

Indice

1. NUOVI SOCI
2. NUOVI QUADERNI CLUSIT
3. LA PROTEZIONE DI RETI E SISTEMI DI CONTROLLO ED AUTOMAZIONE NEGLI IMPIANTI DI PRODUZIONE
4. CYBERCRIME
5. RASSEGNA STAMPA CLUSIT
6. PRISE 2007 - CALL FOR PAPER
7. NOTIZIE DA ENISA
8. INFOSECURITY ITALIA 2007
9. PREMIAZIONE DELLE MIGLIORI TESI IN SICUREZZA INFORMATICA
10. NOTIZIE DAI SOCI

1. NUOVI SOCI

Hanno aderito al Clusit:

- @PSS (Trento),
- Computer VAR Services (Empoli - FI),
- NGX (Roma),
- Saes Getters (Lainate - MI)

2. NUOVI QUADERNI CLUSIT

Segnaliamo la pubblicazione di due nuovi Quaderni Clusit:

- **Implementazione e certificazione dei sistemi di gestione per la sicurezza delle informazioni** Autore: *Fabrizio Cirilli*
- **I rischi del Trusted Computing** Autore: *Claudio Telmon*

I soci Clusit potranno ritirarne una copia stampata in occasione di Infosecurity a Milano.

A breve saranno disponibili su www.clusit.it/download sia i quaderni (con consultazione riservata ai soci) che gli abstract (in consultazione libera).

Dopo 90 giorni dalla pubblicazione la consultazione sarà libera per tutti.

3. LA PROTEZIONE DI RETI E SISTEMI DI CONTROLLO ED AUTOMAZIONE NEGLI IMPIANTI DI PRODUZIONE

Proteggere i sistemi informatici e le informazioni da essi generate o elaborate è divenuto critico in ogni attività, è può esserlo ancora di più nel settore industriale e delle infrastrutture ove sono ampiamente utilizzati reti e sistemi di controllo e supervisione.

I danni che possono provocare incidenti ai sistemi di controllo a volte possono essere altamente pericolosi ed avere conseguenze molto gravi anche per l'impianto stesso, l'ambiente, persone e cose.

Pensiamo (solo per ipotesi, naturalmente) ai danni indotti da un incidente in una centrale nucleare, o alle conseguenze derivanti da un black-out elettrico, da un blocco delle comunicazioni telefoniche, in un aeroporto, oppure ad un problema

in una fabbrica chimica, in raffineria o in un impianto di controllo di una diga, in un depuratore o in un acquedotto, e ancora in un nodo ferroviario, una fonderia o un ospedale.

I sistemi informatici, con l'avanzare della tecnologia, sono ormai ampiamente diffusi e controllano e supervisionano impianti ed edifici ovunque.

Bisogna anche pensare che proteggere un sistema di automazione di fabbrica o di controllo di processo spesso può anche essere più difficoltoso di altri sistemi, per vincoli tecnologici e operativi. Minacce e vulnerabilità alle quali sono esposti questi sistemi a volta sono addirittura sconosciute e molto diverse da quelle in cui tradizionalmente sono incorse banche ed aziende in genere. Spesso errori degli operatori, incuria, sabotaggio ed altro sono eventi che provengono dall'interno, ma la schiera dei malintenzionati può includere anche eventi ed agenti esterni (come riportato dalla stampa) e purtroppo anche terroristi (come appurato anche da CIA, FBI e dalla stessa Casa Bianca).

Come per tutte le attività che hanno rischi insiti, è necessario "pensarci prima".

Ci possono essere diversi approcci per affrontare il problema.

La considerazioni dalle quali bisogna partire sono però le seguenti :

- un sistema non potrà mai essere sicuro al 100%
- un sistema "sicuro" ora, potrà non esserlo più domani o tra un'ora
- la sicurezza non è un prodotto confezionato, è un processo, un modo di pensare
- i problemi di sicurezza non si risolvono solo con la tecnologia
- i comportamenti delle persone sono la parte preponderante per rendere sicuro un sistema

Alcune norme ci possono aiutare a decidere quali sono le migliori politiche per la sicurezza dei sistemi e delle informazioni, a definire rischi, minacce e vulnerabilità e identificare quali sono i controlli e le contromisure da adottare.

Clusit ha deciso di approfondire il tema della protezione di reti e sistemi di controllo, promuovendo la pubblicazione di un Quaderno, che sarà scritto dal socio Enzo Maria Tieghi e potrà essere disponibile nel corso del prossimo mese di marzo.

4 . CYBERCRIME

Aumentano gli "spyware".

Avevamo ribadito, anche nella Newsletter di dicembre 2006, la nostra preoccupazione per un aumento di programmi "malvagi" (c.d."malware" e "spyware") sui personal computer dei Consumatori e di piccole aziende.

In questo mese, che è trascorso, abbiamo avuto altri riscontri e, fra questi, abbiamo raccolto un'informazione riguardante un crescente interesse - da parte di varie fonti, certamente non lecite - nell'acquisto di software "malevolo". Dato che questa notizia è uscita dall' "underground", vuol dire che il sistema dei software "spioni" piace, e molto.

Ricordiamo che parliamo di un sistema consistente nel far memorizzare un software sui pc di ignari cittadini, ai fini di catturare utili informazioni dai file contenuti sui dischi e da quanto digitato sulla tastiera.

Se è vero che il sistema è nato per conoscere le abitudini e le preferenze dei Consumatori, è anche vero che è utilissimo ai criminali, e, perché no, ai terroristi.

E' già accaduto che alcuni computer, "innocenti", sono serviti per lanciare degli attacchi a siti di aziende nemiche, in quanto appartenenti ad ideologie, religioni, ecc. non condivise. Siccome una domanda crescente non può che far aumentare l'offerta, ci dobbiamo attendere una recrudescenza su questo campo.

Su questo tema, che meriterebbe ben più di quattro righe, dobbiamo segnalare alcuni articoli usciti questa settimana.

Il primo accenna alla presenza di pc "zombi", pronti quindi ad agire ad un comando da remoto. Su quotidiano.net e su altri giornali si può trovare trattato questo tema:

<http://qn.quotidiano.net/chan/tecnologia:5454941:/2007/01/14:>

Il secondo, dal titolo "quando il virus diminuisce, phishing e spam festeggiano", tende a dare una spiegazione - supportata da dati - sul perché si è vista una diminuzione nella "cattiveria" di attacco dei virus.

MessageLabs lo giustifica, come dice il titolo, dalla necessità - per i criminali - di attirare i Consumatori nelle trappole connesse alle email con titoli allettanti o che sembrano provenire da aziende o Enti conosciuti, e con i quali si ha un rapporto cliente-fornitore.

Appunto le spam e le email di phishing.

Per maggiori informazioni:

www.vnUNET.it/it/vnUNET/article/2007/01/22/strategie-sempre-pi-complesse

A proposito di titoli allettanti, possiamo citare il recente caso - segnalato da Symantec - delle email riportanti il titolo "230 morti a causa della tempesta che ha colpito l'Europa".

Una volta aperto l'allegato (un videoclip), il computer viene infettato dal Trojan Peacomm, il quale cercherà di connettersi a un indirizzo remoto ed usare il computer infetto per inviare un alto numero di messaggi spam.

Per maggiori informazioni consultare la pagina:

www.agi.it/oggi-in-italia/notizie/200701232034-cro-rt11289-art.html

La **Polizia di Stato** ha realizzato facili istruzioni per i Consumatori.

Suggeriamo di accedere al sito:

www.poliziadistato.it/pds/cittadino/consigli/internet.htm

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

5. RASSEGNA STAMPA CLUSIT

Sono sempre di più i media che riprendono costantemente i nostri comunicati stampa e che ci citano nelle loro testate.

La rassegna stampa è ormai sempre disponibile, e continuamente aggiornata, alla voce **STAMPA** del sito.

6. PRISE 2007 - CALL FOR PAPER

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.

Il prossimo 6 giugno, nell'ambito di Infosecurity Roma, si terrà il secondo workshop italiano su PRIVacy e SEcurity - PRISE 2007

<http://icsecurity.di.uniroma1.it/prise2007>

Il workshop è aperto a ricercatori universitari ed esperti dal 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 13 Aprile 2007 un abstract di al più 4 pagine che descriva i loro migliori risultati ottenuti recentemente (anche se già pubblicati).

Gli autori degli abstract selezionati per la presentazione al Workshop riceveranno comunicazione in questo senso entro il 30 Aprile 2007.

Segue una lista non esaustiva delle principali tematiche considerate: 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.

Presentazione:

Gli autori sono invitati a presentare entro il 13 Aprile 2007 un abstract di al più 4 pagine che descriva il proprio contributo.

La procedura elettronica di presentare è descritta su

<http://icsecurity.di.uniroma1.it/prise2007>

Important dates:

Abstract submission: April 13, 2007

Acceptance notification: April 30, 2007

Camera Ready: May 13, 2007

PRISE 2007 date: June 6, 2007

Workshop Chair

Luigi V. Mancini - Università di Roma "La Sapienza"

Program Committee

Maurizio Aiello - IEIIT CNR Genova

Cosimo Anglano - Università Piemonte Orientale

Massimo Bernaschi - IAC CNR Roma

Claudio Bettini - Università di Milano

Danilo Bruschi - Università di Milano

Giuseppe Corasaniti - Ministero della Giustizia

Bruno Crispo - Università di Trento

Roberto Di Pietro - Università di Roma Tre

Roberto Gorrieri - Università di Bologna

Pino Italiano - Università di Roma "Tor vergata"

Pino Persiano - Università di Salerno

7. NOTIZIE DA ENISA

Segnaliamo che sono disponibili alcune opportunità di lavoro presso ENISA *European Network and Information Security Agency*.

In particolare:

- ENISA/CA/III/2007/01 - Web Master (M/F) deadline 5th February 2007
- ENISA/TA/AD/2007/02 - Legal Adviser (M/F) deadline 5th February 2007
- ENISA/TA/AD/2007/03 - Senior Expert in Network Security Policy (Temporary Agent) deadline 12th February 2007
- ENISA/TA/AD/2007/04 - Junior Expert in Risk Analysis and Management (Temporary Agent) deadline 12th February 2007
- ENISA/TA/AST/2007/05 - Secretary to the Executive Director (Temporary Agent) deadline 12th February 2007
- ENISA/TA/AST/2007/06 - Procurement Officer (Temporary Agent) deadline 12th February 2007
- ENISA/TA/AST/2007/07 - Senior IT Assistant (Temporary Agent) deadline 12th February 2007
- ENISA/TA/AST/2007/08 - Administrative Secretary (Temporary Agent) deadline 12th February 2007
- ENISA/CA/III/2007/09 - Financial Assistant (Contract Agent) deadline 12th February 2007.

Ulteriori informazioni sono disponibili all'indirizzo:

www.enisa.europa.eu/pages/07_05.htm.v

Inoltre, vi segnaliamo le deadline per la presentazione di contributi per la rivista ENISA Quarterly che verrà pubblicata il 30 marzo p.v.

www.enisa.europa.eu/pages/02_02.htm

- Submission of an abstract Proposal for a Contribution: 26 February
- Selection of Proposals and Notification to Authors: 02 March
- Latest submission of Full Articles: 12 March.

Fonte: Daniele Perucchini, ENISA Liaison Officer

8 . INFOSECURITY ITALIA 2007

Dal 6 all'8 febbraio prossimo si terrà la settima edizione di Infosecurity Italia, alla Fiera di Milano. Anche quest'anno il CLUSIT ha contribuito in maniera significativa all'organizzazione della parte convegnistica.

Il programma definitivo dei convegni e delle iniziative collaterali Clusit è disponibile su www.clusit.it/infosecurity2007/infosecMI07.pdf

Tutti i convegni sono a partecipazione libera e gratuita.

Per partecipare ai seminari Clusit, gratuiti per i soci, è necessario seguire la procedura di registrazione su <https://edu.clusit.it/>.

Troverete tutte le informazioni utili su Infosecurity Italia 2007 all'indirizzo www.infosecurity.it/.

Durante i tre giorni della manifestazione, tutto lo staff del Clusit sarà presente allo Stand C29 (Pad. 17/2)

9 . PREMIAZIONE DELLE MIGLIORI TESI IN SICUREZZA INFORMATICA

Il 7 febbraio alle 12.00 circa nell'ambito di Infosecurity, al termine del convegno di presentazione dell'Hacker's Profiling Project, verrà premiata la migliore tesi in Sicurezza Informatica. Il primo premio della seconda edizione di 'Innovare la sicurezza delle Informazioni' consiste in 2.000,00 euro. Il secondo classificato potrà invece partecipare gratuitamente ad un corso per Lead Auditor ISO IEC 27001 (BS7799:2) del valore di 1.600 € (oltre IVA). Inoltre i primi 5 classificati avranno l'adesione gratuita al Clusit per il 2007.

La valutazione delle tesi inviate è stata effettuata da una commissione composta da membri del comitato direttivo, dal comitato tecnico scientifico e da soci CLUSIT, sia del mondo accademico che industriale. Gli elaborati sono stati valutati per l'innovatività dell'argomento trattato, la complessità dell'attività svolta, il livello di conoscenza dimostrato e l'utilizzabilità dei risultati raggiunti.

Il numero dei partecipanti quest'anno è aumentato del 18% rispetto alla precedente edizione e si è ampliato anche il numero degli atenei di provenienza, con cinque nuovi inserimenti. Le tesi che hanno partecipato al premio provengono da 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, Università degli Studi di Firenze, Università di Padova, Università degli Studi di Modena e Reggio Emilia, Roma Tre, Politecnico di Milano, Università di Bologna, Università dell'Aquila, Università degli Studi dell'Insubria, Varese, La Sapienza di Roma, Politecnico delle Marche, Università degli Studi di Siena, Università degli studi di Milano Bicocca, Università degli Studi di Messina.

Il premio è stato sponsorizzato da:



ed è concepito come un'occasione di scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro.

10. NOTIZIE DAI SOCI

Il progetto internazionale OWASP ha recentemente pubblicato la nuova Testing Guide v2 che rappresenta una metodologia per l'audit di sicurezza degli applicativi web.

Tale documento è il risultato di uno sforzo di quasi 4 anni da parte della comunità OWASP con il contributo di oltre 50 professionisti di tutto il mondo.

Il progetto è stato affidato a Matteo Meucci (Fondatore e Chair del capitolo italiano del progetto) che grazie al supporto di altri 10 membri italiani è riuscito a spostare il baricentro di un progetto internazionale dagli Stati Uniti all'Italia.

La guida rappresenta la prima metodologia per la verifica di sicurezza degli applicativi ed è liberamente distribuita on-line con lo scopo di diventare lo standard "de-facto" nel mondo della web security industry.

E' possibile prendere visione della nuova guida direttamente on-line:

www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

oppure leggerla in formato pdf o doc:

www.owasp.org/index.php/Testing_Guide

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

© 2007 Clusit - Vietata la riproduzione

Clausola di esclusione della responsabilità e informazioni relative al Copyright:

www.clusit.it/disclaimer.htm