vettore di attacco più frequente verso le nostre infrastrutture per la gestione delle informazioni?

Cosa deve fare una organizzazione per assicurarsi di affrontare queste minacce in modo adeguato?

Docenti: Alessio Pennasilico e David Gubiani

11:30-13:00 – Sala Zaffiro – Percorso Professionale Tecnico

Quanto diventa costoso non occuparsi della sicurezza per tempo e con mezzi all'avanguardia ?

Il perché di una soluzione end-to-end scalabile ed affidabile diventa sempre più evidente. Analisi dei punti di vista aziendali.

Docenti: Cristiano Cafferata e Giordano Zambelli

11:30-12:15 – Sala Granato – Atelier Tecnologico

Gli strumenti a supporto della Data Governance per l'adeguamento alla circolare 263 di Banca D'Italia

L'intervento verte sugli strumenti a supporto della Data Governance in conformità alle previsioni normative della circolare 263 di Banca d'Italia, in particolare il dizionario dei dati (Data Dictionary) e la documentazione delle regole di trasformazione (Data Lineage). Saranno illustrate le caratteristiche principali che devono avere tali strumenti da un punto di vista logico , come la capacità di descrizione dei dati sia da un punto di vista formale che semantico e la comprensibilità del linguaggio utilizzato da parte degli utenti business.

Verrà inoltre presentata la soluzione Oracle Enterprise Metadata Management che indirizza i requisiti di tracciabilità e governo del dato con approfondimento sulle funzionalità di Lineage Orizzontale e Verticale. Questa soluzione consente di visualizzare e documentare i dati importati dai differenti sistemi aziendali per facilitarne l'interpretazione e la traccibilità anche su grandi volumi, in questo modo si controlla il rischio connesso ai cambiamenti che occorrono sui dati, dai sistemi sorgenti fino ai report destinati agli utenti e si consente la verifica sulla qualità."

Relatori: Claudia Filippini e Stefano Coluccini

12:15-13:00 – Sala Granato – Atelier Tecnologico

Firewall Change & Vulnerability Management: Come rispondere ai requisiti dell'audit andando alla velocità del business

DIGI e Skybox analizzeranno il caso di una grande realtà Italiana e di come Skybox ha permesso di supportare tutte le fasi del processo di Change Management delle configurazioni firewall, controllando in modo attivo l'esposizione delle vulnerabilità nel rispetto delle normative e delle best practice di sicurezza.

Relatori: Mauro Cicognini e Matteo Perazzo

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

Cloud e sicurezza. Scenario e prospettive

Lo sviluppo dei servizi di cloud computing appare inarrestabile. La sicurezza è elemento essenziale da cui non si può prescindere. Per questo motivo a livello normativo esistono precisi vincoli da tenere in considerazione. Anche alla luce delle nuove ISO 27018 appare quindi quanto mai utile fare il punto sullo scenario attuale e sulle prospettive evolutive.

Docenti: Gabriele Faggioli, Fabio Guasconi, Raoul Brenna.

14:30-15:15 – Sala Zaffiro – Atelier Tecnologico

Il fenomeno delle cryptomonete: opportunità e rischi

A partire dal 2009 – anno in cui, con lo pseudonimo di Satoshi Nakamoto, uno o più sviluppatori hanno rilasciato la prima versione del software Bitcoin ed avviato il relativo network con l'emissione dei primi bitcoin – le criptomonete pienamente convertibili suscitano crescente interesse, con un impatto sempre maggiore sull'economia reale.

Basti citare che nel 2013 la Repubblica di Cipro ha scelto il bitcoin come "valuta rifugio'', mentre a partire da qualche anno fornitori di prodotti e servizi del calibro di Amazon o Miscrosoft accettano ufficialmente pagamenti in bitcoin.

Tuttavia, i requisiti funzionali e le specifiche implementative richiesti da approcci come Bitcoin sottendono problemi di non facile soluzione, e di cui in alcuni casi non si conosce neppure una formulazione adeguata.

Ciò espone l'adozione di tali sistemi ad incognite e rischi non solo relativi alla resilienza a frodi informatiche o ad altri tipi di attacco, ma anche alla sostenibilità ambientale e alle conseguenze sull'economia globale.

In questa presentazione cercheremo di chiarire in modo divulgativo quali sono gli aspetti tecnici ed implementativi di Bitcoin e delle sue principali varianti, discutendone vantaggi, criticità e potenziali sviluppi.

Relatori: Giovanni Schmid e Pasquale Forte

14:30-15:15 – Sala Granato – Atelier Tecnologico

Governare la Mobilità : Dimostrazione ed esempi di casi pratici dal vivo

Dal BlackBerry ai dispositivi di nuova generazione iOS, Android & Windows Phone, come affrontare la migrazione al MobileFirst. Dimostrazioni pratiche dal vivo di come alcune grandi aziende hanno affrontato la tematica di controllo e sicurezza di dispositivi, app e contenuti nella nuova era della mobilità. Nella sessione saranno presentati i principali problemi sulla governance della mobilità e illustrate alcune delle nuove tecnologie leader di mercato per la gestione integrata e sicura di app, dispositivi, dati e costi di traffico.

Relatore : Gary McConnell

15:15-16:00 – Sala Zaffiro – Atelier Tecnologico

Malvertising: il malware direttamente a casa tua!

Il Web Advertising stà diventando sempre di più il canale pubblicitario per eccellenza: è interattivo, profilato e tracciabile.

Permette alle aziende di raggiungere i propri "target" in modo selettivo, minimizzando le dispersioni ed aumentando così l'efficacia delle proprie campagne. Il trend di crescita delle pubblicità online è costante ed il numero di aziende che investono in questo settore è in aumento.

Ma uno strumento così potente, può essere utilizzato anche dai cybercriminali ? La risposta è sì, e si chiama Malvertising.

Il termine Malvertising nasce dall'unione di due parole inglesi: Malware ed Advertising.

Come dimostrato dai recenti attacchi che hanno infettato milioni di computer in tutto il mondo, questa tecnica si sta diffondendo velocemente, grazie alle sue caratteristiche principali: capacità di attrarre le vittime dell'attacco, precisione nell'identificazione dei bersagli, altissima velocità di diffusione, supporto multi piattaforma (computer, tablet, smartphones), nessuna esposizione diretta dell'attacante.

Durante l'intervento analizzeremo l'evoluzione del fenomeno attraverso l'analisi dei recenti attacchi, le tecniche utilizzate dai cyber criminali, le modalità di inserzione degli annunci pubblicitari e le possibili contromisure da adottare per difendersi, sia in ottica end-user che enterprise.

Relatori: Andrea Minigozzi e Giacomo Milani

15.15-16.00 – Sala Granato – Atelier Tecnologico

Forensics Readiness e Incident Response

Un'investigazione digitale viene comunemente impiegata come risposta post-evento ad un incidente informatico. Ci sono tuttavia molti casi in cui un'azienda potrebbe beneficiare della capacità di raccogliere e conservare le potenziali prove digitali prima che l'incidente si verifichi (forensics readiness) o durante l'incidente stesso (incident response). La forensics readiness è la capacità di massimizzare il

potenziale in termine di raccolta di prove digitali, minimizzando i costi. Mentre l'incident response è la capacità di gestire l'incidente mentre si sta verificando raccogliendo le prove senza rischiare di perderle o comprometterle. Durante il seminario saranno illustrati alcuni esempi concreti per l'implementazione di un sistema che soddisfi questi requisiti.

Relatori: Mattia Epifani e Francesco Picasso

16:30-17:15 – Sala Rubino – Atelier Tecnologico

APT (Advanced Persistent Threats): la nuova frontiera del malware

In principio c'erano virus e worm. I sistemi di sicurezza sono diventati così precisi e sofisticati da intercettarli tutti (o quasi) e il solo AntiVirus non basta. Ma i cybercriminali non restano fermi ad aspettare e per ogni contromisura cercano nuove mutazioni nei vettori e nuove minacce da sfruttare. Sviluppare contromisure intelligenti in grado di rilevare le mutazioni, i mascheramenti e le nuove minacce prima ancora che vengano classificate: questo è quello che si propone di fare il motore APT Blocker con le innovative tecnologie che utilizza.

Relatore: Emilio Tonelli

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

Sono previsti due interventi.

La governance dei rischi di outsourcing

L'intervento fornirà una serie di approfondimenti sul tema della governance dei rischi di outsourcing, ed in particolare toccherà i seguenti ambiti:

- l'approccio di ISACA per l'outsourcing ed il Vendor Management
- i rischi di outsourcing e la normativa 263 di Banca d'Italia
- le attività di verifica sull'outsourcing
- il Cloud Computing come nuova forma di outsourcing: rischi e controlli.

Docente: Giulio Spreafico

Social Network, APT, e metodi probabilistici per individuare reti di Cybercriminali online

Social Network, minacce avanzate e Cybercrime sono argomenti oramai indissolubilmente legati. Un Security Expert deve fronteggiare attacchi sempre più complessi e difficili da arginare, che uniscono ai vettori di attacco tecnologici l'exploitation of the weakest element, ovvero l'utente. In questo senso i Social Network sono diventati il "terreno di caccia" più sfruttato dai malintenzionati. Inzialmente l'acronimo APT (Advanced Persistent Threat) si riferiva quasi sempre attività di information warfare o di cyber espionage, spesso state-sponsored. Oggi le tecniche e gli approcci tipici di questo genere di attacchi si sono diffusi, tanto da essere ormai utilizzati anche in operazioni di cybercrime "comune". In questo speech parliamo di come i Social Network vengono sfruttati per lanciare attacchi a singoli, imprese ed organizzazioni pubbliche, e presentiamo un metodo statistico utile a rilevare le reti di cybercriminali su Social Network, al fine di prevenire o mitigare le loro aggressioni.

Docente: Gabriele Biondo

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

La rivoluzione digitale e i rischi per le aziende di produzione

Le attuali possibilità di connessione tra persone, processi, cose e dati creano opportunità di crescita e innovazione paragonabili ad una nuova rivoluzione industriale, che sta già modificando la società e l'economia.

1a parte: I CIO di tre differenti settori industriali illustreranno gli ambiti della traformazione digitale in atto.

Modera: Andrea Provini, Presidente AUSED

2a parte: I rischi connessi alla luce dei trend tecnologici in atto

Interviene: Andrea Zapparoli Manzoni, KPMG

3a parte: Le tecnologie disponibili per mitigare i rischi

Tavola Rotonda con i fornitori di tecnologia.

5. ATTESTATI E CREDIT 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.

6. HACKING FILM FESTIVAL

La settima 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 della prima giornata, martedì 17, dalle 18.15 alle 20.15 sarà proiettato il Telefilm Scorpion: prima puntata (pilot), ovvero cosa pensa il mondo degli hacker e della sicurezza informatica.

Durante il Festival Alessio Pennasilico, Corrado Giustozzi, Cristiano Cafferata e Giovanni Ziccardi 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.

La partecipazione è gratuita.

7. GLI SPONSOR DEL SECURITY SUMMIT 2015

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