Indice

1. SECURITY SUMMIT 2010

Sono state definite le tematiche che saranno trattate nelle sessioni formative del Security Summit di Milano (16-18 marzo 2010).

SESSIONI TECNICHE:

- "Log Management"
- "Spionaggio Industriale"
- "Evoluzione del Malware"
- "Soluzioni biometriche e strong autentication per l'accesso ai dati sensibili"
- "Sicurezza e telefonia mobile"

SESSIONI LEGALI:

- "Amministratori di sistema a valle della entrata in vigore del provvedimento"
- "Computer Forensic Aziendale"
- "Data Retention: lo stato dell'arte"

SESSIONI SULLA GESTIONE DELLA SICUREZZA (tutte in collaborazione con AIEA):

- "Il ritorno dell'investimento in sicurezza informatica (ROSI)"
- "Frodi Interne"
- "COBIT, ITIL, ISO27000" (con l'intervento di itSMF e di UNINFO).

Alle sessioni formative saranno affiancate alcune **tavole rotonde**:

- una dedicata al settore Finance, a cura di ANSSAIF
- una seconda con le aziende Partner, dedicata alla ricerca
- una dedicata alla sicurezza dei cittadini in rete, con la partecipazione di Istituzioni, Associazioni dei consumatori e Associazioni per la difesa dei minori.

- la quarta dedicata alle Aziende Utenti, organizzata assieme ad AUSED.

Ospiteremo inoltre i seminari di 6 associazioni e community del settore: AIP, AIPSA, AIPSI, ASIS ITALIA, Open BSD User Italia e OWASP ITALIA.

Il Security Summit 2010 sarà aperto da *Mark Abene*, con una presentazione dal titolo "The Evolution of System Intrusion (and the Changing Face of the Intruder)".

Profilo di MARK ABENE

Da oltre venti anni Mark Abene è un pioniere nel campo delle tecnologie dell'informazione ed un guru nell'ambito della sicurezza delle reti. La sua esperienza professionale è radicato nel suo passato di hacker degli anni 1980 e all'inizio del 1990, conosciuto in tutto il mondo come "Phiber Optik" per la sua ineguagliabile conoscenza dei sistemi di telecomunicazioni e dei packet switched networks. E' stato uno dei primi a dare lezioni in materia di sicurezza informatica dal punto di vista dell'attaccante, e a dibattere apertamente e difendere i meriti dell'hacking etico come strumento utile per l'industria. Da molti anni, la sua vasta gamma di competenze gli ha permesso di svolgere l'attività di consulente per alcune delle più importanti aziende americane e multinazionali, tra le quali val la pena di citare almeno le più note: American Express, UBS, First USA, Ernst & Young, KPMG, Sun Microsystems, Motorola, Toshiba, IBM, Transamerica Insurance Group.

Tra gli altri ospiti internazionali che interverranno in qualità di keynote speakers segnaliamo: Sharon Conheady (grande esperta di social engineering e penetration testing in UK), Pascal Lointier (Presidente CLUSIF, che presenterà una panoramica approfondita sulle attività di cybercrime nel 2009 in Europa e nel mondo), Claude Maury (Presidente CLUSIS, che presenterà un progetto di gestione della sicurezza, appena realizzato in una importante amministrazione svizzera), Sylvain Maret (docente presso l'Università di Ginevra, che presenterà un progetto di strong authentication con implementazione di soluzioni biometriche, appena realizzato in una banca di Ginevra) ed un esperto dell'FBI.

Nella newsletter di dicembre seguiranno i loro profili e gli abstract degli interventi.

2. NUOVO QUADERNO CLUSIT

È stato pubblicato un nuovo Quaderno Clusit: "**PCI-DSS: Payment Card Industry - Data Security Standard**", scritto da Jean Paul Ballerini e Fabio Guasconi.

Per il momento la consultazione del quaderno è riservata ai soci: www.clusit.it/private/p_soci/quad/Q08_web.pdf

Per tutti è disponibile invece una versione abstract: www.clusit.it/download/Q08_abs_web.pdf

Dopo 3 mesi il documento diventerà pubblico.

I precedenti quaderni sono ormai disponibili a tutti su www.clusit.it/download.

Una copia del quaderno sarà distribuita ai soci in occasione delle prossime manifestazioni pubbliche del Clusit.

Buona lettura!!

3. ROSI (RETURN ON SECURITY INVESTMENT)

Ancora oggi, i CISO e i CSO delle aziende fanno leva in particolare sulla gestione dei rischi e sulla necessità di adempiere ad obblighi normativi, per giustificare la richiesta di investimenti in sicurezza dei sistemi informativi. Il ritorno dell'investimento è raramente preso in considerazione, a causa della difficile dimostrabilità dello stesso e della complessità della materia. Eppure, sono sempre più le Direzioni Generali delle aziende che chiedono, e spesso pretendono, una giustificazione quantitativa del ritorno dell'investimento. E in momenti di crisi economica, e quindi di maggior attenzione all'allocazione dei budget, il management delle aziende, in mancanza di tale giustificazione quantitativa, tende a non intraprendere nuovi progetti in ambito sicurezza informatica.

In effetti, è veramente difficile dare una prova dei ritorni economici delle spese consacrate alla sicurezza. L'analisi del rendimento degli investimenti in sicurezza deve infatti tenere conto dei costi diretti e di quelli indiretti, dei costi tangibili (ad esempio, nel quantificare le coinseguenze di un incidente informatico: perdita di produzione, rimpiazzo di materiali, onorari di esperti, penalità di ritardo, costi di ricostruzione, danni ed interessi...) e di quelli intangibili, molto più difficili da quantificare (ad esempio, sempre in un incidente informatico: perdita di produzione non quantificabile, perdita di reputazione, perdita di parti di mercato, responsabilità civile, sanzioni amministrative...). E sono proprio i costi intangibili a rendere difficile la quantificazione finanziaria del ROSI.

Questo spiega perchè esistano così pochi studi e testi sulla materia, e praticamente nulla a livello italiano.

Lo scorso mese di settembre si è costituito un Gruppo di Lavoro sul ROSI (GdL), su iniziativa di AIEA, Clusit e Oracle, con la partecipazione di Deloitte, Ernst & Young, KPMG e PriceWaterhouseCoopers. Il GdL sta lavorando alla preparazione di un quaderno/studio che contenga indicazioni utili per le aziende per il calcolo del ROSI all'inteno dei propri progetti di sicurezza. Non si pretende di ottenere uno strumento preciso, ma almeno una serie di indicazioni sulla metodologia da utilizzare e sui fattori da prendere in considerazione per calcolare il ROSI.

Lo studio sarà presentato a marzo 2010 nel corso del Security Summit di Milano.

4. NOTIZIE DAL BLOG

29.11 - iPhone, primo worm ostile
http://blog.clusit.it/sicuramente/2009/11/iphone-primo-worm-ostile-.html

29.11 - Il Padrino dello spam va in carcere
http://blog.clusit.it/sicuramente/2009/11/il-padrino-dello-spam-va-in-carcere-.html

28.11 - Cronaca dalla Polonia
http://blog.clusit.it/sicuramente/2009/11/cronaca-dalla-polonia.html

18.11 - IDC Banking Forum 2009

http://blog.clusit.it/sicuramente/2009/11/idc-banking-forum-2009.html

Autore: Fabio Guasconi

16.11 - riformabrunetta.it sotto attacco dos

http://blog.clusit.it/sicuramente/2009/11/riformabrunettait-sotto-attacco-dos.html

Autore: Armando Leotta

09.11 - Attacco DDoS colpisce Agenzia di Intelligence Svedese

http://blog.clusit.it/sicuramente/2009/11/attacco-ddos-colpisce-agenzia-di-intelligence-svedese.html

09.11 - Preoccupazione dell'Amministrazione Obama per cyberattacchi e sabotaggi negli USA

http://blog.clusit.it/sicuramente/2009/11/preoccupazione-dellamministrazione-obama-per-cyberattacchi-e-sabotaggi-negli-usa.html

07.11 - FDA (Food & Drug Adiministration USA) allerta sulla CyberSecurity nei Medical Devices

http://blog.clusit.it/sicuramente/2009/11/fda-food-drug-adiministration-usa-allerta-sulla-cybersecurity-nei-medical-devices.html

Autore: Enzo M. Tieghi

04.11 - Quanto vale uno "scalpo" Mac

http://blog.clusit.it/sicuramente/2009/11/quanto-vale-uno-scalpo-mac.html

Autore: Gigi Tagliapietra

03.11 - Polimi e il phishing "accademico" di poste italiane

http://blog.clusit.it/sicuramente/2009/11/polimi-e-il-phishing-accademico-di-poste-italiane.html

Autore: Armando Leotta

5. OFFERTE DI LAVORO

Si ricercano 2 professionisti con i seguenti requisiti:

- Ingegnere informatico / elettronico o dottore in informatica o titolo equipollente
- Possesso di qualifica Auditor/Lead Auditor ISMS Information Security Management System (ISO 27001) - corso di 40 ore con accreditamento CEPAS o AICQ
- Esperienza minima di 3 anni nella gestione di progetti ISMS Information Security Management System (ISO 27001)

- Età 28 - 40 anni
- Preferibilmente lavoratore autonomo (P. IVA o con emissione di ricevuta per collaborazione); se collabora con altre società non dovrà avere alcun rapporto di esclusiva o patti di non concorrenza con queste società.

La contrattualizzazione del rapporto dovrà comunque avvenire direttamente con il professionista.

Le figure di cui trattasi saranno inserite in un team di lavoro per la gestione del progetto di certificazione ISO 27001, già in corso di implementazione, presso un'importantissima società del settore aeronautico.

L'incarico sarà di 6 mesi rinnovabili per altri 6 mesi con impegno giornaliero full time.

Il compenso sarà commisurato in base all'esperienza che il professionista saprà dimostrare.

La zona di lavoro è Roma Nord.

Si richiede disponibilità immediata.

Chi fosse interessato può scrivere a info@clusit.it

Azienda del settore, ricerca per un proprio cliente una figura di "coordinamento tecnico" da affiancare al Responsabile Sicurezza IT.

Sono richiesti :

- 4-5 anni di esperienza in ambito sistemistico/sicurezza
- diploma o laurea in Informatica o Ingegneria Informatica
- eventuali certificazioni (OSSTMM, CCNA/CCNP o MCSE/MCSA)
- buone conoscenze di LAN/WAN internetworking ed esperienza di vulnerability assessment
- capacità di relazione, coordinamento e redazione di documenti tecnici.

Situazione contrattuale e compenso sono ancora da definire.

La zona di lavoro è Milano città.

Chi fosse interessato può scrivere a info@clusit.it

6. CORSI IN AMBITO GIURIDICO

CORSO DI DIRITTO PENALE DELL'INFORMATICA (gennaio - giugno 2010)

Segnaliamo un corso di diritto penale dell'informatica organizzato dall'Università LUMSA di Roma.

Il corso è coordinato dall'Avv. Stefano Aterno e, tra i docenti, notiamo la partecipazione di diversi soci ed amici del Clusit.

Il programma e tutte le informazioni utili sono disponibili su http://www.apdi.it/PROGRAMMA_CORSO_LUMSA.PDF

CORSO DI PERFEZIONAMENTO IN COMPUTER FORENSICS E INVESTIGAZIONI DIGITALI

Segnaliamo la terza edizione del Corso di Perfezionamento in "computer forensics e investigazioni digitali" dell'Università degli Studi di Milano.

Il corso, che è aperto ai laureati in qualsiasi disciplina, è coordinato dal prof. Giovanni Ziccardi.

Il programma e tutte le informazioni utili sono disponibili su www.computerforensics.unimi.it/ e su http://infogiure.typepad.com/

IL TERMINE ULTIMO PER PRESENTARE LE DOMANDE DI ISCRIZIONE È IL 10 DICEMBRE 2009.

7. NOTIZIE E SEGNALAZIONI DAI SOCI

La deadline per l'invio di eventuali segnalazioni dei soci per la pubblicazione sulla newsletter è il 25 di ogni mese

L'UNICRI (United Nations Interregional Crime & Justice Research Institute) organizza dei corsi di formazione contro il cybercrime, i quali avranno luogo presso il Training Campus delle Nazioni Unite a Torino, nel periodo febbraio-aprile 2010.

I corsi, erogati in lingua inglese e suddivisi in 4 moduli principali, prevedono diversi livelli (Basic, Intermediate, Advanced) e verteranno sui seguenti argomenti:

- Information Security (InfoSec)
- Profiling Hackers (HPP)
- SCADA & National Critical Infrastructures (SCADA)
- Digital Forensics (DF)

Sono in via di definizione accordi specifici e sconti per i soci CLUSIT: ne verrà data pubblicazione non appena ufficializzati.

Ricordiamo come partecipare ai moduli formativi erogati dallo UN Campus dia la possibilità, oltre all'aggiornare il proprio know-how tecnico, di entrare in un universo molto particolare e diverso dal proprio, frequentando e confrontandosi con gli altri partecipanti, i quali proverranno in gran parte da istituzioni, Law Enforcement ed aziende private di Paesi esteri.

Per informazioni ed iscrizioni:

http://www.unicri.it/wwd/cybertraining/index.php

NETASQ e la nuova nata econnet Srl hanno siglato un accordo di distribuzione per la commercializzazione delle soluzioni di intrusion prevention e antispam del vendor francese.

Leggi il comunicato stampa su
http://www.netasq.com/_pdf/news2009/ITPR0911_ECONNET.pdf

8. EVENTI SICUREZZA

2 dicembre 2009, Milano

"Nuove disposizioni del Garante: come adeguarsi in tema di Privacy", a cura di Visiant Security

http://www.visiantsecurity.it/VisiantSecurity/fullnews.jsf?main=news

7-11 dicembre 2009, Honolulu

ACSAC 2009

http://www.acsac.org/

10 dicembre 2009, Roma

Seminario CLUSIT "L'importanza delle soluzioni di storage nella sicurezza della Virtualizzazione"

https://edu.clusit.it/scheda_seminario.php?id=45

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