Indice

1. NUOVI SOCI

Hanno aderito al Clusit:

- A&T Consulting (Roma);
- Regione Lombardia (Milano);
- Omedra (Rovereto - TN).

2. SANS AGGIORNA LE TOP 20 INTERNET SECURITY VULNERABILITIES

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

Approvata la legge di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica.

Dopo l'approvazione il 20 febbraio 2008 da parte della Camera dei deputati, il Senato ha definitivamente approvato il disegno di legge A.S. n. 2012 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno".

Il disegno legge è disponibile sul sito del Senato.

www.senato.it/japp/bgt/showdoc/showText?tipodoc=Ddlmess&leg=15&id=00298813&offset=445&length=26672&parse=no&stampa=si

Sicurezza in Internet: un sito su mille è pericoloso.

Google ha studiato il grado di pericolosità dei siti Web, ossia la capacità che questi hanno di trasmettere al computer dell'utente malware o virus. Il risultato è che 1 sito su 1000 è infetto, ossia una totalità di oltre tre milioni di siti.

Nella ricerca di Google vengono anche elencati i paesi da cui più frequentemente provengono siti dannosi per i navigatori. Al primo posto ci sono i siti cinesi, da cui proviene il 67% dei casi di siti virulenti. A seguire, per quello che riguarda i siti di distribuzione dei malware, ci sono gli Stati Uniti, con il 15%, e la Russia, con il 4%. Nella top ten poi ci sono la Malesia con il 2,2%, la Corea con il 2%, Panama con l'1,1%, la Germania con l'1%, Hong Kong, la Turchia e la Francia con percentuali inferiori all'1%.

Un altro aspetto dello studio riguarda la frequenza con cui un utente che esegue una ricerca su un motore come Google si imbatte in un sito infetto: la quota è dell'1,3%.

È possibile visionare/scaricare lo studio completo su:
http://research.google.com/archive/provos-2008a.pdf

Fonte: ANSSAIF - www.anssaif.it

Nuovo Trojan per cellulari.

Si sta diffondendo in maniera massiccia un nuovo tipo di trojan che ha l'obiettivo di "sequestrare" i dati memorizzati su uno Smartphone o pDA-Phone e di rilasciarli solamente dietro il pagamento di un riscatto. Scaricando, anche via Bluetooth, un'applicazione apparentemente innocua, la stessa si annida nel dispositivo per infettarlo con una serie di virus e genera un SMS che compare sul display dello stesso apparecchio. Il proprietario dell'hardware si vede in sostanza apparire un messaggio (in lingua inglese) del tipo (tradotto) "Attenzione, il tuo apparecchio è infetto. Per favore, prepara 50 yuan e poi contatta il numero QQ nnnnnnnnn". In pratica si richiede l'equivalente di circa sette euro per il "rilascio" dei dati presi in ostaggio, da versare mediante un sistema di pagamento online. Gli apparecchi colpiti sono solitamente quelli dotati di sistema operativo Symbian e, oltre a blindarne i dati contenuti, tenta di carpire informazioni tecniche (come la versione del sistema utilizzato sullo smartphone) e capaci di identificate l'apparecchio (come il codice IMEI). Il suggerimento è sempre lo stesso, da applicarsi con adeguati accorgimenti tanto nel mondo dei computer quanto su quello degli smartphone: non acconsentire mai l'installazione di un'applicazione sconosciuta dopo il download di un file, soprattutto se proveniente da una fonte non conosciuta.

Fonte: ANSSAIF - www.anssaif.it

4. DIFENDERSI DAGLI SPAM-BOT

Come si poteva facilmente prevedere, la battaglia con gli spammer sta dimostrando una nuova escalation.

I punti d'attacco preferiti dagli spammer sono ovviamente gli account gratuiti di servizi quali Hotmail, Yahoo, Gmail, o anche i nostri Libero, Katamail, e così via. Poter spedire da uno di questi account significa poter aggirare numerose blacklist, ed anche parecchi filtri basati sulla reputazione del mittente, perché ovviamente non è possibile rifiutare

posta integralmente da questi domini, e farlo per singola casella è comunque oneroso.

Praticamente tutti questi fornitori richiedono, durante la registrazione, di riconoscere ed inserire una stringa alfanumerica più o meno "oscurata" distorcendone i caratteri, modificandone lo sfondo, sovrapponendo righe ed altri disturbi, sistema che viene definito con la sigla CAPTCHA . Teoricamente, per un essere umano è comunque facile venirne a capo, e per una macchina è difficilissimo.

Teoricamente: perché, con il continuo miglioramento dei software OCR, per le macchine diventa sempre più facile. I CAPTCHA diventano quindi sempre più oscurati, al punto che oggi non è facile nemmeno per una persona riconoscere la scritta.

Come peraltro riporta un articolo di Network World www.networkworld.com/news/2008/041108-bot-breaks-hotmails-captcha-in.html?netht=rn_041508&amp, è stato rilevato un bot che si installa, come spesso accade, su un PC di un ignaro utente vulnerabile, e da lì tenta subito di registrare nuovi account su Hotmail per poi usarli per inviare spam. A quanto pare impiega circa sei secondi per riconoscere il CAPTCHA di Hotmail, ed anche se in realtà lo fa correttamente solo una volta su dieci, il punto è che ottiene comunque in breve tempo una grande quantità di account (in apparenza legittimi) da usare per inviare spam e potenzialmente replicarsi.

Finora i CAPTCHA sono stati un po' il chinino dei freemail via Web, ma sembra che la loro malaria ormai sia diventata resistente. Occorre urgentemente trovare una molecola più efficace.

Autore: Mauro Cicognini

5. NOTIZIE DALL'EUROPA

Nuovo programma della Commissione europea per la sicurezza dei minori su internet

Recentemente la Commissione europea ha proposto un nuovo programma per una maggiore sicurezza dei minori che navigano in linea. Di fronte alla diffusione recente di servizi di comunicazione del web 2.0, come i siti di socializzazione, il nuovo programma intende lottare non solo contro i contenuti illeciti, ma anche contro comportamenti dannosi come il bullismo in linea e l'adescamento in rete a scopi sessuali. Basandosi sul successo del precedente programma del 2005, il nuovo programma fruisce di una dotazione di bilancio di 55 milioni di euro e abbraccia il periodo 2009-2013.

Maggiori dettagli nel comunicato stampa della Commissione europea.

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/310&format=PDF&aged=0&language=IT&guiLanguage=fr

Nuovo portale dell'Unione Europea sulla sicurezza.

Il portale della DG Information Society dedicato alla sicurezza delle informazioni è stato ridisegnato e modificato.

http://ec.europa.eu/information_society/policy/nis/index_en.htm.

Da segnalare la disponibilità delle relazioni del seminario di fine 2007 sul tema della security awareness

http://ec.europa.eu/information_society/policy/nis/strategy/activities/awareness_seminar/index_en.htm, particolarmente utile e interessante, soprattutto la presentazione del prof Riguidel del ENST di Parigi http://ec.europa.eu/information_society/policy/nis/docs/wshop/keynote_speech_riguidel.pdf.

Report - attacchi su larga scala.

La DG Internet Society ha pubblicato il report dell'incontro di gennaio che ha analizzato le implicazioni che derivano dagli attacchi su larga scala.

Il report è disponibile su
http://ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/Report_Internet_Security_WS_170108.pdf

Le relazioni e le slide su
http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.htm

Interessanti calls for proposal.

C'è "fermento" alla UE in tema di sicurezza e sicuramente ci possono essere opportunità per i soci CLUSIT, cui raccomandiamo di leggere con attenzione i "Call for proposal" che potrebbero essere interessanti per le imprese o anche per i singoli.

Qui di seguito ne segnaliamo uno con scadenza a breve che vale la pena di leggere.

http://blog.clusit.it/sicuramente/2008/04/attenzione-ai-c.html#more

Gruppo di lavoro di ENISA sulle microimprese.

Qualche giorno fa ho partecipato a nome del CLUSIT alla prima riunione del gruppo di lavoro di ENISA (European Network and Information Security Agency) sulle microimprese. I problemi di sicurezza delle piccole imprese e delle microimprese sono gli stessi in tutta Europa, e quindi la collaborazione a questo livello può aiutare ad affrontare un settore che, dati i numeri in gioco (milioni di piccole imprese e microimprese) richiede una strategia e strumenti specifici. Per ora posso dire che lo scambio di informazioni e di esperienze all'interno del gruppo è estremamente interessante, e aiuterà il CLUSIT nelle sue iniziative in questo settore. Prossimamente vi darò maggiori informazioni sia sull'attività del gruppo di lavoro di ENISA che sulle iniziative del CLUSIT per le PMI.

Autore: Claudio Telmon, coordinatore del progetto Clusit ***Rischio IT e piccola impresa***

6. NOTIZIE DAGLI USA

L'FBI chiede un punto di controllo per il filtraggio di tutte le comunicazioni online in USA

Il Direttore dell' FBI Robert Mueller ha chiesto di poter monitorare tutte le attività illegali su Internet. Il dibattito, che non è nuovo, non può che suscitare preoccupazioni per la privacy ed i diritti degli utenti. È legittimo (anzi doveroso) cercare delle soluzioni per contrastare le attività criminali che si svolgono in rete. Il problema è, come sempre, il rischio di abusi.

Vedi l'articolo su www.news.com/8301-10784_3-9926899-7.html

Fonte: http://blog.quintarelli.it

La sicurezza si studia sui banchi di scuola.

Si segnala che negli Stati Uniti, nello stato della Virginia, la sicurezza sul Web è divenuta una nuova materia di insegnamento: i ragazzi vengono istruiti riguardo ai pericoli che corrono in rete e vengono addestrati all'autodifesa sul Web. A disporre che la materia entri a far parte del piano formativo dei ragazzi fra gli 11 e i 16 anni, è stato il Ministero dell'Istruzione locale: i corsi sono attivi, alcuni ragazzi sono attenti, alcune famiglie sono felici di delegare alle agenzie educative un compito che sono restie ad assumersi o, molto più spesso, che non sono in grado di svolgere.

Dove non arrivano le famiglie, arriva lo stato: la Virginia è il primo stato a rendere obbligatorie le lezioni di educazione alla sicurezza online, anche se i corsi si svolgono anche nelle scuole di Texas e Illinois. Sono inoltre numerosi i governi che stanno valutando l'introduzione di analoghi provvedimenti, spinti dalla crescente apprensione dei genitori nei confronti di dati e vicende a cui i media fanno da cassa di risonanza.

L'azione informativa in Virginia non si rivolge ai soli studenti come una costrizione, ma si coinvolgono le stesse famiglie per educarle ad una vigilanza responsabile dei propri figli mediante:

- una descrizione dei filtri e di tecnologie di "parental control"
- invitando i genitori a non abbandonare i ragazzi davanti allo schermo,
- invitando i genitori a stabilire con i ragazzi un dialogo che li educhi a schivare i pericoli che gli si parano di fronte, dentro e fuori dallo schermo.

Una guida proposta da "Virginia Department of Education", dal titolo "INTERNET SAFETY IN SCHOOL", è disponibile su

www.anssaif.it/allegati/internet-safety-guidelines-resources.pdf

Fonte: ANSSAIF - www.anssaif.it

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

Azienda ricerca Stagista.

L'Ufficio Information Securiy and Privacy di un'Azienda industriale di primaria importanza cerca una figura da inserire nella propria organizzazione. Tutte le informazioni utili sono sul sito web dell'azienda

http://bosch.easycruit.com/vacancy/172257/22053?iso=it

Il socio Data Security ci segnala un corso di Ethical Hacking

www.clusit.net/vetrina_soci/data_security.pdf

Azienda ricerca agente con esperienza in ambito networking e sicurezza informatica.

Società di consulenza ed assistenza informatica ricerca un agente mono/plurimandatario con esperienza di vendita nel settore dei servizi informatici. Si ricerca una persona di 25/35 anni, che si occupi di vendere servizi in ambito networking e sicurezza informatica nell'area di Milano e provincia. Chi fosse interessato può scrivere a info@clusit.it

IISFA Forum 2008.

Sono terminati i lavori dell'IISFA Forum 2008, svoltosi all'Università di Bologna il 18 e 19 aprile, che ha trattato di "Tecnologia, criminalità e attività investigativa: dal data retention alla computer forensic alla luce dell'attuazione della Diretiva 2006/24/CE e della ratifica della Convenzione di Budapest". Durante il Forum si è svolto il 1° Concorso nazionale a squadre sulle indagini informatiche e computer forensic. Le immagini dell'evento e gli atti del convegno sono disponibili sul sito dell'IISFA www.iisfa.it/cybercop2008.html.

8. EVENTI SICUREZZA

22 maggio 2008, Roma *
Seminario Clusit - Computer forensics: aspetti legali e strumenti operativi

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

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

10-11 giugno 2008, Roma
Infosecurity Italia - Storage Expo - trackability

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

* Posti esauriti
** La registrazione ai seminari, temporaneamente sospesa per motivi tecnici, sarà disponibile entro alcuni giorni su https://edu.clusit.it

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