Indice

1. NUOVI SOCI

Hanno aderito al CLUSIT le seguenti organizzazioni:

- Cartiere del Garda (Riva del Garda - TN)
- EasyOne (Camisano Vicentino - VI)
- Italgo (Mezzago - MI)
- XCOM Wide Comunication (Salerno)
- Vision Automation (Cesano Boscone - MI)

2. LA RICERCA IN MATERIA DI SICUREZZA INFORMATICA IN ITALIA

La sicurezza dei dati e delle reti in funzione del suo impatto sul sistema Paese, con particolare riferimento all'economia e alla sicurezza dei cittadini, è oramai diventata un tema centrale nel contesto della moderna Società dell'Informazione e della Comunicazione. In questo quadro si sono moltiplicate in tutto il mondo le iniziative mirate a stimolare attività di ricerca, sviluppo e innovazione nel campo della sicurezza informatica. Gli attori coinvolti in queste iniziative non sono solo le Accademie e gli istituti di ricerca ma anche soggetti privati e pubbliche amministrazioni interessate alla realizzazione di dispositivi e applicazioni che oltre ad innovare i processi produttivi tengano conto dei necessari requisiti di sicurezza. Anche nel nostro Paese, nel corso degli ultimi anni abbiamo assistito al moltiplicarsi di iniziative, tra le più disparate, nel settore. Diversi gruppi di ricerca hanno iniziato ad operare su temi specifici del settore, sono stati avviati Master Universitari sul tema, Corsi di Laurea e numerose realtà aziendali sono impegnate in progetti di ricerca su tematiche centrali o molto contigue a quelle della sicurezza informatica.

Per discutere di questi temi, con l'obiettivo di dare un nuovo impulso alle iniziative di ricerca, i Proff. Danilo Bruschi e Luigi V. Mancini, con il patrocinio del Clusit, organizzano il Primo Workshop Italiano su PRIvacy e

SEcurity (PRISE 2006). La manifestazione si svolgerà a Roma nella seconda quindicina del prossimo mese di giugno, nell'ambito di "Infosecurity Italia 2006" o presso il Dipartimento di Informatica dell'Università "La Sapienza" . Il workshop è aperto a ricercatori, esperti del mondo della pubblica amministrazione e dell'industria. Tutti coloro che sono interessati a contribuire ai contenuti scientifici dell'iniziativa sono invitati a

sottoporre entro il 26 Aprile 2006 un abstract (2-4 pagine all'indirizzo: prise2006@di.uniroma1.it) che descriva il proprio contributo di ricerca.

Gli autori dei contributi selezionati per la presentazione al Workshop riceveranno comunicazione in questo senso entro il 15 Maggio 2006. Segue una lista non esaustiva delle principali tematiche di ricerca interessate: Anonimato - Analisi di codice maligno - Analisi di protocolli - Analisi di nuove forme di attacco - Autenticazione e autorizzazione - Biometria - Controllo degli accessi - Crittografia applicata - File system security - Intrusion detection - Privacy-enhancing technology - Sicurezza dei dati e delle reti - Sicurezza dei Sistemi Operativi - Sicurezza in ambienti eterogenei - Sicurezza in ambienti mobili - Sicurezza in reti peer-to-peer - Sviluppo di Software Sicuro - Trust model and Trust management policies - World Wide Web security.

Per qualunque ulteriore informazione, si può scrivere a: prise2006@di.uniroma1.it.

3. I VIRUS SUI PC HANNO COMPIUTO 20 ANNI

Sono ormai oltre 20 anni che i virus dei Pc imperversano in tutto il mondo. Nel gennaio del 1986, infatti, Brain -l'antenato di tutti i virus informatici- colpì per la prima volta, diffondendosi attraverso i floppy disk: il vecchio Brain era relativamente poca cosa, ma ha segnato l'inizio di un'escalation di cui nessuno, a oggi, può prevedere la fine. Brain era un virus che infettava quella parte di un floppy disk (il boot sector) contenente informazioni necessarie all'avviamento del sistema operativo. E' stato un tipo di virus che ha avuto una sopravvivenza relativamente lunga, all'incirca dal 1986 al 1995, estinguendosi in pratica insieme ai floppy disk. Il fatto che la trasmissione del virus avvenisse solo via dischetto da computer a computer ovviamente ne rallentava molto la diffusione. Le cose cominciarono a cambiare nel 1995 con l'apparizione dei macro virus, che sfruttavano le vulnerabilità di Windows. Il periodo più cruento della loro diffusione durò all'incirca quattro anni, con un tempo di diffusione decisamente più rapido di Brain: circa 1 mese dal momento in cui un macro virus veniva scoperto a quando diventava un problema globale.

Con la diffusione della posta elettronica si è poi avuto il momento dei "worm", che erano in grado di creare una "epidemia" in un solo giorno. Il più noto tra i primi di questa di questa categoria è senz'altro il famoso ILOVEYOU, che nel 1999 ha causato danni economici enormi in tutto il mondo.

Nel 2001 i tempi si accelerano ulteriormente e da un giorno si è passati a un'ora: una sola ora perché nuovi worm in rete come Blaster e Sasser riuscissero a infettare in modo automatico e indiscriminato qualsiasi

computer connesso a Internet che non si fosse dotato di una idonea protezione.

Attualmente, sono oltre 150.000 i virus noti e il numero cresce ogni giorno.

Alla luce anche delle preoccupazioni per un possibile prossimo attacco "virale" massiccio, è lecito domandarsi se tutte le aziende hanno almeno un antivirus attivo ed aggiornato. Ma non basta. Infatti, sappiamo che avere un sistema antivirus attivo e periodicamente aggiornato, su tutte le macchine, nessuna esclusa, non è sufficiente: l'esperienza insegna che è essenziale eseguire periodicamente un'analisi delle vulnerabilità e dei "carotaggi" possibilmente eseguiti da terzi "a sorpresa" (c.d. "vulnerability assessment").

A noi risulta che sono solo il 30% delle banche ad essere in regola; non solo, ma da una indagine a campione del 2004 ben il 3% delle banche non ha mai eseguito un'analisi del rischio nè delle vulnerabilità.

(Fonte: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria. www.anssaif.it)

4. COME REAGIRE AI PEN-TEST NON AUTORIZZATI

Riportiamo integralmente un articolo dell'Avv. Andrea Monti, socio fondatore e membro del CD Clusit, tranno dal primo numero di ICTLEX BRIEFS.

IL CONCETTO IN SINTESI

* Il pen-test non autorizzato è uno strumento con il quale "ricercatori indipendenti" cercano vulnerabilità dei sistemi informativi delle aziende.

* I risultati dei pen-test sono comunicati agli interessati, insieme all'avviso che - nel migliore dei casi - in assenza di dichiarazioni pubbliche di ringraziamento allo "scopritore", l'informazione sulla vulnerabilità sarà comunque resa nota.

* Queste azioni possono configurare quantomeno il reato di estorsione a carico dello "scopritore".

* Le reazioni possibili, da parte di un'azienda, sono tre: azione legale, deniability, muro di gomma.

* Ogni soluzione ha delle controindicazioni. L'azione legale può creare problemi di immagine e deve necessariamente essere portata a compimento; la negazione del problema espone al rischio che l'insabbiamento della notizia sia soltanto parziale; il muro di gomma richiede di adottare alcuni provvedimenti immediati (nei casi più seri anche dei licenziamenti), nella consapevolezza che dopo qualche tempo la vicenda sarà totalmente dimenticata.

IL CONCETTO IN TEORIA

Premessa

Capita sempre più di frequente anche in Italia, che internet provider, compagnie telefoniche e - in generale - aziende di una certa dimensione vengano avvicinate più o meno direttamente da soggetti che dicono di avere scoperto una vulnerabilità dei loro sistemi informativi (spesso si tratta dei web istituzionali). Questi soggetti - quantomeno nei

casi analizzati direttamente - "colgono l'occasione" per formulare vari tipi di richieste che vanno dal preannunciare tout court la diffusione in pubblico della vulnerabilità, al chiedere che venga emesso un comunicato stampa con ringraziamenti pubblici al "ricercatore indipendente" di sicurezza, al proporsi addirittura come consulenti.

1. I reati possibili

Benché non automaticamente illecita, eseguire pen-test non autorizzati e diffondere senza alcun controllo i risultati può degenerare facilmente nell'estorsione, un reato punito dall'art. 629 del codice penale (c.p.) con la reclusione da cinque a dieci anni e una multa da 516,00 a 2065,00 Euro. Questi comportamenti possono inoltre essere sanzionati con l'art. 615 ter c.p. che punisce l'(anche tentato) accesso abusivo a un sistema, e l'art. 615 quater c.p. (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici). La "scoperta" delle vulnerabilità, infatti, non è una scoperta ma - al contrario - una vera e propria "ricerca".

Presuppone cioè un comportamento attivo del soggetto, che deliberatamente comincia ad eseguire attacchi non autorizzati su una piattaforma di produzione specificamente individuata. La differenza fra "scoperta" e "ricerca" è sottile ma non banale perché a seconda che ricorra l'una o l'altra condizione, cambia radicalmente lo scenario delle responsabilità giuridiche anche penali. Una vulnerabilità scoperta accidentalmente e comunicata alla "vittima" senza chiedere nulla in cambio è un atto equivalente a chiamare il 115 quando ci si imbatte in un incendio. Una vulnerabilità ricercata attivamente svolgendo attività sistematica nei confronti di un sistema è un attacco bello e buono.

2. Non è full disclosure

Per chiarire meglio questo ultimo concetto è utile spiegare perché la pubblicazione di una vulnerabilità che affligge una certa piattaforma in quanto tale non è illecita, mentre lo diventa quando il bug si riferisce a una specifica implementazione, in un particolare settore, in una macchina in produzione. Se, nel settore dei beni di consumo dimostro che un certo prodotto contiene delle sostanze tossiche nessuno potrà accusarmi di avere violato la legge. Allo stesso modo, se analizzo il comportamento di un sistema operativo e ne individuo un difetto che indebolisce il sistema, non posso essere considerato responsabile per il solo fatto di parlarne.

Altro discorso è se, invece di descrivere un problema di tipo generale, diffondo la notizia che il server della società XYZ è esposto ad attacchi cross-site scripting, fornendo anche istruzioni dettagliate per realizzare il "colpo". E' vero che anche la full disclosure (cioè, appunto, la diffusione di informazioni sulle vulnerabilità di sistemi operativi e applicazioni) va gestita in modo responsabile per evitare conseguenze spiacevoli. Dunque, se si scopre una vulnerabilità seria è impensabile evitare di avvisare immediatamente il produttore del software difettoso. E se si strumentalizza la scoperta si potrebbero anche passare dei guai giudiziari. Ma è anche vero che, legalmente, esiste una differenza sostanziale fra l'analisi teorica di un problema e l'attacco a un server pubblico. Anche perché non è affatto detto, in questo secondo caso, che la scoperta "casuale" della vulnerabilità sia necessariamente merito originale del "ricercatore indipendente". In altri termini, se il bug viene

scoperto con il semplice uso di strumenti di intrusione o con programmi che automatizzano gli attacchi, viene meno anche la "giustificazione" del voler fare ricerca. Non c'è contenuto scientifico nel lanciare un programma contro un'applicazione e aspettare per vedere cosa succede.

3. Scoppia il caso

Veniamo ora al momento critico: di punto in bianco, qualcuno della divisione sicurezza (o - nei casi di aziende più piccole - il webmaster del sito) trova in mailbox un messaggio che lo avvisa del problema. I toni sono, di solito, abbastanza amichevoli e collaborativi ma, nella sostanza, estremamente chiari: a seguito di una scoperta casuale il mittente della mail si è "imbattuto" in una vulnerabilità che potrebbe creare pericoli alla privacy dei clienti. Per fortuna che se ne è accorto lui che è bravo, perché se invece l'informazione fosse finita in altre mani chissà cosa sarebbe successo, e dunque sarebbe gentile che questa gentilezza fosse ricompensata in vario modo.

4. Reagire in sede giudiziaria

Di fronte a queste "scoperte" più o meno casuali, la reazione a caldo più frequente delle aziende interessate è quella di denunciare il fatto e cercare di ottenere l'eliminazione delle informazioni diffuse in rete. Sebbene questa sia una strada tecnicamente - in senso legale - percorribile, presenta delle criticità in termini di gestione dell'immagine aziendale. Il rischio, in altre parole, è sempre quello di creare un "martire/eroe" e di alimentare il concetto di "multinazionale cattiva". Il "ricercatore indipendente", infatti, si troverebbe in una posizione semplice da comunicare: "ho trovato un bug, ho dimostrato che l'ISP XYZ è vulnerabile e ora questo si vuole vendicare". Viceversa, l'azienda oggetto dell'estorsione, avrebbe qualche difficoltà in più a spiegare ai propri clienti in modo semplice il concetto che un conto è fare il "test dell'alce" su un'automobile dimostrando che si ribalta, e un'altra è "aggredire" abusivamente un servizio internet in produzione. In questo caso, una strada per attenuare l'impatto della notizia può essere quella di evidenziare il tentativo di strumentalizzazione da parte del "ricercatore", per esempio nel caso in cui prima che la vulnerabilità sia stata eliminata, questa venga resa pubblica. Circostanza che consentirebbe di dimostrare la volontà di provocare danni e non quella di cooperare per risolvere un problema. Quello che è certo, è che se l'azienda sceglie di perseguire legalmente il "ricercatore indipendente", non può permettersi di tornare indietro o di avere la mano leggera, ma deve assolutamente ottenere una condanna. L'effetto di una assoluzione o di una "marcia indietro" sarebbe peggiore del danno che si intendeva contrastare. Scegliere la via giudiziaria, comunque, richiede alcune cautele di tipo legale per evitare che il processo si trasformi un nulla di fatto. Se la vulnerabilità segnalata dal "ricercatore indipendente" è di quelle che consente l'accesso ai sistemi bersaglio, costui ha commesso un accesso abusivo che è sanzionato dall'art. 615 ter del codice penale. Questo reato - salve alcune eccezioni - è "perseguibile a querela". Ciò significa due cose: la prima è che bisogna rivolgersi alla magistratura entro novanta giorni dal momento in cui si scopre il fatto; la seconda è che - se la vittima è un'azienda - solo il legale rappresentante (o chi ha una procura speciale) può firmare la

querela. Se anche uno solo di questi due elementi viene trascurato è fortissimo il rischio che il responsabile del reato riesca a farla franca.

5. Negare il problema

Una cosa da evitare a meno di non essere assolutamente certi di avere tutto sotto controllo è la deniability; vale a dire la negazione del problema. Una volta messa a posto la vulnerabilità, infatti, si potrebbe semplicemente "fare finta di nulla". Ma - come sanno i servizi segreti di tutti i paesi - la deniability funziona se e solo se sono cancellate irrimediabilmente tutte le tracce del fatto che si vuole nascondere; perché altrimenti si rischierebbe di essere sbugiardati due volte (la prima per non essersi accorti della vulnerabilità, la seconda per avere cercato di negarla). Sono stati registrati casi, in Italia, di soggetti che - per vanificare l'insabbiamento della "scoperta" - addirittura si erano precostituiti la prova dell'esistenza della vulnerabilità con una una vera e propria perizia depositata in uno studio legale.

6. Il muro di gomma

Un'ultima opzione è quella di ignorare semplicemente il problema. Smorzatasi l'ondata di rumore eventualmente generata dalla notizia - e adottati quei provvedimenti disciplinari minimi che consentono di raffreddare gli animi - tutto ritorna come prima. Chi ricorda il rumore provocato dal bug dei modem Alcatel Speed Touch scoperto da Shimomura Tsutomu, quello dei router Telindus o il DRM-rootkit nascosto da SonyBMG in decine di titoli musicali?

IL CONCETTO IN PRATICA

* Chi entra in contatto con il "ricercatore indipendente" deve mantenere la calma, non fare commenti, e ottenere le generalità del "segnalante".

* La notizia deve essere immediatamente comunicata alla direzione affari legali, alle relazioni esterne, alla direzione sicurezza, ai responsabili del servizio attaccato.

* Prima di decidere l'approccio da utilizzare è necessario verificare se la vulnerabilità dipende dagli apparati in sé (es.: router difettoso, sistema operativo o applicazione con difetti non documentati), da errori di implementazione (es: mancato cambio delle password di default) o ancora da errori di amministrazione (es: mancata installazione di patch).

* Bisogna inoltre ottenere velocemente dati attendibili sul numero dei clienti potenzialmente affetti dal problema e sull'effettivo impiego della vulnerabilità, congelando - con una perizia indipendente - lo stato di fatto (a prescindere dal non uso che se ne dovesse fare).

* Può essere utile - in casi gravi - rivolgersi a società di relazioni pubbliche specializzate in crisis management per gestire in modo più efficiente il controllo delle informazioni e le strategie da adottare.

* Le relazioni esterne (quando esistono come struttura autonoma) e l'ufficio stampa devono essere immediatamente pronti a rilasciare dichiarazioni serie, concrete e non ambigue in modo da ridurre l'impatto della eventuale strumentalizzazione della notizia.

5. LUGANO: SECURITY DAY 2006

CLUSIS e CLUSIT hanno organizzato anche quest'anno il Security Day, evento di apertura del Lugano Communication Forum.
La manifestazione si svolgerà al Palazzo dei Congressi di Lugano il prossimo 11 aprile.

PROGRAMMA
SALA B1 - 10.00-13.00
Security Day 2006
Moderatore: Davide Gai, Presidente Gai&Partner

- **Benvenuto - Introduzione al convegno - Presentazione Clusis**.
  Paolo Giudice, C.D. Clusis (Associazione Svizzera per la Sicurezza dei Sistemi d'Informazione), Responsabile per la Svizzera Italiana
- **Più o meno sicuri? Nuovi segnali nella sicurezza delle informazioni**
  Gigi Tagliapietra, Presidente Clusit (Associazione Italiana per la Sicurezza Informatica)
- **La sicurezza nell'IP-Telephony (VoIP)**
  Simone Posti, NextiraOne
- **La gestione di un attacco di phishing da parte di un istituto bancario**
  Andrea Monti, Avvocato, C.D. Clusit
- Pausa Caffè
- **Alcune Basi Didattiche e Scientifiche per la Sicurezza Informatica**
  Antonio Carzaniga, Assistant Professor presso la Facoltà di Scienze informatiche, Università della Svizzera Italiana
- **Identity Management as prerequisite for secure end-to-end network based transactions**
  Hellmuth Broda, Dr. Distinguished Director and European Chief Technology Officer, Corporate Strategic Insight Office, Sun Microsystems, Inc.
- **Un nuovo approccio al Cybercrime: l'Hacker Criminal Profiling Project (HCCP)**
  Raoul Chiesa, C.D. e C.T.S. Clusit

La partecipazione è libera e gratuita.
È possibile riservare un posto in sala inviando una e-mail a info@clusit.it.

6. INFOSECURITY VERONA E ROMA

Sono state fissate date e tematiche dei convegni e dei seminari.

VERONA ♦ 9-10 maggio. La manifestazione è dedica in particolare alla Piccola e Media Industria ed alle Amministrazioni Locali.

Martedì 9 maggio - 10.30-12.30

Sessione di Apertura

Moderatore: Gigi Tagliapietra, presidente Clusit

Dopo una panoramica strategica su Storage e Sicurezza Informatica, a cura di Francesco Sacco (SDA Bocconi), si terrà una tavola rotonda riservata ai manager di alcune delle più importanti aziende, in diversi settori industriali, al fine di delineare le politiche d'investimento in Sicurezza Informatica e Storage.

Martedì 9 maggio - 14.30-17.00

La Sicurezza delle informazioni in azienda: Normative e Standard

Moderatore: Stefano Quintarelli, presidente AIIP (Associazione Italiana Internet Providers)

Nell'ambito di questo convegno, Gabriele Faggioli (Avvocato, CTS Clusit) illustrerà i principali vincoli normativi (DLGS 196/03, Data Retention...), e Riccardo Bianconi (SINCERT) farà una panoramica sulle proposte di standard internazionale (ISO 17799, ISO 27001, BS 7799) per effettuare la memorizzazione delle informazioni aziendali. Saranno poi presentate, attraverso l'esposizione di diversi casi di studio, alcune soluzioni pratiche.

Martedì 9 maggio - 10.30-17.00

Programmazione sicura

Seminario CLUSIT (gratuito per i soci)

Docente: Mattia Monga, Dipartimento di Informatica e Comunicazione - Università degli Studi di Milano, CD Clusit

Mercoledì 10 maggio - 10.30-13.00

Servizi e prodotti innovativi per la sicurezza ICT

Moderatore: Danilo Bruschi, Università degli Studi di Milano

Saranno presentate le principali novità nel settore della ICT security, nei comparti tecnologico e dei servizi sia insource che outsource. Particolare attenzione sarà posta ai prodotti più confacenti alla realtà delle piccole e medie imprese. Gigi Tagliapietra (presidente Clusit), interverrà sugli aspetti metodologici e Luca Marzegalli (Cefriel, Politecnico Milano) interverrà sull'evoluzione delle tecnologie di sicurezza, le novità e la ricerca. Attraverso i casi di studio saranno poi presentate realtà aziendali che hanno recentemente fatto ricorso a detti prodotti e servizi.

Mercoledì 10 maggio - 14.30-17.00

La Sicurezza delle informazioni in azienda: Prodotti e architetture

Moderatore: Francesco Pignatelli, IDG

Saranno analizzate le nuove proposte in termini tecnologici legate alla memorizzazione delle informazioni in azienda sottolineando l'impatto di queste nuove tecnologie sulla Sicurezza ICT nel suo complesso. È previsto l'intervento di un esperto di storage, che tratterà della standardizzazione delle tecnologie e degli approcci nel mondo storage, oltre che del peso che le tecnologie di storage hanno sulle prestazioni della rete aziendale. Ci sarà poi l'intervento di un esperto di security in ambito storage. Seguiranno alcuni casi di studio, che mostreranno le applicazioni concrete di tali tecnologie.

ROMA ♦ 20-21 giugno. La manifestazione è dedicata in particolare a: Amministrazione Centrale, Amministrazioni Locali, Telcom, Finance.

Martedì 20 giugno - 10.30-12.30

Sessione di Apertura

Quale governance per la Sicurezza ICT nel nostro paese?

Sarà una tavola rotonda con soli relatori istituzionali in cui saranno invitati gli attori nuovi e vecchi della governance della Sicurezza ICT in Italia (Ministero delle Comunicazioni, Autorità Garante per la protezione dei dati personali, Presidenza del Consiglio dei Ministri, Ministero dell'Interno, Confindustria, Confcommercio) con lo scopo di indicare un'agenda per il nostro paese in tema di sicurezza ICT.

Martedì 20 giugno - 14.30-17.00

La sicurezza ICT nella PA

Nell'ambito di questo convegno si farà il punto, attraverso i casi di studio, su progetti e iniziative in corso nell'ambito della PA (centrale e locale) relative al tema Sicurezza ICT. I relatori istituzionali illustreranno invece le iniziative a medio e lungo termine che coinvolgeranno le PA.

Mercoledì 21 giugno - 10.30-17.00

Web Application Security: linee guida per la progettazione e l'audit di sicurezza degli applicativi

Seminario CLUSIT (gratuito per i soci)

Docenti: Matteo Meucci e Alberto Revelli

Mercoledì 21 giugno - 10.30-13.00

Soluzioni Tecnologiche per la Sicurezza ICT nelle grandi organizzazioni

Nel corso di questo convegno, i relatori istituzionali proporranno una serie di problematiche tecnologiche per realizzare la sicurezza ICT in una grande organizzazione (sia pubblica che privata). Attraverso i casi di studio si cercherà di mostrare soluzioni tecnologiche in cui alcuni problemi di sicurezza di grandi organizzazioni sono stati risolti.

Mercoledì 21 giugno - 14.30-17.00

I servizi di supporto alla security governance

Saranno presentate ed analizzate le problematiche relative alla gestione della Sicurezza nell'ambito di grosse organizzazioni (sia pubbliche che private), toccando anche temi di attualità come certificazioni, Business continuity e Basilea2. Nei casi di studio si presenteranno soluzioni a supporto della governance della Sicurezza e realtà in cui queste soluzioni sono state applicate .

Mercoledì 21 giugno - 10.30-17.00

All'interno di Infosecurity Roma si terrà la ISSA European Security Conference, organizzata da AIPSI, capitolo italiano di ISSA.

7. NOTIZIE DAI SOCI

Il Dipartimento di Informatica de "La Sapienza", al termine del Master in Sicurezza dei sistemi e delle reti informatiche, ha organizzato un convegno dal titolo "La sicurezza dell'informazione: fattori critici", che si terrà il prossimo 5 aprile, alle ore 9.00, presso il Centro Congressi dell'Università di Roma "La Sapienza" - Via Salaria 113 - Piano Terra.

Scopo dell'incontro è offrire agli allievi del Master, a studiosi ed operatori del settore, un'approfondita panoramica sullo stato dell'arte della sicurezza dell'informazione, dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione. Nell'ambito dell'evento, alla presenza del Magnifico Rettore, Prof. Renato Guarini, alle 11.45, è prevista la cerimonia di consegna dei primi Diplomi di Master.

La partecipazione al convegno è gratuita ed è consentita, tramite iscrizione, fino all'esaurimento dei posti disponibili.

Maggiori informazioni sono disponibili su
http://mastersicurezza.uniroma1.it

8. SEMINARI CLUSIT EDUCATION

Sono aperte le registrazioni al seminario di MAGGIO a Milano.

Crittografia Moderna: Teoria e Pratica
MILANO 4 maggio 2006

Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form.pdf
Per i Soci Clusit la partecipazione è gratuita*
La partecipazione al seminario riconosce 8 crediti/ore CPE

PROGRAMMA

- **Mattina**

1. Introduzione alla crittografia ed agli algoritmi crittografici

1.1 generalità sulla crittografia e suoi utilizzi
1.2 principi di funzionamento: chiavi, testi, numeri casuali, algoritmi, protocolli
1.3 algoritmi più semplici: Cifrario di Cesare, One-Time-Pad
1.4 crittoanalisi del Cifrario di Cesare
1.5 algoritmi Simmetrici, Asimmetrici e Hash

2. Algoritmi Simmetrici

2.1 algoritmi Simmetrici: blocchi, stream
2.2 noti algoritmi Simmetrici
2.3 breve rassegna dei principi di funzionamento di DES
2.4 cenni su AES

3. Algoritmi Asimmetrici e di Hash

3.1 algoritmi Asimmetrici: principi generali
3.2 introduzione alla matematica di RSA

3.3 uso delle chiavi pubbliche e private
3.4 algoritmi di Hash e MAC

4. Utilizzo degli algoritmi crittografici
4.1 cifrare con algoritmi Simmetrici
4.2 cifrare con algoritmi Asimmetrici
4.3 firma digitale ed autenticazione
4.4 utilizzo congiunto degli algoritmi

- **Pomeriggio**

5. OpenPGP: teoria e pratica
5.1 Introduzione a OpenPGP: storia e concetti fondamentali
5.2 La gestione delle chiavi PGP, keyserver e web-of-trust
5.3 Il formato dei documenti cifrati e/o firmati
5.4 Esempi pratici di firma e cifratura di documenti
5.5 PGP e la posta elettronica

6. CA, PKI e Openssl
6.1 Cosa sono i certificati digitali
6.2 CA e PKI
6.3 Creare una CA con Openssl
6.4 Creare certificati digitali con Openssl
6.5 Gestire certificati digitali e CRL con Openssl

7. Esempi di Applicazioni di Certificati Digitali
7.1 La navigazione web cifrata, analisi di una connessione
7.2 Effettiva sicurezza della navigazione web e PKI
7.3 Stunnel, OpenVPN ed altri esempi

Agenda:
- 08,50 registrazione e consegna del materiale didattico
- 09,10 inizio seminario
- 10,50 coffe break
- 11,10 ripresa seminario
- 12,50 termine della sessione del mattino
- 13,00-14,00 buffet
- 14,10 inizio sessione pomeridiana
- 15,50 coffe break
- 16,10 ripresa seminario
- 17,50 termine del seminario

Docenti: Andrea Pasquinucci, Lorenzo Cavallaro
Luogo: StarHotel Splendido - Viale Andrea Doria, 4

*Condizioni e modalità di iscrizione per Soci e non soci su www.clusit.it/edu

9. EVENTI SICUREZZA

3-5 aprile 2006, Parigi
17° EUROSEC - Forum Européen sur la Sécurité des Systèmes d'Information
www.xpconseil.com/eurosec2006

4 aprile, Roma ♦♦♦♦ **POSTI ESAURITI** ♦♦♦
Seminario CLUSIT "Phishing: profili tecnici e legali. Tecniche di prevenzione e casi pratici"
www.clusit.it/edu

6 aprile, Firenze
"Panorama sulle Certificazioni professionali nella Sicurezza delle Informazioni"
www.sicurinfo.it/informazioni/visinf.asp?IDInfo=232&CAT=53

11 aprile, Lugano
CLUSIS e CLUSIT presentano il Security Day 2006, Convegno di apertura del Lugano Communication Forum
www.gaiandpartner.com/ma_lcf2006.asp

29 aprile 2006, Roma
Esame CISSP
www.clusit.it/isc2

4 maggio, Milano
Seminario CLUSIT "Crittografia Moderna: Teoria e Pratica"
www.clusit.it/edu/index.htm#CR02

9-10 maggio, Verona
Infosecurity Italia 2006
www.infosecurity.it/Verona/index.php

9 maggio, Verona (nell'ambito di Infosecurity)
Seminario CLUSIT "Programmazione sicura"
www.clusit.it/edu/index.htm#PR01

12 maggio, Firenze
Convegno in tema di sicurezza informatica nell'ambito della manifestazione "VIVERE SICURI" (12-14 maggio)
www.viveresicuri.it/infor.htm

25 maggio, Roma
Seminario CLUSIT "Crittografia Moderna: Teoria e Pratica"
www.clusit.it/edu/index.htm#CR02

20-21 giugno, Roma
Infosecurity Italia 2006
www.infosecurity.it/Roma/index.php

21 giugno, Roma (nell'ambito di Infosecurity)
Seminario CLUSIT "Web Application Security: linee guida per la progettazione e l'audit"
www.clusit.it/edu/index.htm#WG01

22 giugno, Milano
Seminario CLUSIT "Aspetti legali della sicurezza informatica: lo stato dell'arte"
www.clusit.it/edu/index.htm#CF02

6 luglio, Roma
Seminario CLUSIT "Aspetti legali della sicurezza informatica: lo stato dell'arte"
www.clusit.it/edu/index.htm#CF02

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