Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- EOLAS (Meda - MI),
- EUROIMPRESE (Roma),
- Joram.IT (Roma),
- OSCAR (Roma),
- RE-TI (Reggio Emilia),
- SafeNet Italy (Milano),
- SHAFT (Torino),
- SIRMI (Milano),
- TEL & CO (Modena).

2. PROTEZIONE DI SISTEMI INDUSTRIALI ED INFRASTRUTTURE

La protezione dei sistemi che controllano gli impianti industriali e le infrastrutture: segnalati attacchi e sabotaggi a sistemi di telecontrollo negli acquedotti ed a sistemi di controllo del traffico.

Due episodi negli ultimi mesi, entrambi segnalati negli USA, hanno riportato l'attenzione dei media sulla criticità di alcuni sistemi che gestiscono il controllo ed il monitoraggio di impianti ed infrastrutture.

E' di fine ottobre 2006 la segnalazione di un hacker penetrato nel sisteme di controllo per la filtrazione dell'acqua di un acquedotto vicino a Philadelphia: http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html ed è del mese di gennaio la notizia di eventi accaduti a Los Angeles che hanno messo fuori servizio alcuni sistemi di controllo di segnalamenti (semafori, ecc.) che hanno comportato disagi nel traffico per alcuni giorni (No accidents were reported, but it took four days to get the city's traffic control system fully operational): http://cbs2.com/local/local_story_008145026.html

Come emerge da diverso tempo la protezione e security dei sistemi di controllo utilizzati nell'industria e nelle infrastrutture diviene un tema attuale, ove le metodologie e le tecnologie utilizzate nell'IT tradizionale non sempre risultano adeguate.

Fonte: Enzo Maria Tieghi - Vision Automation www.visionautomation.it

3. RAPPORTO CLUSIF SUL CYBERCRIME: BILANCIO DEL 2006 E TENDENZE PER IL 2007

Come ogni anno, il CLUSIF ha presentato un rapporto sugli eventi più significativi che hanno caratterizzato l'anno precedente, in materia di cybercrime.

La presentazione è disponibile in francese (prossimamente lo sarà anche in inglese) all'indirizzo

https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k6-fr.pdf

Le riprese video della presentazione effettuata dagli esperti del CLUSIF è disponibile all'indirizzo https://www.clusif.asso.fr/fr/infos/event/#conf070118

Il rapporto di quest'anno è particolarmente interessante.

Tra gli argomenti emergenti:

- Les Mules : recrutement de particuliers
- Vol d'identité : décorticage d'une affaire
- SPIT : Nouvelles opportunités de spamming
- Manipulation de cours de bourse
- Vulnérabilités et attaques "0-Day"
- Ecoutes et enquêtes à haut risque

I rapporti degli anni precedenti sono disponibili in francese ed inglese all'indirizzo:
www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER%2DCRIMINALITE

4. LA CHIAVE DEL CYBER RISK

Segnaliamo una interessante ricerca sulla sensibilità dei manager europei al tema dei rischi informatici, disponibile all'indirizzo:

www.aceeurope.it/NR/rdonlyres/C7B2BDBC-4D75-4332-9500-608697E2ADEA/0/StrategicRISKCyberRiskReportSml.pdf

Lo scorso settembre, a Parigi, alcuni esperti del settore hanno partecipato ad una tavola rotonda organizzata per commentare la ricerca.

I lavori della tavola rotonda, con gli interventi degli esperti, sono disponibili all'indirizzo:

www.aceeurope.it/NR/rdonlyres/FEB68072-3F65-4485-9864-71FA69724124/0/EUROFORUMCyberEng.pdf

Quello del Cyber Risk è uno dei temi chiave per i Risk Manager, questo a causa della presenza di network vulnerabili e di pericoli che emergono dalle nuove abitudini di lavoro.

Organizzata da Strategic Risk Magazine e sponsorizzata da ACE European Group Ltd e da CLUSIF (Club de la Sécurité de l'Information Français) la tavola rotonda svoltasi a Parigi lo scorso settembre ha riunito esperti del settore allo scopo di discutere dei risultati dell'indagine effettuata sui rischi di natura informatica.

Dall'indagine è emerso che il 60% del campione, composto da 50 Risk Manager o IT staff in 48 compagnie e settori pubblici europei, crede che la propria organizzazione abbia solo in parte identificato come fronteggiare i rischi legati ai sistemi informativi. I rischi informatici provenienti dall'esterno e ritenuti più significativi sono: virus, hacker e divulgazione di informazioni riservate. Quelli interni invece sono frodi da parte di dipendenti e cattivo uso dei dati. I pochi sistemi di prevenzione studiati dalle aziende o dai consulenti sono rivolti principalmente al data processing error, ad attacchi inficiosi dei dipendenti, furti

o cattivo uso di dati, a danni o perdita ad attrezzature ed errori umani. Lo studio rivela inoltre che un intervistato su sette ha avuto esperienza di frodi negli ultimi 12 mesi. Tre i casi menzionati nella ricerca che hanno subito una perdita di 500.000 $, ma per altri quattro il danno è stato calcolato tra 1 e 5 milioni di $.

Per quanto riguarda le assicurazioni, è raro che tali rischi siano coperti da una polizza specifica. Le compagnie tendono a coprire tutti i tipi di danni commerciali e da interruzione di esercizio coprendo anche i rischi relativi ai sistemi informativi.

Fonte: ACE Europe www.aceeurope.it

5. CINA CONTRO US

Link: www.fcw.com/article97658-02-13-07-Web&printLayout

Feb. 13, 2007 NORFOLK, Va. --

At the Naval Network Warfare Command here, U.S. cyber defenders track and investigate hundreds of suspicious events each day. But the predominant threat comes from Chinese hackers, who are constantly waging all-out warfare against Defense Department networks, Netwarcom officials said.

Centinaia di attacchi ogni giorno al comando delle forze navali, ma gli attacchi maggiori provengono dalla Cina.

Attacks coming from China, probably with government support, far outstrip other attackers in terms of volume, proficiency and sophistication, said a senior Netwarcom official, who spoke to reporters on background Feb 12. The conflict has reached the level of a campaign-style, force-on-force engagement, he said.

Sembra una campagna contro gli USA.

Io credo che prima o poi, anche in italia, dovremo fare un ISAC www.it-isac.org

Autore: Stefano Quintarelli, Socio Fondatore e membro del Comitato Direttivo Clusit

6. I VINCITORI DEL PREMIO TESI

Il 7 febbraio, nell'ambito di Infosecurity Italia a Milano, sono state premiate le migliori tesi in Sicurezza Informatica.

Il primo premio della seconda edizione di **Innovare la sicurezza delle Informazioni**, consistente in 2.000,00 euro oltre all'adesione gratuita al clusit per il 2007, è stato attribuito ad **Andrea Beretta** (Università degli Studi di Milano, Dipartimento di Tecnologie dell Informazione - Crema) per la tesi "Metodologie e tecniche avanzate per il test di NIDS: realizzazione degli operatori di mutazione".

Il secondo premio, consistente in un corso per Lead Auditor ISO IEC 27001 (BS7799:2) del valore di 1.600 € (+IVA) oltre all'adesione gratuita al Clusit per il 2007, è stato assegnato a: **Matteo Rosi** (Università degli studi di Firenze, Facoltà di Ingegneria) per la tesi "S.T.R.E.S.S.: piattaforma per l'analisi della sicurezza di applicativi ed apparati di rete"

Gli altri 4 vincitori, premiati con l'adesione gratuita al Clusit per il 2007 sono stati:

Corona Igino (Università degli studi di Cagliari) per la tesi: "HTTPGuard, un sistema per la rilevazione di attacchi contro Web Server"

Fresi Roglia Gianpaolo (Università degli studi di Milano Bicocca) per la tesi: "Studio e realizzazione di un Anomaly Based Network Intrusion Detection System"

Maggi Federico (Politecnico di Milano) per la tesi: "Efficacia ed integrazione di sistemi di anomaly detection"

Strabla Ruggero (Università degli studi di Milano - Polo di Crema) per la tesi: "Metodologie per il test di Network Firewall".

Quest'anno il compito della Commissione che ha valutato le tesi è stato particolarmente difficile. La maggior parte delle tesi presentate era di buona qualità e, delle sei premiate, quattro avevano il livello necessario per vincere il primo premio.

I numeri di questa seconda edizione, gli abstract delle tesi premiate e le foto della premiazione sono disponibili su www.clusit.it/archivio.htm#premiotesi2007

Ancora una volta si ringraziano gli sponsor del Pemio, che ci hanno consentito di aumentare sensibilmente il montepremi di quest'anno:

7. NOTIZIE DAI SOCI

Il socio I.NET ci segnala un interessante programma di seminari gratuiti, realizzati da SPC Italia a Milano.

- 16 marzo, "Pianificare un Penetration Test"
- 23 marzo, "Luci ed ombre della tecnologia RFID"
- 27 marzo, "Legge ed ICT: La strana coppia"
- 29 marzo, "Analisi dei rischi: Come rendere «percepito» un problema «intrinseco»"
- 30 marzo, "Disabilità e accessibilità: L'implementazione della sicurezza informatica dell'e-Gov".

Per ulteriori informazioni e per partecipare ai seminari:
www.spcitalia.it/offerte/marzo07clusit.htm

AIPSI www.aipsi.org ci segnala una Tavola Rotonda del Titolo: "Le certificazioni professionali in Sicurezza Informatica", che si terrà il 7 marzo a Milano.

L'offerta di certificazioni professionali in ambito di sicurezza informatica e' estremamente variegata. Cosa vale di più sul mercato, una certificazione professionale rilasciata da un vendor, da una università o una certificazione indipendente ? Quanto sono rilevanti nel nostro paese le competenze garantite dalle certificazioni indipendenti ? Qual'e' l'offerta universitaria italiana ? Come si comportano le aziende nella selezione del personale certificato in sicurezza informatica ? Vi sono complementaritá fra le diverse offerte o le filosofie sono discordanti ?

Per ulteriori informazioni e per iscriversi online:

www.aipsi.org/eventi/#evento_f9464fcbf03af51e4ae05e2dd8a27a8e2bb51b50

8. EVENTI SICUREZZA

7-8 marzo 2007, Milano - Cisco Expo 2007
http://www.clusit.it/eventi/070307_ciscoexpo.pdf

Clusit Education

8 marzo 2007, Roma - Presentazione dei risultati del Gruppo di Ricerca AIEA-CLUSIT: "L'Outsourcing IT: best practice e Auditing"
https://edu.clusit.it/scheda_seminario.php?id=4
Sono disponibili ancora pochi posti.
La partecipazione e' gratutita per il soci Clusit, che possono registrarsi online su https://edu.clusit.it
Istruzioni per la registrazione su www.clusit.it/registrazioni2007.htm

Clusit Education

13 marzo, Milano - Seminario CLUSIT - "L'utilizzo delle strumentazioni informatiche e telematiche aziendali. Poteri di controllo e repressione degli abusi da parte del datore di lavoro"
https://edu.clusit.it/scheda_seminario.php?id=5
La partecipazione e' gratutita per il soci Clusit, che possono registrarsi online su https://edu.clusit.it
Istruzioni per la registrazione su www.clusit.it/registrazioni2007.htm

19-23 marzo 2007, Milano - Seminario CISSP
www.clusit.it/isc2/calendario_isc2.htm
Sono disponibili ancora pochi posti.

16-17 aprile 2007, Amsterdam - Forrester's Security Forum EMEA 2007
www.forrester.com/events/eventdetail?eventID=1590
(Sconto 30% per i soci Clusit)

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