Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- ENAV - Società Nazionale per l'Assistenza al Volo (Roma)
- UNICRI - United Nations Interregional Crime and Justice Research Institute (Torino)

2. SECURITY SUMMIT 2009

È confermata la partecipazione dei primi due keynote Speaker che interverranno al Security Summit di Milano (24-26 marzo 2009): Gadi Evron e Steve Santorelli.

Gadi Evron ha fatto le sue prove nel campo delle Internet Security Operations ed è uno dei massimi esperti in materia di botnet. Riconosciuto come esperto nel settore della Corporate Security, controspionaggio e cybercrime (e-fraud e phishing), ha fondato il CERT del governo israeliano. Si è fatto conoscere in particolare quando ha aiutato il governo dell'Estonia a difendersi dall'attacco informatico subito nel 2007 (vedi www.itnews.com.au/News/76651,expert-dissects-estonian-cyberwar.aspx). Un profilo più esteso è disponibile su www.linkedin.com/in/gadievron.

Steve Santorelli è uno dei maggiori esperti mondiali in tema di investigazioni in rete e di Internet Crime.
Diventa ufficiale di polizia nel 1994, lavorando inizialmente ad Hackney nell'East London, entrando nella Computer Crime Unit di Scotland Yards nel 2000. Dopo 5 anni, durante i quali si è specializzato in casi di malware e botnet, Steve ha lasciato il mondo del law enforcement per unirsi all'Internet Crimes Investigation Team di Microsoft a Redmond, USA. Nei successivi due anni ha investigato su casi relativi a botnet, per poi riportare a polizie in tutto il mondo, definendo il

lavoro necessario per arrivare agli arresti. Circa 18 mesi or sono Steve ha lasciato Microsoft per Team Cymru, un piccolo gruppo di ricercatori, ingegneri ed investigatori che si occupano di indagini sull'Internet Crime. In questi mesi Steve ha lavorato nell'istruttoria di casi estremamente rilevanti contro alcune delle più note organizzazioni criminali presenti oggi su Internet.

Ci è stata poi confermata la presenza di un tecnico di gran valore: **Piotr Oleszkiewicz**, che sarà uno dei docenti del Percorso professionale "tecnico" del Summit.
Piotr gestisce il security team presso Surfland Systemy Komputerowe S.A. (Polonia) ed è il fondatore della società di consulenza SentiNode.
Laureato alla Technical University di Wroclaw con un master in computer science, Piotr ha un forte background nel networking, nella crittografia, nel software design e nell'information security, con oltre 12 anni di esperienza sul campo nell'amministrazione dei sistemi e nelle architetture di rete.

Un quarto ospite, dall'estero, sarà **Claude Maury**, presidente del Clusis (la nostra consorella svizzera, che nel 2009 festeggerà i suoi 20 anni). Claude Maury, che sarà il docente principale del Percorso professionale sulla "gestione della sicurezza" del Summit, ha alle spalle un'esperienza professionale di tutto rispetto.
Claude ha iniziato ad occuparsi di elaborazione dell'informazione nel 1962 a Lausanna su degli IBM 609 e IBM 407. In seguito è entrato in DuPont de Nemours International, un colosso multinazionale della chimica. In questa azienda si è occupato, negli USA, di programmazione, analisi ed elaborazione di sistemi informatici ed ha messo in piedi e gestito, in Europa, una rete di telecomunicazioni di tipo x.25. Nel 1982, è stato nominato responsabile del centro informatico europeo (35 persone) con un budget annuale di 22 milioni di USD (di allora!). È proprio presso DuPont de Nemours che ha sviluppato, ad alto livello, le sue competenze in materia di sicurezza fisica, tecnologica ed organizzativa. Nel 1991, è passato alla società Firmenich di Ginevra, una multinazionale svizzera nel settore dei profumi ed aromi, per la quale ha messo in piedi una infrastruttura di rete IP e di servizi per le 32 filiali internazionali della compagnia (3.500 utenti). È poi rimasto fino al 2002 come responsabile IT (72 persone) per l'Europa, l'Africa ed il Medio-Oriente. Dal 2003, ha svolto diversi incarichi consulenziali in materia di audit, sensibilizzazione e organizzazione nell'ambito della sicurezza dei sistemi informatici, come pure in materia di integrazione della sicurezza nella gestione dei servizi IT secondo ITIL. Insegna sicurezza informatica all'Università di Ginevra e tiene regolarmente dei seminari sull'utilizzo delle norme ISO 2700x, rivolti ai Chief Information Security Officer (CISO) di aziende di diversi settori.

3. LA CRISI ECONOMICA ED IL SETTORE ICT

Abbiamo appena assistito al convegno Assinform su "Congiuntura economica e sviluppo del Paese: l'IT italiano come opportunità di sistema", che si è tenuto nella sede di Assolombarda a Milano.

È stata presentata un'analisi dettagliata dei dati relativi all'andamento del 2008 ed alle prospettive per il prossimo anno. Per il 2009, più che azzardarsi in

previsioni, Giancarlo Capitani, che ha presentato il rapporto, ha dato indicazioni molto interessanti sulle opportunità e le criticità proprie del settore IT.

Molte le richieste rivolte alle Istituzioni dal Presidente Lucarelli, dal Presidente di Confindustria Servizi Innovativi e Tecnologici Alberto Tripi e dal Presidente di Confindustia Emma Marcegaglia: il rispetto dei termini di pagamento da parte della P.A., l'intervento presso il sistema bancario perchè faciliti (e non renda più difficile, come sta facendo) l'accesso al credito, l'avvio di opere infrastrutturali indispensabili per il rilancio del sistema paese, in particolare la banda larga.

Il video del convegno è disponibile su http://assinform.dolmedia.tv

Usciamo dal convegno con l'impressione che le aziende del settore, e soprattutto le PMI, hanno veramente voglia di innovare, di continuare a investire e anche di conquistare nuovi mercati. Si è trattato di una buona iniezione di ottimismo e, in questi tempi, non può che far bene.

4. I "MITI" DELLA SICUREZZA

Trovo assai interessante ed istruttivo questo articolo di Network World: www.networkworld.com/news/2008/110608-security-myths.html

che riunisce alcuni dei principi sui quali, a ragione o a torto, si basa larga parte della sicurezza informatica, e li sottopone ad una sana ed utile critica da parte di un gruppo di esperti.

Le persone intervistate sono di alto livello, e senz'altro la loro opinione è estremamente valida e da tenere in considerazione.

Mi permetto inoltre di aggiungere anche il mio personalissimo parere, invitando esplicitamente tutti i lettori a lasciare il proprio su http://blog.clusit.it/sicuramente/2008/11/i-miti-della-si.html.

1. C'è sicurezza nell'occultare (security through obscurity).
   Questo principio mi fa pensare a molte situazioni dove è l'unica contromisura adottata, ed in questi casi è chiaramente da scartare - il fatto che nessuno conosca il mio algoritmo di crittografia non lo rende automaticamente sicuro, anzi.
   Per contro, non c'è dubbio che alcune cose vadano tenute riservate e con la massima cautela (le password, i PIN, le configurazioni di dettaglio, ecc.).
2. Il software Open Source è più sicuro di quello proprietario.
   Così come è detta, questa frase è falsa. Che però il software O.S. sia potenzialmente più sicuro di quello proprietario è senz'altro vero, perché ci sono più occhi che lo possono esaminare e statisticamente ci saranno anche più occhi esperti.
   Nella pratica, poiché è un principio statistico, vale sui grandi numeri, e nulla si può inferire sul caso singolo.
3. La misura dell'aderenza a leggi e regolamenti è un buon metro della sicurezza.
   In Italia probabilmente no: anche solo l'esistenza di un proverbio come "fatta la legge, trovato l'inganno" ci svela la pervasività in ciascuno di noi

dell'abitudine ad eludere le leggi, ed azzera di fatto il valore della compliance formale come misura dell'efficacia sostanziale.
Portiamo ad esempio le migliaia di DPS che non hanno migliorato di fatto la tutela dei dati personali.

4. Non è possibile misurare il ritorno d'investimento (ROI) della sicurezza.
   Probabilmente questo non è vero in assoluto, ma senz'altro è molto difficile. Nel caso generale, non conosco alcun modo per farlo in maniera tale che i numeri che ne escono abbiano un qualche significato.
   Esistono tuttavia alcuni casi particolari in cui ciò è possibile, per cui non perdo la speranza che prima o poi si riesca a sistematizzare la materia e generalizzare il calcolo.

5. La mafia russa è colpevole dei peggiori reati online.
   Sinceramente non credo. I più pervicaci spammer, ad esempio, sono americani (degli USA, intendo).
   La regola del vantaggio, peraltro, richiede che chi commette un crimine lo faccia per averne un tornaconto, e quindi la mafia russa sarà coinvolta in tutti - e soli - i casi in cui potrà trarre denaro dallo specifico crimine, o direttamente o indirettamente perché commissionatole da qualcun altro. Ma in questo secondo caso ovviamente potrebbe essere chiunque (perché solo la mafia russa, e non quella giapponese, o Cosa Nostra?).

6. Un antivirus è indispensabile per prevenire il malware.
   Qualche anno fa questa regola era senz'altro molto più valida di oggi.
   Attualmente il numero di virus "tradizionali" è drasticamente diminuito, sostituito da qualcosa di assai più redditizio per chi lo scrive che è lo spyware, e lo spam che indirizza su siti di phishing, che se non è spyware tecnicamente in pratica ha gli stessi fini.
   Quindi, se per antivirus si intende software che protegga in generale da queste minacce, sicuramente sì; se si intende il solo tradizionale schermo da "programmi infetti", allora è ormai quasi inutile.

7. L'outsourcing della sicurezza pone più rischi che gestirlo in casa.
   Questo è in generale falso: basti un controesempio.
   Quando la gestione della sicurezza è "casalinga" le persone sufficientemente influenti riescono di solito ad ottenere assai rapidamente eccezioni alle regole generali.
   Quando si va in outsourcing l'inserimento di eccezioni viene molto rallentato, perché il singolo operatore richiede (saggiamente) un'autorizzazione prima di procedere; quando poi - generalmente dopo un escalation - l'eccezione viene inserita, l'azione viene documentata.
   Si può quindi argomentare che in questo caso l'outsourcing aumenta la sicurezza (a prezzo della flessibilità, ovviamente, e quindi l'effetto netto sul risultato aziendale può essere positivo o negativo).

8. La biometria è il miglior sistema di autenticazione.
   Nella mia esperienza, poiché due volte su tre il lettore biometrico non funziona (perché non riconosce l'impronta digitale, o la confonde con quella di qualcun altro, ecc.), oppure è assai scomodo da usare (perché bisogna avvicinare l'iride al sensore, oppure richiede di rimanere immobili, ecc.), l'utente tipico si stanca assai rapidamente del sistema.

L'utente stufo cerca mezzi (di solito procedurali) di aggirare il sistema.
Poiché nessun sistema è perfetto, generalmente ci riesce.
=> diminuzione della sicurezza.
Ciò mi porta a dire che la biometria non è un buon sistema di autenticazione.

9. I certificati digitali identificano un sito Web.
In generale sì, ma non solo.
Peraltro, identificano "qualcosa" o "qualcuno" solo perché certificano (in un modo assai difficile da contraffare) che quello che c'è scritto al loro interno non è stato alterato da quando è stato scritto.
Quindi, se chi ha prodotto il certificato è affidabile - e lo si deve sapere per altre vie - allora l'informazione contenuta nel certificato è affidabile.

10. È possibile formare i dipendenti ad adottare comportamenti sicuri ed a resistere ai tentativi di social engineering su Internet.
Sì, è possibile, ma lo si fa assai poco. Questo tipo di allenamento dovrebbe anzi partire molto prima, probabilmente nella scuola dell'obbligo.
I bambini di oggi probabilmente cresceranno con un tipo di mentalità che contempla anche queste cautele (l'equivalente moderno del "non accettare caramelle dagli sconosciuti"), ma gli adulti di oggi non la hanno naturale.
Ciò detto, nessuna formazione può dare la certezza che nessun tentativo di social engineering funzionerà. Anche 007 ogni tanto cade nelle trappole delle fascinose spie che sembrano incontrarlo per caso al bar.

11. Non preoccupatevi, il governo (USA) ha un sistema segreto di difesa dagli attacchi informatici.
Questa frase mi ricorda un po' Mussolini che credeva nelle famigerate armi segrete di Hitler.
Non che non ci fossero (erano le V1 e le V2 di Von Braun): soltanto che non si sono dimostrate sufficienti.
Credo che anche in questo caso la situazione sia simile.

12. Più è lunga la chiave (di crittografia), più è sicuro il messaggio cifrato.
A parità di algoritmo, senz'altro è vero.
Confrontando algoritmi diversi, ovviamente no.

Autore. Mauro Cicognini

5. ANCHE I CHIMICI PENSANO ALL'ICT SECURITY

American Chemistry Council patrocina un programma per la cyber security awareness per le minacce di tipo informatico e stila linee guida per messa in sicurezza dei sistemi utilizzati.
Finalmente, a sei anni di tempo dal primo sforzo da parte di uno sparuto gruppo di specialisti, guidati da Eric Cosman (ex-Dow Chemical, ora Direttore ISA di Standard & Practices e chairman del comitato ISA s99 per la security nel manufacturing), preoccupati per la salute dei sistemi utilizzati nell'industria chimica, oggi più di 30 tra le maggiori industrie USA del settore hanno deciso che è meglio essere preparate ad affrontare in modo adeguato i rischi informatici.
Per saperne di più: www.automationworld.com/webonly-4822

Autore: Enzo M. Tieghi

6. CYBERCRIME

Riportiamo una notizia apparsa recentemente sul Corriere della Sera.

"Un detenuto romeno primo al test da ingegnere all'Università. Il ragazzo è in cella per aver svuotato via Internet il conto di un vincitore del Superenalotto.

Si può vincere all'Enalotto in tanti modi: rubando in banca su Internet i soldi che la ruota della fortuna ha appena regalato a qualcun altro, oppure afferrando dal carcere l'opportunità dell'unica vera lotteria costituita dall'autorealizzarsi in una vita nuova e onesta."

Leggi il seguito su:
www.corriere.it/cronache/08_ottobre_31/detenuto_romeno_universita_daa8632c-a716-11dd-90c5-00144f02aabc.shtml

7. SEMINARI CLUSIT

L'ultimo seminario Clusit Education dell'anno, che si è già tenuto a Milano, si replicherà a Roma l'11 dicembre e ci sono ancora posti disponibili.

11 dicembre 2008, Roma

RFID e NFC: aspetti di sicurezza nelle applicazioni reali

Scheda informativa del seminario:
https://edu.clusit.it/scheda_seminario.php?id=31

La partecipazione e' gratuita e riservata ai Soci Clusit.
Per partecipare e' necessario registrarsi online su:
https://edu.clusit.it

Per il 2009 abbiamo previsto ben 10 seminari Clusit Education, che si terranno come al solito sia a Milano che a Roma.

Il programma sarà presentato alla prossima assemblea dei soci del 15 dicembre e ne sarà data comunicazione anche nella newsletter di fine anno.

8. 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

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

Quest'anno il corso sarà dedicato alla mobile forensics, con particolare attenzione alle questioni informatico-giuridiche relative al trattamento dei telefoni cellulari, delle console, degli iPod, dei PDA e alla forensics aziendale.

Come tradizione, il corso si occuperà, ad alto livello, sia degli aspetti giuridici sia di quelli informatico/operativi. Le lezioni si terranno SOLO il giovedì pomeriggio dalle 14 alle 19 presso la sede centrale in via Festa del Perdono, dal 15 gennaio al 30 aprile 2009. La frequenza è obbligatoria per circa 70 ore di lezione, ed è prevista una prova finale. Sono ammessi iscritti laureati in qualsiasi disciplina, anche triennalisti. Il costo è stato contenuto in 1.000 euro, il numero massimo di partecipanti è 50. Non sono ammessi uditori o studenti non laureati, né sono previste quote speciali per particolari categorie. Il termine per le iscrizioni, che si possono effettuare anche online, è il 10 dicembre.

E' in corso la procedura di accreditamento presso il Consiglio dell'Ordine degli Avvocati di Milano.

Il bando per l'ammissione al corso è disponibile all'indirizzo
www.unimi.it/studenti/corsiperf/5411.htm#c32320.

Locandina e programma sono disponibili all'indirizzo
http://infogiure.typepad.com

È stato rinnovato l'accordo con la società BSI Management Systems www.bsigroup.it che prevede uno sconto del 20% su tutti i loro corsi (in particolare ISO 27001, ISO

20000 e BS 25999) per i soci Clusit. Per informazioni sui corsi, scrivere a sales.italy@bsigroup.com

---

È stato siglato un accordo con TÜV Italia www.tuv.it che prevede per i soci Clusit uno sconto minimo del 25 % sui Corsi per auditor/lead auditor per i Sistemi di Gestione per la sicurezza delle informazioni IT- ISO/IEC 27001:2005. Per informazioni e iscrizioni ai corsi scrivere a tuv.formazione@tuv.it o telefonare a Chiara Villani (Divisione Akademie TÜV Italia) allo 051 2987417.

Il Dipartimento di Informatica dell'università di Verona ha il piacere di invitarvi Mercoledi' 10 dicembre 2008 alle ore 14.00 ad un pomeriggio dedicato alla sicurezza informatica. Interverranno: Gigi Tagliapietra (Presidente CLUSIT) su "Quali talenti per la security: la lezione di JPGR", Alessio Pennasilico (Alba ST S.r.l.) su "VoIP (in)security: Italians do it better" e Antonio Ruzzelli (University College Dublin) su "Sensori wireless in ambienti residenziali e industriali".

Per maggiori informazioni:
www.di.univr.it/dol/main?ent=iniziativa&id=2143&lang=it

9. EVENTI SICUREZZA

2-4 dicembre 2008, Roma
Broadband Business Forum
www.bbfeurope.com

10 dicembre 2008, Verona
Seminario su VoIP, Sicurezza e Reti di Sensori
www.di.univr.it/dol/main?ent=iniziativa&id=2143&lang=it

11 dicembre 2008, Roma
Seminario Clusit - RFID e NFC: aspetti di sicurezza nelle applicazioni reali
https://edu.clusit.it/scheda_seminario.php?id=31

11 dicembre 2008, Pisa
Real Life Security: quando gli hackers diventano professionisti
www.atsystem.org/it/attivita/real+life+security

11-12 dicembre 2008, Dublin
EC2ND 2008: European Conference on Computer Network Defense
www.ec2nd.org

19 dicembre 2008, Mestre -VE
La Gestione della Continuità operativa
www.clusit.it/eventi/081219_aicq.pdf

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