Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- AT4M (Jesi - AN)
- OGS (Milano)

2. INFOSECURITY, CLUSIT E SECURITY SUMMIT

Per otto anni il clusit è stato il partner scientifico di **Infosecurity Italia**, che è sicuramente il più importante evento in Italia nel settore della sicurezza informatica. In questi anni la manifestazione è cresciuta assieme a noi, ci ha apportato grande visibilità e ci ha permesso di sviluppare molte iniziative. Di fatto, l'abbiamo sempre considerata come la *nostra* manifestazione.

Ora, nel momento in cui la Reed Exhibitions ha preso la decisione di sospendere la manifestazione, in considerazione del fatto che "il mercato dell'Information Technology nel nostro paese si sta orientando verso altri strumenti di promozione diversi dagli eventi fieristici di taglio tradizionale", il Clusit ha deciso di mantenere, con l'aiuto di alcuni partner, questo fondamentale appuntamento.

La nuova manifestazione, che vedrà un considerevole coinvolgimento dei soci, si chiamerà **Security Summit** e la prima edizione si terrà nei giorni **24, 25 e 26 marzo 2009, a Milano**, e nel mese di **giugno a Roma**.

Intendiamo superare il format ormai logoro di eventi dalla spiccata fisionomia fieristica per concentrarci invece su un format innovativo, caratterizzato da contenuti culturali di alto livello, keynote speaker di profilo internazionale e in generale una forte attenzione alla qualità. Per far questo stiamo mettendo a punto un programma convegnistico che vedrà sessioni plenarie, seminari di approfondimento, tavole rotonde, sessioni verticali ecc. in una varietà e articolazione di offerta culturale che permetta al partecipante di costruirsi un percorso professionale di approfondimento su misura.

Fortemente basato sulla possibilità di interazione dei partecipanti, il **Security Summit**, oltre alle tematiche tipiche del mondo business, svilupperà anche una

attenzione particolare a quelle della sicurezza in rete per i cittadini: i risparmiatori, le famiglie, i più giovani e gli anziani.

Per realizzare questo ambizioso progetto avremo bisogno dell' aiuto e dei suggerimenti di tutti i soci, per costruire assieme un evento veramente innovativo: originale, accattivante e di gran qualità.

3. LA SICUREZZA INFORMATICA COME L'IMMONDIZIA

Riportiamo integralmente un articolo del *Prof. Bruschi*, scritto alcune settimane or sono, in piena "emergenza immondizia".

La Sicurezza Informatica come l'immondizia

In questi giorni il problema dell'immondizia ha di nuovo rivitalizzato le cronache. Al di là dei diversi risvolti che caratterizzano il problema, descritti in tono più o meno approfondito dai media, c'è un aspetto che ci sembra stia sfuggendo alle considerazioni dei più. Siamo difatti di fronte ad un esempio da manuale di come la classe dirigente di questo paese è abituata a risolvere i problemi: rinviarne la soluzione sino a che il problema non "esplode". Un atteggiamento che può rivelarsi vincente in alcuni casi, un pò meno in altri, come appunto l'immondizia e la sicurezza informatica. Si tratta di due problemi che nonostante la loro diversa natura condividono non poche affinità concettuali. In entrambi i casi infatti ci troviamo di fronte ad un problema che è generato dall'assenza di una classe dirigente consapevole e competente, che sappia predisporre opportuni interventi preventivi, al fine di calmierare e tenere sotto controllo il fenomeno e contemporaneamente predisponga efficaci piani di disaster recovery.

Nel caso dell'immondizia le misure preventive che dovevano essere messe in atto erano di fatto la raccolta differenziata accompagnata da un programma di sensibilizzazione rivolto alla popolazione, e l'istituzione di opportune infrastrutture di supporto quali centri di riciclaggio, centri di compostaggio e termovalorizzatori. Nulla di ciò è stato fatto, il problema con l'andare del tempo si è acutizzato e i risultati sono oggi sotto gli occhi di tutti. Il problema ha assunto dimensioni nazionali, il danno di immagine per il paese non è quantificabile e la soluzione al problema non sarà immediata. Si tratta di un problema principalmente culturale; usanze ed abitudini delle persone non si cambiano certo nell'arco di qualche mese e men che meno con il ricorso a misure costrittive.

Nel caso della sicurezza informatica le misure che, come comunità di esperti, da anni chiediamo siano messe in atto sono la diffusione di tecnologie di protezione e la responsabilizzazione e il coinvolgimento degli utenti finali, oggi, il principale obiettivo della criminalità informatica. Queste iniziative dovrebbero essere supportate, a più alto livello, dalla costituzione di centri di ricerca e centri per la raccolta e l'analisi di eventi anomali, centri con capacità di intervento in caso di incidenti informatici (i cosi detti **C**omputer **E**mergency **R**esponse **T**eam). Questa è tra l'altro la direzione in cui si stanno muovendo da anni i maggiori paesi industrializzati. Ovviamente, nulla di tutto ciò non solo non è stato realizzato ma non si trova nell'agenda dei nostri dirigenti per gli anni a venire.

Come nel caso dell'immondizia il problema è destinato a degenerare e inevitabilmente con l'andare del tempo, nel nostro paese si creeranno grossi

cumuli di immondizia informatica, cioè centinaia di miglia di PC infettati all'insaputa dei loro legittimi proprietari, i cosi detti BOT. Questi PC saranno controllati da malviventi, che li utilizzeranno per compiere le più svariate attività illecite a danno di tutti gli utenti della rete, tra cui il furto di brevetti industriali, di informazioni commerciali, di identità digitali e ovviamente di denaro. In questo senso siamo già sulla buona strada, Cagliari Milano e Roma sono tra le 10 città europee con il maggior numero di PC infettati.

In questo caso però non sarà facile individuare soluzioni immediate al problema. Il problema non sarà circoscrivibile ad una particolare area geografica, avrà ripercussioni globali che andranno ben oltre la perdita di immagine, l'"odore" dell'immondizia informatica si diffonde alla velocità della luce in tutto il globo, contaminando i PC che incontra sulla sua strada. Ad essere compromessa non sarà solo l'immagine del nostro paese ma la sua struttura produttiva, la sua competitività e la sua credibilità di paese tecnologicamente avanzato. Unica consolazione, l'immondizia informatica non puzza!!

Danilo Bruschi
Ordinario di Informatica
Università degli Studi di Milano
Presidente Onorario Clusit

4. CYBERCRIME

Banche poco sicure online?

Ricercatori dell' Università del Michigan hanno avviato una ricerca nel 2006 finalizzata ad analizzare i siti web di 214 banche.

Ricerca che è nata quasi per caso su iniziativa del Prof. Atul Prakash (del dipartimento di Electrical Engineering e Computer Science), in collaborazione con un paio di dottorandi dell'università), a seguito di una esperienza poco positiva con l'home banking della sua banca subita da Prakash.

I risultati della ricerca sono stati sconcertanti ed hanno portato a concludere che i siti web per l'home banking sono molto meno sicuri del previsto dal momento che sono state scoperte numerose falle di sicurezza ed errori di progettazione potenzialmente pericolosi per la privacy e la protezione dei dati di accesso dei clienti: malfunzionamenti che spesso, purtroppo, non possono essere risolti con una semplice patch, ma solamente con una radicale riprogettazione dei siti.

Il 75% dei siti web ha, infatti, evidenziato la presenza di almeno una falla in grado di mettere seriamente a rischio la sicurezza degli utenti nel corso dello svolgimento delle più comuni operazioni di home banking come consultare i dati del proprio conto corrente, emettere e ricevere bonifici.

Uno dei problemi maggiormente riscontrati dalla ricerca interessa il mancato utilizzo delle tecnologie per la criptazione dei dati nel corso delle fasi di login. I certificati SSL (Secure Sockets Layer) non sono utilizzati nelle pagine di login dal 47% dei siti web delle banche, una mancanza che potrebbe consentire a un malintenzionato di sottrarre facilmente le informazioni di accesso degli utenti, permettendogli di avere il pieno controllo sul conto corrente online. Lo scarso

utilizzo di certificati SSL si rivela pericoloso non solo nelle pagine per effettuare il login e compiere le operazioni di home banking, ma anche nelle sezioni dei siti dedicate all'assistenza ai clienti.

Quasi tutte le istituzioni bancarie, inoltre, per fornire informazioni, servizi aggiuntivi e dettagli di vario genere sulle opportunità offerte dalla gestione online del proprio conto, offrono ai loro utenti servizi di assistenza telefonica e via email. Nel 55% dei casi, i dati per poter usufruire di tali funzionalità sono generalmente contenuti in pagine non protette e particolarmente vulnerabili.

La ricerca ha, inoltre, evidenziato come il 30% dei siti web analizzati rimandino ad altri domini per effettuare il login e accedere al proprio conto. Tale pratica spingerebbe gli utenti a sottovalutare i rischi derivanti da un dirottamento malevolo da parte dei pirati informatici (phishing), generalmente teso a proporre un sito del tutto simile all'originale, ma concepito unicamente con lo scopo di sottrarre i dati di accesso dei clienti della banca. Per risolvere il problema, gli istituti di credito dovrebbero ospitare i servizi di home banking sui medesimi server su cui sono ospitati i loro siti istituzionali, abituando così gli utenti a rimanere sul medesimo dominio, senza il rischio di strani e pericolosi dirottamenti.

Lo studio, infine, ha messo in evidenza come le politiche attuate dalle banche per la gestione dei dati di accesso siano nel 28% estremamente carente sul lato della sicurezza, per la mancanza di regole sufficientemente rigide. Mancanza di regole che induce spesso gli utenti a elaborare password e ID molto semplici e facilmente ricordabili, ma anche maggiormente esposte ai problemi di sicurezza. Anche in questo caso, una maggiore attenzione verso dettagli così importanti da parte delle banche potrebbe scongiurare il rischio di brutte, spiacevoli e costose sorprese per i loro clienti.

Nelle Istituzioni Creditizie Italiane, per fortuna, non viene sottovalutata la sicurezza online.....O NO ??????

Per maggiori informazioni (in lingua Inglese):
www.ns.umich.edu/htdocs/releases/story.php?id=6652

Per maggiori informazioni (in Spagnolo):
www.umich.edu/Es/news/08/pr080722.php

Per scaricare un abstract della ricerca: www.anssaif.it/allegati/Atul_Falk.pdf

Autore: Antonio Caricato
Tratto dalla Newsletter ANSSAIF - www.anssaif.it

5. DUE NUOVE PUBBLICAZIONI DEL NIST

NIST, National Institute for Standards and Technologies ha segnalato la disponibilità di due nuove pubblicazioni, quanto mai attuali.

La prima, intitolata **Guide to SSL VPNs** esplora l'ambito delle SSL VPN, tecnologia che sta guadagnando sempre più popolarità rispetto al "tradizionale" approccio IPsec. Si parte dalle tecnologie su cui si fondano le SSL VPN per passare poi a scenari d'implementazione e raccomandazioni d'uso.

Il documento è disponibile su http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

La seconda pubblicazione è ancora in draft (e quindi può essere commentata prima della chiusura e pubblicazione) ed offre linee guida sulla sicurezza di cellulari e palmari: **Guidelines on Cell Phone and PDA Security**. Con l'uso sempre più massiccio di dispositivi mobili e palmari; con telefoni cellulari con intelligenza crescente; con un ambito d'azione che parte dal semplice telefono per arrivare all'integrazione di calendario, email, contatti, telefono e accesso alle risorse aziendali, diventa imperativo chiedersi quali considerazioni sono da fare per migliorare l'effettivo livello di sicurezza di questi dispositivi. La pubblicazione offre alcune linee guida da applicare per un utilizzo sicuro.

Il Draft è disponibile su http://csrc.nist.gov/publications/drafts/800-124/Draft-SP800-124.pdf

Autore: Marco Misitano

6. BLUETOOTH PERICOLOSO PER LA PRIVACY?

Il bluetooh, tecnologia che consente di sincronizzare i dati di un dispositivo con quelli di un altro e di trasferirli, può essere pericolosa per la privacy.

Questa scoperta discende da un progetto (denominato Cityware) condotto dall'Università inglese di Bath avviato per studiare e capire i movimenti delle persone nelle città.

Tre anni fa i ricercatori hanno installato nelle vie della città alcuni scanner, riuscendo a raccogliere informazioni da cellulari, computer e altri apparecchi portatili: quattro ricevitori Bluetooth sono stati posizionati nel centro cittadino e dopo quattro mesi di rilevazioni sono stati raccolti 10 mila segnali di telefoni dotati della tecnologia in questione. In pratica i ricercatori sono riusciti a ricostruire gli incontri delle persone nei negozi e nei locali.

Dalla cittadina di Bath il progetto si è poi esteso a livello mondiale, con installazione di scanner nelle città di San Diego, Hong Kong, Singapore, Toronto e Berlino. Le informazioni raccolte sono poi finite nel database centrale situato a Bath, che ha in pratica tracciato oltre 250.000 possessori di dispositivi con tecnologia Bluetooth.

PRIMI RISULTATI DEL PROGETTO:

invito rivolto alle persone a disattivare il Bluetooth, ovvero, a inserire la password, pena il rischio/certezza, in caso contrario, che informazioni riservate finiscano in mano a persone malintenzionate o all'industria dell'advertising, che potrebbe sfruttarle per realizzare campagne pubblicitarie ancora più mirate di quelle attualmente presenti sul mercato.

Maggiori informazioni sul sito dell'Università:
www.cs.bath.ac.uk/pervasive/projects/malware.html

Autore: Antonio Caricato

Fonte: Newsletter ANSSAIF - www.anssaif.it

7. LA FCC PUBBLICA LA BOZZA DEL SUO PIANO STRATEGICO

La FCC (Federal Communications Commission) pubblica la bozza del suo piano strategico.

La notizia non è che ha un piano strategico nè che lo pubblichi nè che pubblichi le bozze (che si trovano sul sito della Commissione www.fcc.gov/omd/strategicplan).

La notizia sono alcuni dei suoi obiettivi:

Objective 2: The Commission shall evaluate and strengthen measures for protecting the Nation's critical communications infrastructure.

The Commission shall provide strong leadership to industry and other governmental agencies in the protection of the Nation's critical communications infrastructure. The Commission must explore all available ways to work collaboratively with industry to increase network diversity and redundancy and maximize the availability, interoperability, and reliability of all communications. The Commission shall work with industry and government both at home and abroad to establish Best Practices that should be adopted by communications providers.

Objective 3: The Commission's policies shall facilitate rapid restoration of the U.S. communications infrastructure and facilities after disruption by any cause.

Protection of the Nation'scritical communications infrastructure requires that the Commission adopt policies to ensure rapid restoration of communications after disruptions due to any cause. The Commission shall work collaboratively with industry, other governmental agencies, and foreign counterparts to coordinate and engage in outreach to develop standards for Emergency Telecommunications Services (ETS); to increase awareness of the TSP and WPS programs; to stimulate participation in the TSP and WPS programs by 911 Centers, first responders, and federal, state, tribal, and local governmental agencies; to propose ways of making TSP and WPS participation more affordable; to identify obstacles to TSP and WPS participation; and to recommend changes to overcome such obstacles.

The Commission shall also work collaboratively with the satellite industry and other governmental agencies to identify and ensure the availability of facilities for restoration of satellite and other services.

In addition, the Commission shall explore all availableways to ensure that all emerging technologies, networks, and services are reliable, interoperable, redundant, and rapidly restorable.

Objective 4: The Commission shall coordinate with industry and other federal, state, tribal, and local agencies on matters of public safety, homeland security, and disaster management.

Over 90 percent of the Nation's communications infrastructure is privately owned. Cooperation and coordination among industry, public safety organizations, and federal, tribal, state, and local governments is therefore essential to the successful nationwide implementation of critical infrastructure protection, public safety communications interoperability, and effective public alert and warning systems.

Accordingly, the Commission shall coordinate with private industry to develop policies that will further the vision, goals, and objectives of public safety, homeland security, and disaster management.

Autore: Stefano Quintarelli

8. EVENTI SICUREZZA

2-7 agosto 2008, Las Vegas
Black Hat Briefings & Training USA
www.blackhat.com/html/bh-usa-08/bh-us-08-main.html

8-10 agosto 2008, Las Vegas
DEFCON 16
www.defcon.org

8-11 settembre 2008, Asterdam
SANS Process Control & SCADA Security Summit 2008
www.sans.org/euscada08_summit

16 settembre 2008, Milano
Seminario Clusit - La Sicurezza fisica: implementazioni concrete
https://edu.clusit.it/scheda_seminario.php?id=26

16-17 settembre 2008, Rotterdam
Govcert.NL Symposium
www.govcertsymposium.com

7 ottobre 2008, Milano
Oracle Security Symposium - Gli strumenti di Sicurezza per l'Information Security Governance e il GRC
www.oracle.com/global/it/events/symposium/index.html

7 ottobre 2008, Roma
Seminario Clusit - La Sicurezza fisica: implementazioni concrete
https://edu.clusit.it/scheda_seminario.php?id=27

7-8 ottobre 2008, Milano
Insurance IT Forum 2008 - Sconto di 200 € per i soci Clusit
www.iir-italy.it/upload/general/D3945D15.pdf

7-9 ottobre, Madrid
Information Security Solutions Europe (ISSE) 2008
www.isse.eu.com

8-9 ottobre 2008, Roma
Forum Expo ICT Security
www.nstecna.com/eventi/ict2008/index.php

20-24 ottobre 2008, Roma
Seminario CISSP
www.clusit.it/isc2/calendario_isc2.htm

27-29 ottobre 2008, London
RSA Conference Europe 2008
www.rsaconference.com/2008/Europe/Home.aspx

22 novembre 2008, Roma
Esame CISSP
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