

Indice

- 1. NUOVI SOCI**
- 2. INFOSECURITY ROMA - PROGRAMMA DEI CONVEGNI CLUSIT**
- 3. CYBERCRIME**
- 4. VULNERABILITÀ IN SOFTWARE SCADA**
- 5. AL VIA LA 4ª EDIZIONE DEL PREMIO TESI**
- 6. INIZIATIVE CLUSIT PER LE PICCOLE E MICROIMPRESE**
- 7. NOTIZIE E SEGNALAZIONI DAI SOCI**
- 8. EVENTI SICUREZZA**

1. NUOVI SOCI

Hanno aderito al Clusit:

- Banca Mediolanum (Basiglio - MI);
- NeoNevis (Pisa).

2. INFOSECURITY ROMA - PROGRAMMA DEI CONVEGNI CLUSIT

Nei giorni 10 e 11 giugno si terrà l'edizione romana di Infosecurity Italia, all'hotel Sheraton di viale del Pattinaggio www.infosecurity.it/IT/roadshow/Locationroma2008.aspx.

Anche quest'anno il CLUSIT ha contribuito all'organizzazione della parte convegnistica.

In particolare, abbiamo organizzato i seguenti eventi:

10 giugno - ore 14.00/18.00

SEMINARIO CLUSIT EDUCATION

"Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro"

Vedi dettaglio su https://edu.clusit.it/scheda_seminario.php?id=24

11 giugno - 10.30/13.30

CONVEGNO INFOSTORAGE

"Sicurezza delle informazioni: come difendersi dalle nuove forme di attacco"

ABSTRACT:

Nel corso del convegno i relatori istituzionali analizzeranno alcune delle nuove forme di attacco informatico e delle corrispondenti contromisure. I casi di studio illustreranno alcune soluzioni che, opportunamente implementate, possono ridurre le conseguenze di tali attacchi.

CHAIRMAN: Danilo Bruschi, Università degli Studi di Milano, Presidente Onorario Clusit

PARTECIPANTI:

- Domenico Vulpiani, Direttore Servizio Polizia Postale e delle Comunicazioni In questo intervento si farà una panoramica sulla situazione della criminalità informatica in Italia e sulle numerose attività di controllo e contrasto portate avanti dalle Forze dell'Ordine.
- Stefano Aterno, Avvocato, Docente di informatica forense e criminologia informatica presso l'Università La Sapienza di Roma.

La normativa in materia di Data Retention. Il Decreto Legge 27 luglio 2005, n. 144 (Misure urgenti per il contrasto del terrorismo internazionale convertito in legge 31 luglio 2005, n. 155 e il Provvedimento generale del Garante per la protezione dei dati personali del 17 gennaio 2008 (La sicurezza dei dati di traffico telefonico e telematico).

- Michele Bianco, Security Service Line Security Senior Manager ACCENTURE Spa " Data Protection e Retention di Infrastrutture Critiche e Ambienti Virtuali Innovativi"
- Gerardo Costabile, Responsabile Sicurezza Logica - Security & Safety di Poste Italiane, Presidente IISFA Italian Chapter.

"Data Retention, compliance ed information forensics nella nuova disciplina italiana".

- Raoul Chiesa, Comitato Direttivo CLUSIT, ISECOM, TSTF e OWASP/IT, Consulente per le Nazioni Unite presso l'UNICRI.

"Attacchi informatici: evoluzione delle tecniche e dei profili degli attaccanti".

In questo intervento, dopo aver illustrato l'evoluzione delle nuove tecniche di attacco informatico, sarà presentato uno studio aggiornato sull'evoluzione del profilo tipo dell'attaccante di oggi e di domani.

- Valerio Neri, Direttore generale Save the Children Italia "Minori e nuovi media: educazione, prevenzione, protezione"

11 giugno - 14.30/17.30

CONVEGNO INFOSTORAGE

"I servizi di supporto alla sicurezza delle informazioni"

Nel corso del convegno saranno presentate ed analizzate le problematiche relative alla gestione della Sicurezza delle informazioni nell'ambito delle medio-grandi organizzazioni (sia pubbliche che private).

CHAIRMAN: Gigi Tagliapietra, Presidente Clusit

PARTECIPANTI:

- Marco Bavazzano, Chief Information Security Officer di Telecom Italia.

Il CISO di una delle più importanti aziende del nostro Paese, farà una panoramica sulle principali problematiche legate alla gestione della sicurezza delle informazioni e dei sistemi nel settore delle Telecomunicazioni.

- Anthony Cecil Wright, MBCI, Presidente ANSSAIF.

Uno dei principali esperti italiani in materia di Business Continuity, ci parlerà dell'evoluzione della BC e dei principali servizi di sicurezza informatica in ambito bancario.

- Antonio Naletto, DUBLE-TAKE Italy.

Il Country manager di DUBLE-TAKE Italy ci presenterà dei case study di Business Continuity (Problematiche e soluzioni).

- Raoul Chiesa, Membro del Comitato Direttivo CLUSIT.

"Cosa si può chiedere e cosa si può pretendere da un fornitore di servizi di sicurezza informatica". In questo intervento, uno dei soci fondatori del clusit illustrerà i criteri e principi di base che devono ispirare il management delle medio-grandi organizzazioni (sia pubbliche che private) nel valutare e scegliere un fornitore di servizi di sicurezza informatica.

Il programma di tutti i convegni (che sono a partecipazione libera e gratuita), compresi quelli non direttamente organizzati dal Clusit, è disponibile su www.infosecurity.it/IT/roadshow/Visitatoriroma2008.aspx

Per ridurre al minimo le formalità di ingresso alla manifestazione, si consiglia di registrarsi on line sul sito della manifestazione www.infosecurity.it/IT/roadshow/iscrizione-workshop-2008.aspx

È disponibile in italiano l'ultimo aggiornamento di un documento del SANS Institute sulle 20 vulnerabilità più critiche per la sicurezza su internet. La versione italiana www.clusit.net/whitepapers/080408_top20_2007.pdf è stata realizzata da Data Security, con il patrocinio del Clusit.

Ringraziamo Romano Favero (Data Security) ed il SANS Institute, che ci hanno consentito la divulgazione del documento, e Luca Spingolo e Simone Brun, che hanno collaborato alla localizzazione italiana della SANS Top 20.

3. CYBERCRIME

Nuova forma di Social Engineering

Il Compartimento della Polizia Postale di Potenza ha individuato e denunciato due persone che avevano adottato una nuova forma di social engineering finalizzata non a carpire credenziali (logonid, password,...) da utilizzare direttamente in operazioni di Home Banking e similari, ma ad accedere alle caselle email delle potenziali vittime.

L'accesso alle mailbox delle vittime consentiva ai malfattori non solo di accedere a informazioni personali e riservate sugli utenti, ma li metteva anche in condizione di ricevere password di accesso ad ulteriori servizi Internet, oltreché ottenere tutti i dati anagrafici degli utenti poco accorti caduti nella trappola, con conseguente furto di identità.

Il meccanismo adottato aveva inizio con email di "spamming" con le quali gli ideatori della truffa, seguendo un rituale ormai consolidato (phishing), inducevano gli utenti a cliccare su un indirizzo web inserito nel messaggio stesso. Un indirizzo che portava gli sprovveduti su due siti all'apparenza del tutto identici a quelli dei propri fornitori di servizi di posta elettronica, siti nei quali le vittime inserivano username e password, in cambio dei quali ricevevano un errore di connessione.

I legittimi proprietari delle mailbox, ovviamente, per molto tempo non si sono accorti di aver "condiviso" le proprie caselle email con degli sconosciuti: sono centinaia le persone che sembrano aver subito questa truffa. Un raggirio scoperto soltanto quando alcuni utenti hanno denunciato l'accesso abusivo a conti correnti bancari online e ad altri servizi, una circostanza che ha messo la Polizia Postale sulle tracce dei due uomini ritenuti responsabili di quanto accaduto.

Sulle due persone fermate sono state mosse accuse di accesso abusivo a sistemi informatici, sottrazione di codici di accesso personali, furto di identità (sostituzione di persona, art. 494 C.P.).

(Tratto dalla Newsletter ANSSAIF - www.anssaif.it)

Cronaca dell'attacco informatico all'estonia

Pubblicata su ITnews Australia www.itnews.com.au/News/76651_expert-dissects-estonian-cyberwar.aspx

A security researcher involved in defending against last year's Web attacks on Estonia has shared his account of the crisis, and is offering advice on how to prevent similar assaults in the future.. Gadi Evron has published an article in the Georgetown Journal of International Affairs <http://journal.georgetown.edu> detailing his experiences in helping Estonia's government defend against a "cyber-riot" from Russian nationalist hackers.

Il racconto dell'esperto che ha aiutato il governo Estone a difendersi, è disponibile su www.ciaonet.org/journals/gjia/v9i1/0000699.pdf.

(Autore: Stefano Quintarelli)

4. VULNERABILITÀ IN SOFTWARE SCADA

E' forse la prima volta che una vulnerabilità di un pacchetto software SCADA <http://en.wikipedia.org/wiki/SCADA> di grande diffusione (alcune centinaia di migliaia di installazioni al mondo, in molti settori, dai processi industriali, chimici ecc., alle infrastrutture ed utilities), per applicazioni per automazione di fabbrica e controllo di processo, supervisione e monitoraggio di impianti, finisce sotto i riflettori degli addetti alla security dei sistemi utilizzati nell'industria e nelle infrastrutture.

"A vulnerability was found in Wonderware SuiteLink Service (slssvc.exe) that could allow an un-authenticated remote attacker with the ability to connect to the SuiteLink service TCP port to shutdown the service abnormally by sending a malformed packet. Exploitation of the vulnerability for remote code execution has not been proven, but it has not been eliminated as a potential scenario."

vedi www.coresecurity.com/?action=item&id=2187

A fronte di questa segnalazione si è acceso un vivace dibattito nella community del comitato ISA s99 (Industrial Automation and Control System Security).

Per molti è suonata la sveglia (non ci si può più fidare della security dei prodotti per l'automazione industriale out-of-the-box) ed è necessario quindi iniziare a pensare alla cyber security come processo anche in ambiente industriale, identificare i rischi, pensare ad adeguate contromisure.

Di Cyber-Security Industriale ne abbiamo parlato anche nel 2007: Clusit ha pubblicato il quaderno dal titolo "Introduzione alla protezione di reti e sistemi di controllo ed automazione (DCS, SCADA, PLC, ecc.)" che si può scaricare da www.clusit.it/download/Q07_web.pdf.

(Autore: Enzo Maria Tieghi)

5. AL VIA LA 4^a EDIZIONE DEL PREMIO TESI

Sono già aperte le iscrizioni alla quarta edizione del premio Clusit "Innovare la Sicurezza delle Informazioni".

Il premio, riservato alle migliori tesi sulla sicurezza delle informazioni, ha lo scopo di promuovere una collaborazione tra i soggetti che si occupano di sicurezza informatica in Italia: le aziende, le Università, gli studenti. Un punto scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro, alimentato direttamente dai singoli soggetti che vi partecipano portando i propri bisogni e le proprie esperienze.

La Commissione designata ad assegnare il Premio sarà costituita da membri del Comitato Tecnico Scientifico, membri del Comitato Direttivo e Soci CLUSIT.

Le iscrizioni saranno accettate fino al 31.12.2008 e la premiazione si svolgerà durante Infosecurity 2009.

Le prime 5 tesi classificate saranno premiate ed in particolare il primo riceverà la somma di 2.000 €; al secondo classificato sarà offerto un Corso di preparazione alla certificazione internazionale ISECOM OPST - OSSTMM Professional Security Tester; al terzo classificato un corso Lead Auditor ISO IES 27001.

A tutti i classificati sarà accordata l'adesione gratuita al Clusit per il 2009.

Si sono già confermati come sponsor della quarta edizione: BSI Management Systems, Lampertz Italia e @mediaservice.net.

Sul portale <https://tesi.clusit.it> sono disponibili tutte le informazioni sul premio.

6. INIZIATIVA CLUSIT PER LE PICCOLE E MICROIMPRESE

Continua l'attività del CLUSIT per favorire l'introduzione di una corretta gestione del rischio ICT nelle piccole e microimprese italiane. Per intervenire sulle microimprese è necessario un modello che sia facilmente scalabile sui grandi numeri e che tenga conto delle competenze disponibili sul territorio. Per questo, il CLUSIT sta sviluppando un modello di intervento che coinvolge fortemente le associazioni imprenditoriali, che sono in grado di individuare le esigenze dei loro associati, di veicolare informazioni e di tutelare gli associati riguardo all'adeguatezza di quanto viene loro proposto.

Il modello prevede di operare su categorie di imprese uniformi come settore di attività, dimensioni, territorio e quindi in buona misura anche struttura del sistema informativo ed esigenze di gestione del rischio e conformità alle normative. Per ogni categoria su cui si pianifica di intervenire, viene selezionato un campione di imprese che viene analizzato direttamente. In base a questa analisi sono individuate le esigenze e vengono sviluppati strumenti per guidare l'impresa a

raggiungere un livello di sicurezza e una gestione del rischio adeguati. Gli strumenti sono poi applicabili con poche variazioni alle altre imprese della stessa categoria, autonomamente o al più con il supporto di poche ore di consulenza.

Anche dal punto di vista della consulenza, il modello prevede l'utilizzo delle competenze presenti sul territorio, con una formazione limitata a quanto necessario per utilizzare correttamente gli strumenti sviluppati. È da sottolineare che l'attività di consulenza non vuole in generale sostituirsi all'attività dei fornitori e gestori dei sistemi informativi delle piccole e microimprese, ma si limiterà a fornire loro indicazioni su come correggere le carenze rilevate principalmente mediante strumenti di autoanalisi. Successivi incontri, sempre della durata di poche ore e ripetuti con cadenza semestrale o annuale, permetteranno di mantenere nel tempo i risultati raggiunti.

La speranza è che con questo approccio sia possibile influire in modo significativo sulla sicurezza dell'enorme numero di piccole e microimprese italiane, che non sono raggiungibili se non in piccola parte con gli strumenti tradizionali.

In questi giorni si stanno già attivando i primi progetti pilota, sul cui sviluppo vi manterremo informati.

Naturalmente il CLUSIT è interessato al supporto di queste iniziative da parte di aziende e sponsor. Chi fosse interessato, può contattare ctelmon@clusit.it.

Parallelamente a questa attività, continua la partecipazione al gruppo di lavoro di ENISA sulle esigenze di sicurezza delle informazioni delle microimprese. La partecipazione a questo gruppo di lavoro permette fra l'altro di scambiare informazioni ed esperienze con rappresentanti di altri paesi, di individuare best practices e di discutere le difficoltà e i vantaggi delle diverse iniziative in atto in Europa.

(Autore: Claudio Telmon, coordinatore del progetto Clusit "Rischio IT e piccola impresa")

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

Presentazione del volume "Diritto Privato dell'Informatica e di Internet".

Il 5 giugno si terrà a Roma, presso l'Autorità Garante della Concorrenza e del Mercato, la Tavola Rotonda dal titolo "Il Diritto Privato delle nuove tecnologie".

Nel corso della manifestazione sarà presentato il volume "Diritto Privato dell'Informatica e di Internet" (GIUFFRÈ Editore), scritto dall'Avv. Emilio Tosi, uno dei soci fondatori del Clusit. L'invito alla manifestazione è disponibile su www.tosilex.it/documenti/Invito%20TOSI.pdf ed è esteso a tutti i soci.

Anche i farmaceutici parlano di Industrial Cyber Security.

Al 48° Simposio AFI (Rimini, 11-12-13 giugno), tradizionale appuntamento annuale dell'Associazione Farmaceutici Industria, nel pomeriggio di giovedì 12

giugno ci sarà una sessione dal titolo "La protezione dei processi farmaceutici dai rischi informatici", moderata dall'ing. Silvano Vianello del board di AFI.

Questa sessione è stata coordinata da Enzo M. Tieghi, socio Clusit, che presenterà una memoria dal titolo "Introduzione alla protezione da rischi informatici di reti e sistemi di fabbrica", che tratterà alcuni degli argomenti già pubblicati nel quaderno Clusit dallo stesso titolo www.clusit.it/download/Q07_web.pdf, con particolare riferimento al mondo produttivo regolamentato quale quello del Life Science.

Nella sessione sono previste presentazioni da parte di esponenti di Gamp Italia e di testimonial di primarie aziende farmaceutiche multinazionali quali GSK GlaxoSmithKline Manufacturing ed Eli Lilly.

Per maggiori informazioni sull'evento: www.afiweb.it

Convegno sul Computer Forensics Investigation.

Mercoledì 18 Giugno 2008 - Ore 9:30 - Aula Magna "Francesco Leoni" presso la Libera Università S. Pio V (Roma).

Il programma dell'evento è disponibile sul sito www.cfitaly.net

Sono stati pubblicati i bandi relativi alla V edizione del Master di I livello in "Sicurezza dei sistemi e delle reti informatiche per l'impresa e la Pubblica Amministrazione" ed alla III edizione del Master di II livello in "Gestione della sicurezza informatica per l'impresa e la Pubblica Amministrazione"- a.a. 2008/2009, attivati dal Dipartimento di Informatica dell'Università degli Studi di Roma "La Sapienza", la cui didattica anche quest'anno si svolgerà il venerdì pomeriggio ed il sabato mattina.

I Corsi avranno inizio a fine ottobre 2008 per terminare a luglio 2009.

La data di scadenza per la presentazione delle domande è fissata per l'08/10/2008.

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

Per un colloquio di approfondimento, rivolgersi a:

SEGRETERIA DEL MASTER

Raffaella Toscano - Tel. 06.49918537

E-mail: mastersicurezza@di.uniroma1.it

8 . EVENTI SICUREZZA

4 giugno 2008, Bologna

Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

https://edu.clusit.it/scheda_seminario.php?id=25

5 giugno 2008, Firenze

Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro

https://edu.clusit.it/scheda_seminario.php?id=23

10-11 giugno 2008, Roma
Infosecurity Italia - Storage Expo – trackability
www.infosecurity.it/IT/roadshow/roma%202008.aspx

10 giugno 2008, Roma
Seminario Clusit: Dal Penetration Testing alla Risk Analysis: la metodologia OSSTMM 3.0, lo standard ISO 27001 ed i punti di incontro
https://edu.clusit.it/scheda_seminario.php?id=24

**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

© 2008 Clusit - Vietata la riproduzione

Clausola di esclusione della responsabilità e informazioni relative al Copyright:

www.clusit.it/disclaimer.htm