Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- Imprivata international (Arese - MI)
- In Servizi IT (Brescia)
- Mr. Office (Monopoli - BA)
- Open System (Roma)
- Sisge Informatica (Rivoli - TO)
- Xtrust (gallicano nel Lazio - RM).

2. SECURITY SUMMIT A ROMA

Stiamo ultimando il programma del Security Summit di Roma (10-11 giugno).

In apertura del Summit è previsto un incontro con i rappresentanti del Governo, delle Autority di riferimento, del sistema Confindustria e delle Imprese.

Seguirà un convegno dedicato alla Sicurezza ICT in ambito Sanitario, organizzato in collaborazione con l'ospedale Pediatrico Bambino Gesù.

Moderatore: Massimiliano Raponi, Direttore Sanitario Ospedale Bambino Gesù

Interventi:

- Sicurezza e privacy: misure minime e misure adeguate - Pierfrancesco Ghedini, Direttore Sistemi Informativi e Biotecnologie AUSL Modena e Presidente AISIS – Associazione Italiana Sistemi Informativi Sanitari
- L'importanza del fattore umano: informazione, formazione, coinvolgimento e collaborazione - Andrea Oliani, AO Verona
- Verso un ospedale "senza carta" - Elio Soldano, Responsabile Sistemi Informativi ULSS 9 di Treviso
- Apparati biomedicali, applicativi informatici e reti: informatico e bioingengere a confronto - Direzione Tecnologie e Infrastruttura Ospedale Bambino Gesù

- Presentazione di uno studio per la Commissione Europea sull'utilizzo delle tecnologie RFID in Sanità - Lorenzo Valeri, RAND Europe

Un altro convegno sarà dedicato alle novità sulla sicurezza digitale nella Pubblica Am"ministrazione

Moderatore: Giovanni Manca, Responsabile Ufficio sicurezza del CNIPA

Tra gli argomenti trattati:

- L'impatto sulla PA delle recenti disposizioni del Garante per la privacy;
- Fascicolo Sanitario Elettronico e Dossier Sanitario;
- Nuove regole sull'Identità Digitale e Interoperabilità a livello Europeo;
- Nuove regole sulla firma digitale;
- Biometria e nuovi passaporti.

Sono poi previste 3 tavole rotonde:

La sicurezza delle Infrastrutture Critiche

MOderatore: Luisa Franchina, Direttore Generale del Dipartimento della Protezione Civile.
Tra l'altro, si parlerà anche dell'impatto di un evento drammatico come il terremoto in Abruzzo sull'informatica, sui database, sulla rete, sulle infrastrutture critiche locali.

Identità, sicurezza e privacy al tempo dei Social Network

Moderatore: Gigi Tagliapietra, presidente Clusit
Con la partecipazione di alcuni tra i più conosciuti blogger italiani.

Le attività delle Istituzioni Europee a supporto della sicurezza informatica e delle reti

Moderatore: Lorenzo Valeri, delegato Clusit ai rapporti con la Commissione Europea.
Con la partecipazione della Commissione Europea, dell'ENISA, di Europol e del Garante europeo per la privacy.

Nell'ambito del Summit si terranno alcuni atelier tecnologici e due percorsi professionali (di 3 sessioni ciascuno): uno di taglio tecnico ed uno sugli aspetti legali.

Si replicheranno inoltre 2 seminari Clusit già tenuti al Security Summit di Milano: "Le novità nel campo degli standard per la sicurezza IT" e "SCADA Security".

3. CYBERCRIME

Riportiamo un articolo tratto dall'ultima newsletter di ANSSAIF www.anssaif.it

IL PHISHING CAMBIA STRUMENTI E MODALITÀ

I clienti della Regions Bank, Stato del Mississipi, e Bangor Savings Bank, Maine, sono oggetto di tentativi di ottenere fraudolentemente i codici di accesso ai conti o i dati della carta di credito, via telefono. In particolare, alcuni clienti hanno avvertito di aver ricevuto comunicazione della disponibilità di una voicemail e di un nuovo numero telefonico da contattare per le operazioni bancarie, dotato di una nuovissima tecnologia. Chiaramente ai clienti viene chiesto di

digitare al telefono le credenziali in loro possesso ed utilizzate per le disposizioni tramite gli altri canali.

Un'altra tecnica è ora quella di mandare messaggi sul telefono cellulare, invitando il cittadino a chiamare un certo numero telefonico per notizie urgenti che lo riguardano, quali l'uso fraudolento del proprio conto bancario. I clienti della Citizens Bank di Pittsburgh che hanno risposto all'appello, sembra abbiano subito perdite di denaro.

Siccome gli USA sono i primi in genere a sperimentare le nuove tecniche di attacco, è forse il caso di iniziare a sensibilizzare il Cliente.

In Italia si sono avuti recentemente dei tentativi di frode tramite inserimento fraudolento di un "proxy" nel computer di alcuni ignari cittadini. Il cittadino transitava su Internet "guidato" dal criminale che, in tal modo, poteva catturargli le chiavi di accesso ad alcuni siti. Nell'unico caso di cui abbiamo tutte le necessarie informazioni, è stato accertato che (ahimè!) l'antivirus non era aggiornato da tempo.

Come si può notare dagli episodi citati, i criminali inventano sempre nuove tecniche e noi, che ci occupiamo di sicurezza, troviamo assai difficile stare dietro ad ogni novità, malgrado cerchiamo il più possibile di anticipare gli eventi.

Siccome non si può rinunciare ad utilizzare strumenti e canali che consentono di contattare un Cliente ovunque egli si trovi, bisogna educare il cittadino ad essere giustamente e correttamente sospettoso, così come del resto già dovrebbe fare quando preleva i soldi in contanti, o apre la porta di casa ad un presunto tecnico dell'ENEL o ispettore della Finanze!

Da una nostra recente indagine è emerso che quasi il 40% degli utilizzatori dell'home banking è fortemente preoccupato quando usa questi nuovi canali. A conferma della necessità di una migliore qualità dell'informazione e di investimenti nella sensibilizzazione al cybercrime.

A questo proposito, cogliamo l'occasione per annunciare che è in corso di ultimazione la scrittura di un nuovo volumetto sul furto di identità ed il cybercrime: ciò ai fini di aggiornare quello da noi redatto e pubblicato l'anno scorso, grazie al contributo di ADICONSUM.

IL PIN INTERCETTATO E DECRIPTATO?

Da notizie recenti, risulta che i criminali, considerati gli insuccessi nel phishing via email, siano riusciti ad ottenere i PIN della carta di credito o di debito tramite intercettazione durante la trasmissione tra gli ATM e il centro applicativo, decriptando il contenuto del messaggio.

Domanda: da noi è possibile?

AZIENDE BLOCCATE PER ORE A CAUSA DEL VIRUS "NEERIS"

Il nuovo virus, di tipo worm, sfruttando delle vulnerabilità del software di sistema, ha provocato un forte rallentamento delle transazioni in rete per diverse ore, per arrivare in modo ciclico (per la contemporanea divulgazione delle richieste in rete) anche a blocchi temporanei per saturazione.

Alcune aziende sono state inserite in blacklist dai Provider, in quanto generavano traffico assai elevato sulla rete pubblica, isolandole in tal modo dal mondo esterno.

Qualche nostro lettore si ricorderà che ANSSAIF segue da tempo queste tipologie di attacco (DOS), in quanto potrebbero essere attuate da bande terroriste su più larga scala, impedendo la trasmissione dei dati tra le aziende e bloccando il mercato per ore se non per giorni (ci risulta che la "patch" per eliminare l'ultimo virus sia pervenuta ad alcune aziende dopo più di 24 ore).

Ci appare quindi necessario aggiornare i piani di continuità, prevedendo tale tipologia di evento con una durata dell'indisponibilità di almeno due giorni lavorativi.

4. LE 10 TECNOLOGIE SU CUI INVESTIRE NONOSTANTE LA CRISI ECONOMICA

Un'indagine su 1.400 CIO rivela le aree in cui le aziende investono anche in caso di budget ridotti: in testa sicurezza, virtualizzazione e data center.

Di tutti i CIO alle prese con la crisi economica, e quindi con la riduzione dei budget IT, sette su dieci sono comunque convinti di dover continuare a investire su tecnologie ritenute fondamentali anche in tempi come questi: sicurezza, virtualizzazione e riduzione dei costi nei data center.

E' in sintesi il risultato di un'indagine di Robert Half Technology su 1.400 CIO in tutto il mondo, secondo la quale il 70% di essi pianifica di avviare comunque dei nuovi progetti IT nei prossimi 12 mesi, con priorità numero uno per l'area della sicurezza informatica (43%), seguita dalla virtualizzazione delle risorse IT (28%) e subito dopo dalle nuove tecnologie per rendere più efficienti i data center aziendali (27%).

"In qualsiasi scenario economico, la protezione dell'integrità, confidenzialità e disponibilità dei dati è una necessità per aziende di tutti i tipi e dimensioni - si legge nel report -. L'attenzione è massima nei settori finanziario e logistica-trasporti, dove rispettivamente il 59% e 58% dei CIO hanno intenzione di investire nella sicurezza informatica".

Altre aree piuttosto alte come priorità sono poi voice over IP (VoIP) e software-as-a-service (SaaS), in cui investirà quest'anno il 26% degli intervistati. Non a caso, entrambe queste tecnologie promettono riduzioni di costi e più flessibilità per i dipartimenti IT. Il 20% inoltre ha segnalato come area d'investimento la 'green IT', mentre il 19% inizierà progetti di business intelligence.

Di minore priorità, ma comunque di interesse di non poche aziende le aree social networking e Web 2.0 (rispettivamente il 18% e il 17% dei CIO ci investiranno), e outsourcing (16%).

"Notiamo che nonostante i tempi, molte organizzazioni sanno di non potersi permettere di rimandare gli investimenti in IT che comportano in tempi brevi più sicurezza, meno costi o maggiori entrate – commenta Dave Wilmer, executive director di Robert Half Technology -: molte stanno cercando di essere preparate quando l'economia tornerà a crescere, e per questo sentono che è indispensabile migliorare la propria infrastruttura IT".

Le 10 tecnologie irrinunciabili

1) Sicurezza informatica 43%
2) Virtualizzazione 28%
3) 'Efficientamento' dei data center 27%

4) VoIP 26%
5) Software as a service 26%
6) Green IT 20%
7) Business intelligence 19%
8) Social networking 18%
9) Web 2.0 17%
10) Outsourcing 16%

Autore: Ettore Guarnaccia

L'indagine: www.roberthalftechnology.com/PressRoom?id=2458

5. NOTIZIE DAL BLOG

30.04 - Abrogato l'emendamento D'Alia

http://blog.clusit.it/sicuramente/2009/04/abrogato-lemendamento-dalia.html

24.04 - Symantec presenta l'Internet Security Report per il 2008

Autore: Armando Leotta

http://blog.clusit.it/sicuramente/2009/04/symantec-presenta-l-internet-security-report-per-il-2008.html

22.04 - Attacco ai sistemi informatici del Pentagono: sottratti i piani del caccia F35

http://blog.clusit.it/sicuramente/2009/04/attacco-ai-sistemi-informatici-del-petagono-sottratti-i-piani-del-caccia-f35.html

L'approfondimento di Armando Leotta:

http://blog.clusit.it/sicuramente/2009/04/attacco-ai-sistemi-informatici-del-petagono-sottratti-i-piani-del-caccia-f35.html#comments

15.04 - Sciacallaggio tecnologico: il phishing alla Croce Rossa Italiana

Autore: Armando Leotta

http://blog.clusit.it/sicuramente/2009/04/sciacallaggio-tecnologico-il-phishing-alla-croce-rossa-italiana.html

07.04 - In USA una proposta di legge per creare il Capo della Cybersecurity

http://blog.clusit.it/sicuramente/2009/04/in-usa-una-proposta-di-legge-per-creare-il-capo-della-cybersecurity.html

05.04 - Se security è (anche) continuity...

Autore: Mauro Cicognini

http://blog.clusit.it/sicuramente/2009/04/se-security-%C3%A8-anche-continuity.html

03.04 - Fascicolo Sanitario Elettronico e Dossier Sanitario

Autore: Luca Bechelli

http://blog.clusit.it/sicuramente/2009/04/fascicolo-sanitario-elettronico-e-dossier-sanitario.html

02.04 - Security is a lifestyle...

http://blog.clusit.it/sicuramente/2009/04/security-is-a-lifestyle.html

6. 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

Nei giorni 7, 8 e 9 maggio si terrà a Bologna l'IISFA Forum 2009 & Cybercop 2009.

Programma e scheda di iscrizione:
www.iisfa.it/IISFA_FORUM_2009_P.pdf

Nei giorni 9 e 10 maggio si terrà ad Assisi il XX Congresso Nazionale dell'Associazione Informatici Professionisti.

Per maggiori informazioni ed iscrizioni: www.congresso.aipnet.it

AUSED invita tutti gli amici e simpatizzanti dell'Associazione al tradizionale Convegno Nazionale dei Direttori Sistemi Informativii che quest'anno festeggia i trentatre anni di vita associativa. Il Convegno si terrà il 21-5-09 al Circolo della Stampa di Milano.

La locandina dell'evento è disponibile su
www.aused.org/attachments/269_Convegno_2009_3ante.pdf

Nei giorni 21 e 22 maggio si svolgerà a Pisa il XXIII Convegno Nazionale di IT Auditing, Security e Governance, organizzato da AIEA.

Per maggiori informazioni ed iscrizioni:
www.aiea.it/html/pisa_2009.html

Il 9 giugno si terrà a Roma il Congresso Nazionale romano di itSMF.

Informazioni e scheda d'iscrizione:
www.itsmf.it/index.php?method=section&action=zoom&id=1066

La Facoltà di Economia - Università di Roma "Tor Vergata" ci segnala il "Premio di studio per tesi in comunicazione delle organizzazioni universitarie e di ricerca" indetto da Aicun con scadenza 31 dicembre 2009. Per maggiori informazioni:
www.economia.uniroma2.it/Public/files/img_news/file/locandina.pdf

7. EVENTI SICUREZZA

5 maggio 2009, Roma
Seminario Clusit "Identity Management"
https://edu.clusit.it/scheda_seminario.php?id=35

11-15 maggio 2009, Monza
Seminario CISSP
http://www.clusit.it/isc2/calendario_isc2.htm

15-16 maggio 2009, Krakow
CONFidence 2009
http://2009.confidence.org.pl/lang-pref/en

10-11 giugno 2009, Roma
Security Summit 2009
http://securitysummit.it

13 giugno 2009, Monza
Esami (ISC)²
www.clusit.it/isc2/calendario_isc2.htm

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