Indice

1. NUOVI SOCI

Hanno aderito al CLUSIT le seguenti organizzazioni:

- BIT Sistemi (Gioia Del Colle - BA)
- NerInformatica (Romano D'Ezzelino - VI)
- Novell Italia (Sesto S. Giovanni - MI)
- Ring Zero - (Monterotondo - RM)
- T.E.S.I. (Firenze)

2. INFOSECURITY MILANO - BILANCIO POSITIVO

L'edizione 2006 di Infosecurity si è caratterizzata per un'ottima affluenza, non solo presso gli stand, ma soprattutto presso le sale dove si svolgevano incontri e tavole rotonde. Segno che sta aumentando il numero dei professionisti in ambito ICT che desiderano approfondire le tematiche legate alla sicurezza, e utilizzano eventi molto profilati come questo per trovare occasioni di scambio e incontro. Crediamo che sempre di più il successo di un evento dipenda dalla qualità dei dibattiti, perché c'è bisogno di contestualizzare le soluzioni, che si trovano poi nell'area espositiva, con lo stato dell'arte della ricerca.

"THE FUTURE OF COMPUTER SECURITY"

Thomas E. Noonan, Presidente e CEO di Internet Security System, Dan Sarel, Director of Product Management di Check Point Software Technologies e William Beer, Director di Symantec Security Sevices, Southern Region sono stati, insieme al professor Danilo Bruschi, Presidente Onorario del CLUSIT, i protagonisti di una Tavola Rotonda che si è tenuta nella giornata inaugurale della manifestazione.

Numerosissimi i presenti, che hanno seguito le tre personalità in un percorso virtuoso che ha presentato le nuove frontiere della sicurezza digitale.

L'incontro, organizzato dal CLUSIT, aveva proprio lo scopo di suscitare interrogativi e stimolare il confronto. È emersa infatti, come prioritaria, la necessità di una collaborazione molto più ampia tra le aziende fornitrici di sistemi per la sicurezza: diventando sempre più articolata la minaccia,

occorre infatti che anche i sistemi di difesa collaborino per la totale security del cliente.

Diversi gli spunti che i partecipmti alla Tavola Rotonda hanno lasciato alla platea:

- I "semplici" antivirus, da soli, non sono più efficaci. Occorrono oggi soluzioni "complessive" di sicurezza aziendale. "Gli attacchi, ormai - spiega Dan Sarel, Check Point Software Technologies - puntano non solo a distruggere i sistemi, ma a carpire informazioni, boicottarle, rivenderle. Un sistema protetto, ma non strutturato, può non essere sufficiente".

- Spesso le aziende si ritrovano a "presumere" di avere sistemi di security efficaci. Ha spiegato William Beer, Symantec Security Sevices: "C'è questo falso senso di sicurezza che contraddistingue molte imprese, che magari possiedono sistemi perfetti di sicurezza, ma non li utilizzano in tutte le potenzialità a disposizione".

- Temi come il phishing e la diffidenza persistente nei confronti del pagamento on line, devono essere combattuti, ma allo stesso tempo le aziende fornitrici di sicurezza devono garantire tempi di risposta agli attacchi sempre più brevi.

- L'allargamento delle tematiche legate alla sicurezza deve portare, secondo Thomas E. Noonan, che fa parte del National Infrastructure Advisory Council (NIAC) - iniziativa statunitense per la difesa nazionale - a una: "Visione sistematica della sicurezza, olistica. Posto che ormai le infrastrutture di security esistono, è necessario allargare la visuale. Inglobare, nei sistemi di sicurezza, interno ed esterno delle aziende, le relazioni con la clientela, i device a disposizione.

L'optimum, ma la strada è ancora lontana, sarebbe quella di riuscire a far comunicare i prodotti dedicati alla sicurezza tra loro, renderli interoperabili".

Danilo Bruschi ha così riassunto i trend dell' ICT Security:

L'hacking ludico che aveva caratterizzato i primi anni dell'era Internet sta oramai cedendo il posto agli attacchi mirati e fraudolenti ad opera di grosse organizzazione criminali, che con i mezzi di cui dispongono sono in grado di predisporre intrusioni sempre più sofisticate ma soprattutto sempre più difficili da rilevare. In questo contesto è necessario un salto di qualità nei sistemi di sicurezza che oltre ad estendere e raffinare il proprio dominio di controllo devono dotarsi di quella che viene chiamata in gergo "Security Intelligence", intesa come la capacità di anticipare o rilevare tentativi di intrusione in un sistema, attraverso l'individuazione e correlazione di eventi derivanti da fonti diverse, non necessariamente correlate alla natura del problema.

IL PREMIO CLUSIT PER LA MIGLIORE TESI IN SICUREZZA INFORMATICA

Nel corso della manifestazione di chiusura il CLUSIT ha presentato il vincitore del Premio Tesi di Laurea "Innovare la sicurezza delle Informazioni", edizione 2006. Il Premio, che si propone di incentivare gli studenti a confrontarsi con i temi dell'ICT Security, ha visto la partecipazione di universitari provenienti dai maggiori atenei italiani: Politecnico di Torino, Ca' Foscari di Venezia, Università Cattolica sede di Brescia, Università degli Studi di Milano Statale, Università

degli Studi di Torino, Università di Cagliari, Firenze, Padova, Bologna, l'Aquila, Modena e Reggio Emilia, Roma Tre e Politecnico di Milano.

Il Premio ha dato modo agli studenti di affrontare diversi temi cari alla Security, dalla sicurezza di rete all'analisi statica e dinamica del codice, dalla criptografia quantistica al conditional access per il digitale terrestre. La valutazione è stata effettuata da una commissione composta da membri del comitato direttivo e dal comitato tecnico scientifico del CLUSIT, provenienti sia del mondo accademico che industriale. Sono state premiate maggiormente l'innovatività dell'argomento trattato, la complessità dell'attività svolta, il livello di conoscenza dimostrato e l'utilizzabilità dei risultati raggiunti.

Il vincitore è risultato essere Piergiorgio Venuti, del Politecnico di Torino, con una tesi dal titolo: "Configurazione automatica di sicurezza degli apparati di rete", che ha sviluppato un sistema di distribuzione delle policy di sicurezza per un router, pix o switch Cisco, studiando e realizzando anche una soluzione che permettesse di proteggere la comunicazione tra la postazione di gestione e gli apparati di rete.

Questi gli studenti arrivati tra i primi cinque:

Daniele Bianco, dell'Università degli Studi di Torino, con la tesi "Sviluppo di un applicativo per l'analisi dei ritmi di battitura al calcolatore";

Matteo Ferrara, dell'Universita di Bologna, con la tesi: "Sviluppo di un dispositivo crittografico per la firma digitale con autenticazione biometria";

Pietro Ferrara, Ca' Foscari di Venezia, con la tesi "Development of a static analyzer for object oriented languages and application to the firewall analysis of JavaCard";

Emanuele Sindoni, del Politecnico di Milano, con la tesi: "Model driven development of secure Web Service applications".

Anche il 2006 vedrà una nuova edizione del Premio, con il sostegno di Fiera Milano International e del MIUR.

Il CLUSIT dedicherà alle Tesi in modo permanente una sezione del sito web, per permettere agli studenti di segnalare l'intenzione di svolgere tesi di sicurezza informatica e alle aziende di suggerire le tematiche di maggiore interesse.

CAPTURE THE FLAG

Sono stati presentati i risultati di "Capture the flag", primo campionato nazionale di hacking, edizione 2005. Sono intervenuti i componenti della prima squadra classificata, che hanno potuto commentare brevemente l'esperienza di "hackerare" le macchine del nemico e allo stesso tempo proteggere le proprie.

La competizione, organizzata dal CERT-it, si ripeterà ogni anno, con il sostegno di CLUSIT e di Fiera Milano International.

La finale della prossima edizione di "Capture the flag" sarà organizzata in forma spettacolare nell'ambito del prossimo salone Infosecurity, a Milano.

Per consentire al pubblico di accedere alle informazioni relative all'esperienza dell'hacking, è in preparazione un Quaderno con il resoconto dettagliato dello svolgimento della prima edizione della gara,

compresi ovviamente tutti gli aspetti tecnici e le strategie adottate sia in fase di attacco che di difesa.

LA RICERCA EUROPEA

Con Infosecurity Milano si è conclusa la raccolta dei dati italiani per la ricerca europea, voluta dalla Commissione Europea e dall'ENISA, sulla preparazione delle aziende ai rischi informatici. Lo studio, realizzato da Unisys e Rand Europe, è stato condotto nei 25 Stati Membri e CLUSIT si è occupato della parte italiana.

Per ringraziare coloro che hanno partecipato all'indagine, durante la manifestazione di chiusura (il 10 febbraio) abbiamo assegnato 5 iPod Nano, sorteggiandoli tra tutti coloro che ci hanno inviato il questionario europeo compilato. A breve potremo presentare i risultati globali dello studio.

I PROSSIMI APPUNTAMENTI: VERONA E ROMA

Ora stiamo preparando il programma delle prossime manifestazioni Infosecurity: a Verona, nei giorni 8 e 9 maggio, e a Roma, nei giorni 21 e 22 giugno.

A Verona i convegni saranno diretti principalmente a piccole e medie aziende ed amministrazioni locali; a Roma ci focalizzeremo piuttosto sulle aministrazioni centrali, sulle Telcom e sul settore Finance. A partire da Verona, il format dei convegni sarà ancora migliorato. Ai convegni di Milano, abbiamo registrato un particolare interesse dei partecipanti per la presentazione di casi pratici ed abbiamo pertanto deciso di aumentare il numero delle testimonianze di aziende utenti.

3. SICUREZZA DEI SISTEMI E PA

Riportiamo integralmente un'articolo di Gigi tagliapietra, pubblicato sull'ultimo numero della rivista "PubblicA" (Edizioni Edipi).

SECURITY E PA: SFIDE E COMPITI

Esiste una consapevolezza diffusa del ruolo determinante che la sicurezza riveste per la PA oggi? Qualunque risposta sarebbe parziale e imprecisa perchè il solo modo di leggere una simile risposta è in una dimensione temporale: diciamo quindi che rispetto solo a pochi anni fa il trend è largamente positivo.

Non c'è dubbio che la diffusione crescente dell'utilizzo delle tecnologie dell'informazione nella Pubblica Amministrazione rappresenti un cambiamento significativo non solo nei suoi modelli organizzativi ma sopratutto nel rapporto con la vita quotidiana di milioni di cittadini.

Basti pensare alla recente entrata in vigore del nuovo Codice per l'Amministrazione Digitale che stabilisce specifici diritti che cittadini e imprese potranno esercitare: dal diritto all'utilizzo della posta elettronica nella comunicazione con gli enti al diritto ad effettuare qualsiasi pagamento in forma digitale.

In questo contesto i riferimenti alla sicurezza sono espliciti e strutturali tanto nei mezzi (Firma digitale, posta elettronica certificata, carte

elettroniche) che nelle modalità di fruizione. E non potrebbe essere altrimenti. Senza sicurezza, ad esempio, nella validità, autenticità e disponibilità delle informazioni, senza la difesa di tali informazioni da intrusioni e abusi l'intero progetto vedrebbe minata la sua stessa esistenza.

E' del tutto evidente come la PA stia compiendo grandi sforzi per agire simultaneamente sui due fronti, quello della digitalizzazione dell'informazione e quella della sua protezione e dobbiamo valutare positivamente questo processo, anche se ancora contraddittorio, che vede i due aspetti intrinsecamente connessi e non come nel recente passato in cui ci si preoccupava della sicurezza quando i sistemi erano ormai attivi (e, ahimé, esposti a grandi rischi).

Il problema cruciale è che la PA, come le altre imprese del resto, si trova ad operare in un contesto altamente dinamico in cui la crescita di servizi on line di valore, aumenta l'appetibilità di tali servizi per potenziali intrusi e in cui la crescita degli utenti e delle informazioni messe a disposizione aumenta esponenzialmente la complessità del sistema da proteggere.

SICUREZZA COME FATTORE CHIAVE

Il fatto peculiare è che in sistemi come quelli della PA che si rivolgono, per definizione, alla massa dei cittadini in un rapporto bidirezionale e non di pura fruizione come nel caso della televisione, la necessità non è solo quella di garantire l'integrità dei sistemi a cui si accede ma anche, e direi soprattutto, di fare in modo che i milioni di utenti non diventino elementi di vulnerabilità (consapevole o meno poco conta) della rete.

E' un'operazione che richiede tempi medio-lunghi e grandi sforzi di formazione e comunicazione e non credo esista una soluzione che si possa basare solo sulle tecnologie per quanto necessarie e imprescinidibili.

La posta in gioco è molto alta e non riguarda solo la PA: riguarda tutti coloro che attraverso la rete erogano e utilizzano servizi di qualsiasi natura e cioè tutti quanti. La PA infatti non è solo uno dei "tanti fornitori di informazioni" in rete è anche il garante di validità e di legalità di transazioni e documenti, di identità dei cittadini, il soggetto con il più alto numero di dati sensibili da tutelare: in somma la protezione dei sistemi della PA non è un fatto "interno" ma una questione che tutti dobbiamo avere a cuore.

VULNERABILITÀ E DEBOLEZZE

Se, come abbiamo visto, il sistema diventa più rischioso e complesso con il suo crescere, esistono alcuni fattori di vulnerabilità o meglio di "debolezza" a cui bisognerebbe porre attenzione immediata.

Innanzitutto porre attenzione al ruolo che giocano in questo contesto le Amministrazioni locali e periferiche perchè sono meno preparate delle Amministrazioni centrali ad affrontare il tema della sicurezza e perchè sono in prima linea nella erogazione di servizi quotidiani ai cittadini.

Formazione e certificazioni specifiche di sicurezza sono ancora troppo limitate e del tutto inadeguate alla dimensione e diffusione di sistemi altamente critici anche perchè molta attenzione viene ancora posta alla sicurezza in termini di prodotti più che di funzioni o di impatti organizzativi e di gestione degli incidenti.

E' un fatto estremamente positivo che stiano crescendo e coordinando le proprie iniziative i CERT (I team di sorveglianza e di risposta agli incidenti) all'interno della PA è però preoccupante il ritardo che abbiamo accumulato e che non sembriamo in grado di colmare.

Ma un ritardo ancora più grave lo stiamo segnando nel campo della raccolta e condivisione di informazioni che possono aiutare a prevenire incidenti che potrebbero avere conseguenze devastanti. Prevalgono ancora forse piccole gelosie di "territorio" o peggio sottovalutazioni circa l'esigenza di un costante scambio di informazioni con modalità strutturate e di qualità. A questo proposito il CLUSIT si è fatto promotore dell'avvio anche in Italia degli ISAC (Information Sharing and Analysis Center) sul modello attivo da molti anni negli USA perchè tanto nel settore privato che in quello pubblico, la creazione di "reti di fiducia" tra persone che operano ai massimi livelli è il fattore chiave per prevenire quanto più possibile incidenti gravi ma soprattutto per gestire efficacemente le situazioni di crisi.

COSTI ED ETICA

La prima area d'azione riguarda il modello di valutazione del costo dei sistemi di sicurezza nella PA. Di certo tutti vorrebbero sistemi di protezione estremamente sicuri, a bassissimo costo e ad altissime prestazioni ma queste tre condizioni sono, almeno per il momento, inconciliabili. Possiamo avere sistemi molto sicuri e ad alte prestazioni ma non costano poco. Con pochi soldi a budget possiamo pensare di costruire buoni sistemi di protezione ma le prestazioni potranno darci non pochi grattacapi. In sostanza il nostro triangolo non si chiude e dobbiamo accettare un compromesso, decidere quale delle tre variabili dovremo penalizzare. Nella PA in passato hanno prevalso i criteri di scelta di tipo economico e le stesse gare d'appalto assegnano punteggi molto rilevanti alla voce "prezzo" e quindi non potremmo aspettarci sistemi sicuri o performanti. Possiamo continuare così anche in futuro? Dobbiamo auspicare un cambio di rotta, quanto meno che identifichi il costo di una soluzione di sicurezza non nel suo valore di acquisto ma, almeno, nella sua solidità nel tempo, nel suo costo di gestione e nella sua capacità di ridurre i costi dei danni derivati da incidenti e violazioni.

La seconda e ben più importante area d'azione non riguarda la tecnologia nè tantomeno l'economia in senso stretto: riguarda l'etica.

Se vogliamo indurre comportamenti virtuosi e attenti in migliaia di operatori e in milioni di utenti-attori, dobbiamo restituire valore e rilevanza a concetti importanti come "il rispetto della persona", "la sacralità della confidenzialità", "il dovere di tutelare i più deboli".

Non c'è tecnologia che possa proteggere un sistema i cui utenti non riconoscano come valore il diritto alla privatezza delle conversazioni, o che non trattino con sacro rispetto i dati di qualsiasi genere che riguardano le persone.

Gigi Tagliapietra, presidente CLUSIT

4. CONSULTAZIONE EUROPEA SULLA FUTURA POLITICA BREVETTUALE

La Commissione europea ha avviato una consultazione pubblica sul tema della futura politica brevettuale europea. Il documento può essere scaricato all'indirizzo:

http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/38&format=HTML&aged=0&language=EN&guiLanguage=fr

E' possibile partecipare alla consultazione pubblica, rispondendo all'apposito questionario entro il 31 marzo 2006.

Fonte: Federcomin

5. SEMINARI ED ESAMI CISSP

Riprendono i Seminari e gli Esami.

Sono disponibili ancora posti al **Seminario di preparazione all'esame CISSP** che avra' luogo a **Roma dal 27 al 31 marzo 2006**.

Per registrarsi ai Seminari inviare il modulo di registrazione disponibile su www.clusit.it/isc2/SeminarRegistrationFormItaly_2005.pdf

Per i Soci Clusit sono previste delle tariffe agevolate per il Seminario.

La prossima sessione d'esame avrà luogo sempre a Roma il 29 aprile 2006

La registrazione agli Esami si può effettuare dalla pagina www.clusit.it/isc2/calendario_isc2.htm o direttamente online

https://www.isc2.org/cgi/exam_schedule.cgi

Maggiori informazioni sono disponibili su www.clusit.it/isc2.

Per qualsiasi chiarimento inviare una email a isc2@clusit.it.

6. SEMINARI CLUSIT EDUCATION 2006

E' stato pubblicato su www.clusit.it/edu il calendario dei Seminari Clusit Education

Phishing: profili tecnici e legali. Tecniche di prevenzione e casi pratici

Milano 14/03/2006
Roma 04/04/2006

Crittografia Moderna: Teoria e Pratica

Milano 04/05/2006
Roma 25/05/2006

Aspetti legali della sicurezza informatica: lo stato dell'arte

Milano 22/06/2006
Roma 06/07/2006

Web Applications Security:hands-on lab

Milano 19/09/2006
Roma 03/10/2006

Il Social Engineering e la sua applicazione nel Penetration Testing
professionale.
Milano 17/10/2006
Roma 31/10/2006

Sicurezza nella virtualizzazione dei servizi di rete
Milano 28/11/2006
Roma 12/12/2006

Sono aperte le iscrizioni al primo Seminario del programma:
Il Phishing: profili tecnici e legali. Tecniche di prevenzione e casi pratici
a MILANO il 14 marzo 2006
a ROMA il 4 aprile 2006

Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form.pdf
Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

1. Aspetti tecnici del phishing. Case study
   - Spam, virus, worm, phishing: una radice comune
   - Analisi dell'evoluzione del Phishing in Italia
     - Case study # 1
     - Case study # 2
   - Tecniche di attacco avanzate: vulnerabilità lato Internet Browser
   - Conclusioni
2. Aspetti legali del phishing
   - Aspetti civili e penali del phishing
   - Profili sanzionatori
   - Problematiche processuali
3. Phishing e cybericiclaggio, le corrette politiche di risposta alle frodi informatiche: il crisis management"
   - Il fenomeno "phishing": trend attuali e futuri
   - La crescita vertiginosa del fenomeno
   - L'estensione a nuovi mercati e i danni in termini di immagine e reputazione aziendale
   - Phishing e codice penale
   - I casi nazionali ed internazionali
   - Non solo phishing: gli altri casi di furto di identità elettronica
   - Phishing e cybericiclaggio
   - Coordinamento informativo tra le banche
   - Come non deve comportarsi l'azienda a livello di comunicazione con i propri clienti

Agenda:
- Registrazione: 13,50
- Inizio Seminario: 14,10
- Fine lavori: 18,10

Docenti: Andrea Ghirardini, Giuseppe Bellazzi, Gerardo Costabile
Luogo:

- Milano allo StarHotel Splendido - Viale Andrea Doria, 4
- Roma al Centro di formazione Percorsi SpA - Viale Manzoni 22

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

7. EVENTI SICUREZZA

14 marzo 2006, Milano
Seminario CLUSIT "Phishing: profili tecnici e legali. Tecniche di prevenzione e casi pratici"
www.clusit.it/edu

27-31 marzo 2006, Roma
Seminario CISSP
www.clusit.it/isc2

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

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

11 aprile, Lugano
CLUSIS e CLUSIT presentano il Security Day 2006, Convegno di apertura del Lugano Communication Forum

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

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

© 2006 Clusit - Vietata la riproduzione
Clausola di esclusione della responsabilità e informazioni relative al Copyright: www.clusit.it/disclaimer.htm