

Sicurezza Informatica: concetti, metodologie, possibili rischi

Seminario Formativo Nazionale

30 settembre 2006

Lanciano (CH)

Sala Congressi - Banca Popolare di Lanciano e Sulmona
Viale Cappuccini, 76



Le informazioni gestite dai sistemi informativi privati e pubblici costituiscono una risorsa di valore strategico per il mercato ed il governo del paese. L'obiettivo di questo seminario è quello di incrementare la "sensibilità" al tema della sicurezza ICT attraverso l'acquisizione di una maggiore consapevolezza alle nuove minacce, vulnerabilità e rischi.

Grazie ad una impostazione originale e grazie alla partecipazione di noti ed autorevoli esperti del settore ICT lo svolgimento del seminario è suddiviso in due parti: nella prima parte si concentreranno gli interventi volti a descrivere i nuovi scenari della sicurezza ICT; nella seconda parte saranno realizzati dei laboratori nei quali i partecipanti potranno "realmente" vedere le principali tecniche di attacco utilizzate dagli hacker le contromisure e le metodologie di difesa. Inoltre sempre nella seconda parte saranno predisposte, dai vendor partecipanti, tre sessioni dimostrative, "turbo-talks" di nuovi prodotti e soluzioni sulla sicurezza ICT.

in collaborazione con :



"Improve your Security"



Comune di Lanciano

Target : Il seminario è rivolto a tutti i responsabili e tecnici informatici, personale amministrativo e consulenti legali che vogliono acquisire o aggiornare le basi teoriche e pratiche della sicurezza ICT.

Relatori : Il seminario è tenuto da esperti del settore ICT di vari ambiti professionali : docenti universitari, rappresentanti delle forze dell'ordine, professionisti, consulenti e legali .

Adesioni: La partecipazione al seminario è gratuita. I posti sono limitati. Si prega di verificare la disponibilità e confermare l'adesione al seguente indirizzo:

<http://www.dinets.it/iscrizioni>

Al termine del seminario sarà rilasciato l'attestato di partecipazione dall'Università degli studi di Teramo. Per ulteriori informazioni contattare:

DiNets s.r.l.

Tel. : 071 7211234 email : info@dinets.it

con il patrocinio di :



Arma dei Carabinieri



Guardia di Finanza



Sicurezza Informatica: concetti, metodologie, possibili rischi

Programma del Seminario

Parte A – mattina (09.30 – 13.00)

- Segreteria organizzativa:** *Pina Nativio – Banca Popolare di Lanciano e Sulmona*
- Moderatore:** *Roberta Zimei – giornalista - Università degli Studi di Chieti e Pescara*
- 09.30 **Inizio Lavori:** *Filippo Paolini – Sindaco di Lanciano*
- 09.45 **Il problema della sicurezza nel settore ICT: risorse da proteggere, dati, sistemi e reti**
Antonio Teti – Responsabile ICT (Information and Communication Technology) Università degli Studi di Chieti e Pescara
- 10.05 **La criminalità in Rete: scenari e metodologie per combatterla**
Giovanni Antolini – Generale Comandante della Regione Carabinieri Abruzzo
- 10.25 **Hacking e Computer Crime**
Domenico Vulpiani – Direttore del Servizio Polizia Postale e delle Comunicazioni
- 10.45 **CIA (Confidentiality, Integrity and Availability) e il valore delle informazioni**
Umberto Rapetto – Colonnello Comandante Gruppo Anticrimine Tecnologico (GAT) della Guardia di Finanza
- 11.05 **Sicurezza: il punto di vista della pubblica amministrazione**
Gianfranco Pontevolpe – CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione)
- 11.25 **La normativa vigente, il Codice della Privacy e il Documento Programmatico sulla Sicurezza**
Andrea Monti – Avvocato
- 11.45 **Coffee Break**
- 12.00 **Il mercato della sicurezza IT: richiesta e offerta**
Matteo Sticozzi – DiNets
- 12.15 **Ethical Hacker: Anatomia di un Hacking**
Francesco Arruzzoli – Security Manager – CEH
- 12.45 **Certificazioni e Formazione nel settore IT: l'esigenza di percorsi formativi specialistici**
Luciano D'Amico – Coordinatore Master Business and Information System Analyst – Università degli Studi di Teramo
- 13.05 **Certificare il processo di sicurezza delle informazioni: dalla BS7799 all'ISO20000**
Gabriele Picchi – Enterprise Solution Consultant
- 13.25 **Lunch break**

Sicurezza Informatica: concetti, metodologie, possibili rischi

Parte B – pomeriggio (14.15 – 18.00)

14.15 **Principali architetture di sicurezza ICT**
Pierpaolo Fava - ICT Security Engineer - DiNets

14.35 **Tecniche di analisi per la sicurezza dei sistemi ICT (network e vulnerability assessment, Hardening, HoneyPot, Penetration Test, etc.), strumenti e tecniche di computer forensics per la conservazione e l'analisi delle evidenze.**
Francesco Arruzzoli - Security Manager - CEH

15. 30 - **Coffee Break**

15. 40 **Laboratorio pratico dimostrativo**

Esempi delle più frequenti tipologie di attacco:

Come si realizza un Exploit :

- *Buffer overflow (come prendere il controllo remoto di un computer)*
- *Extended Unicode Directory Traversal Vulnerability (Attacco al Web Server)*
- *Cross Site Scripting (sfruttare le debolezze di un content management)*
- *SQL Injecton (attacco al database)*

Come si realizza un Denial of Service :

- *DDOS Flooding Attack (bloccare servizi di rete)*
- *RPC Attack (crash di un computer remoto)*
- *Malicious Scripts (crash di un computer)*

Social Engineering Attack:

- *Phishing (mascheramento e reindirizzamento)*

Wireless Attack:

- *Wardriving e WEP Cracking*

Esempi di architetture e metodologie di sicurezza

- *Configurazione di un laboratorio virtuale di test*
- *Strumenti per l'analisi ed il Vulnerability Assessment*
- *Effettuare un Penetration Test*
- *Realizzazione di una Honeypot*
- *Strumenti e tecniche per la crittografia e steganografia delle informazioni*
- *Ricerca e conservazione delle evidenze, alcuni dei principali Computer Forensics tools: autopsy, sleuthkit, etc.*

17.00 **TurboTalks:** 3 tavoli di discussione e dimostrazioni sui Prodotti e sulle soluzioni presentate dai vendor partecipanti

17.45 **Conclusioni e dibattito**

18.00 **Fine Lavori**

Vendor partecipanti :



www.f5.com



www.infoblox.com



www.landesk.com

Sicurezza Informatica: concetti, metodologie, possibili rischi

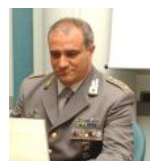
Relatori

Antonio Teti è responsabile dell'I.C.T.S. (Information and Communication Technology Service) dell'Università degli Studi "G.d'Annunzio" di Chieti-Pescara. È docente di informatica presso l'Ateneo di Chieti-Pescara, l'Università degli Studi di Teramo e l'Università Cattolica del Sacro Cuore di Roma. Ha collaborato per attività di formazione con le Facoltà di Informatica dell'Università Politecnica di Valencia e l'Università Politecnica di Madrid. Svolge attività di formazione e consulenza presso strutture pubbliche e private. È Consulente Tecnico di Ufficio per i Tribunali italiani per perizie e consulenze informatiche. È componente, per l'AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico) del gruppo di progettazione e sviluppo del programma di certificazione europeo EUCIP (European Certification of Informatics Professionals). È consigliere direttivo dell'AIP (Associazione Informatici Professionisti) e componente del CLUSIT (Associazione Italiana per la Sicurezza Informatica del Dipartimento di Scienze dell'Informazione dell'Università di Milano). È autore di diversi testi, tra cui "EUCIP - Il manuale per l'Informatico professionista" - U. Hoepli Editore, indicato come testo di riferimento per gli informatici dall'Institute for Future Studies (IFS) di Innsbruck. Scrive su riviste e periodici del settore.



Giovanni Antolini è Generale di Brigata dei Carabinieri e Comandante della Regione Carabinieri Abruzzo. Ha prestato servizio presso il Battaglione Carabinieri Laives, Comandante della Compagnia di S. Candido (BZ), Aiutante di Campo del Vice Comandante dell'Arma dei Carabinieri, Comandante del Nucleo Operativo di Messina, del Comando Provinciale di Vicenza e Bolzano. È stato impegnato in "prima linea" nella lotta contro la criminalità organizzata quale comandante della Sezione Anticrimine (ROS) di Palermo. Ha frequentato numerosi corsi di specializzazione presso la scuola Ufficiali e la Scuola di Guerra dell'Esercito di Civitavecchia. Laureato in Scienze della Sicurezza Interna ed esterna, presso l'Università degli Studi di Roma Tor Vergata, è stato titolare della Cattedra di Tecniche Investigative della Scuola Ufficiali Carabinieri di Roma.

Domenico Vulpiani, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Coordina le attività operative e organizzative della Polizia di Stato specializzata nel contrasto ai crimini informatici e nella tutela delle comunicazioni. In precedenza è stato il responsabile dei servizi di scorta e sicurezza del Capo dello Stato e di altre figure istituzionali di rilievo. In ambito investigativo ha operato nel mondo dell'antiterrorismo (UCIGOS) e ha diretto per 5 anni la DIGOS di Roma svolgendo numerose operazioni di servizio che hanno condotto all'arresto di pericolosi criminali e terroristi. Ha frequentato con profitto molti corsi di alta qualificazione professionale. Ha inoltre redatto articoli a carattere tecnico-giuridico pubblicati su riviste specializzate e ha partecipato a numerosi convegni nazionali ed internazionali in qualità di relatore.



Umberto Rapetto è Colonnello della Guardia di Finanza e comanda il GAT (Gruppo Anticrimine Tecnologico). Dirigente per sette anni dell'Authority per l'Informatica nella P.A., ha prestato servizio al Comando Generale, al Nucleo Speciale di Polizia Valutaria e al Nucleo Speciale Investigativo. Iscritto all'Ordine dei Giornalisti, editorialista su quotidiani e periodici nazionali, ha scritto numerosi libri su temi relativi ai crimini informatici, la tutela della privacy, gli scenari internazionali del terrorismo. È docente presso prestigiose università italiane e straniere.

Gianfranco Pontevo lavora presso il Centro Nazionale per l'Informatica della Pubblica Amministrazione (CNIPA) dove è responsabile dell'ufficio che si occupa delle tecnologie per la sicurezza informatica. Partecipa, in qualità di relatore, a diversi eventi formativi e divulgativi sulla sicurezza informatica. È membro di gruppi di lavoro nazionali e internazionali: Osservatorio sulla sicurezza delle reti e delle comunicazioni, Comitato di garanzia Internet e minori e Comitato OCSE su sicurezza e privacy. Nella sua venticinquennale carriera ha partecipato a numerosi progetti tecnici concernenti l'analisi, la progettazione, la realizzazione, la gestione e l'evoluzione dei sistemi informativi.



Andrea Monti esercita la professione di avvocato e si occupa di diritto delle telecomunicazioni e delle nuove tecnologie. Fra i suoi clienti annovera software house internazionali, operatori telefonici, internet provider, società internazionali di consulenza, gruppi bancari, gruppi editoriali e case editrici. Ha collaborato e collabora con diverse università (in particolare, con quella di Chieti e di Milano). Svolge regolarmente attività di formazione per le forze di polizia. Scrive di rete e di legge per svariate riviste. Tra i vari testi prodotti si citano: "Spaghetti Hacker" e "Segreti, spie, codici cifrati" di Apogeo Editore e la traduzione italiana del libro di Alan Cooper "The inmates are running the asylum" edito con il titolo "Il disagio tecnologico". È relatore in numerosi convegni italiani e internazionali.

Matteo Sticozzi laureato in Ingegneria Elettronica con specializzazione in Telecomunicazioni, membro della commissione informatica e telecomunicazione dell'ordine degli ingegneri di Ancona, è Direttore Commerciale di Dinets società specializzata nella progettazione e realizzazione di infrastrutture ICT ad alta disponibilità, soluzioni di sicurezza e management. Ha maturato una ventennale esperienza in aziende quali GTE Telecomunicazioni, IBM, Centron International e TrendMicro dove si è occupato di consulenza, progettazione reti e soluzioni di sicurezza. È membro del comitato direttivo di Sphaer@-HI (International Co-Operation) onlus per la cooperazione internazionale mirata alla telemedicina.



Francesco Arruzzoli è il responsabile della divisione ICT Security della DiNets. Progettista di sistemi esperti da più di 15 anni si occupa dello sviluppo di applicazioni per il management e la sicurezza di reti TCP-IP, consulenza, auditing, progettazione ed implementazione di soluzioni per la sicurezza di sistemi informativi complessi. Ethical Hacker certificato all'E-Council americano (International Council of E-Commerce Consultants), esperto indipendente dell'ENISA (European Network and Information Security Agency), membro del Clusit (Associazione Italiana per la Sicurezza Informatica) e dell'AICA (Associazione Italiana per l'Informatica ed il Calcolo Automatico) ha ricoperto in passato ruoli di responsabile software, System Engineer e ICT Security Manager presso aziende di informatica e telecomunicazione, società multinazionali e importanti strutture della sanità italiana.

Luciano D'Amico è professore ordinario di Economia Aziendale all'Università di Chieti-Pescara e Coordinatore del Master Business and Information System Analyst della Facoltà di Scienze della Comunicazione dell'Università degli Studi di Teramo. Membro dell'Accademia Italiana di Economia Aziendale e della Società Italiana di Storia della Ragioneria, è stato delegato dal Magnifico Rettore dell'Università di Teramo per la formazione professionale e al bilancio dell'Ateneo. È Presidente della Commissione Programmazione, Bilancio e Derghe dell'Università di Teramo e componente della Commissione per la Diffusione e applicazione dei principi contabili del Consiglio Nazionale Dottori Commercialisti a partire dal 2004.



Gabriele Picchi è certificato EUCIP Enterprise Solution Consultant e consulente scientifico e direttore dell'area organizzazione di Euristicia Srl. Opera dal 1996 come project manager per progetti di informatica ed organizzazione per aziende, pubblica amministrazione, Istituti ed Enti di Ricerca. È docente in corsi di alta formazione e di corsi di Educazione Continua in Medicina nell'area dell'informatica scientifica. È membro del Collegio dei Provvisori dell'Associazione Informatici Professionisti e del Project Management Institute della IEEE Computer Society. Lead Auditor ISO27001.