Indice

1. NUOVI SOCI

Durante l'ultimo mese hanno aderito al CLUSIT le seguenti organizzazioni:

- ABACO (Verona),
- URIZEN (Napoli).

2. DPS AL 31 DICEMBRE

Il Documento Programmatico sulla Sicurezza slitta al 31 dicembre 2004.

Chi non potrà adottare le misure di sicurezza richieste, avrà tempo fino al 31 marzo 2005.

Nel frattempo, numerose sono le aziende che si sono già adeguate alle misure minime di sicurezza e che hanno aggiornato le proprie procedure e le informative secondo quanto previsto dal dlg 196/2003, non trascurando un opportuno piano di formazione per i Responsabili e gli Incaricati del trattamento dei dati.

Ci auguriamo che lo slittamento permetterà a molte altre aziende di mettersi in regola e non contribuirà invece a banalizzare il problema e ad abbassare il livello di attenzione.

3. INNOVAZIONI TECNOLOGICHE E PRIVACY

Nei giorni 17 e 18 giugno l'Autorità Garante per la protezione dei dati personali ha tenuto due giornate di riflessione su "Innovazioni tecnologiche e privacy. Il diritto alla protezione dei dati tra sicurezza, efficienza e sviluppo".

Potete leggere il resoconto dei lavori su:
http://key4biz.metsviluppo.it/index.jsp?notizia=144525&urlChiamata=visNotizia.jsp

4. COMPUTER CRIME

Gli attacchi di "Phishing" aumentano e si perfezionano.

Secondo notizie apparse su diversi siti negli ultimi giorni, questa tipologia di attacco è aumentata e si è perfezionata.

Infatti, nel solo mese di Aprile gli attacchi di questo tipo sono cresciuti del 178% rispetto al mese precedente.

Le "esche" lanciate sul Web sono ora di tre tipi:

- Email che invita ad accedere al sito della banca per ottenere il nuovo pin di sicurezza (gli ultimi colpiti sono stati i clienti russi della Citybank);

- Email contenente un avviso di addebito in conto, di un importo non indifferente, per l'acquisto, ad esempio, di un pc; maggiori dettagli il destinatario li può trovare nel sito indicato nella email; per accedere al sito viene poi richiesta la userid e la password, in modo da poterla catturare;

- Email con avviso analogo al precedente, ma il destinatario, accedendo al sito, riceve sul computer un programma "trojan" che si metterà in "ascolto" e provvederà a raccogliere i dati digitati dal cliente sul suo pc e, successivamente, ad inviarli all'hacker o ad una banda criminale; in tal modo, vengono reperiti dati importanti, fra i quali user e password, numeri di carte di credito, ecc..

E' da notare che specialmente l'ultima tecnica sopra citata può colpire gli utenti interni alla nostra Azienda, con possibili gravi conseguenze. Infatti, quanti utenti abbiamo in Internet ogni giorno? Quanti siti riusciamo a bloccare?

Qualche altra considerazione.

Se fino ad oggi le email erano in inglese, e ciò lasciava relativamente tranquilli i Paesi non di lingua inglese, ora le email sono tradotte in altre lingue, italiano incluso. Anche i virus inviano ora email in italiano.

Da pochi giorni, infine, si ha un virus che sfrutta la vulnerabilità LSASS ed "inietta" un trojan sui pc infettati. Cosa fare?

Diamo per scontato che siano state adottate tutte le opportune misure per proteggersi dai virus e da attacchi diretti ad alcune "porte". Ciò anche se stiamo assistendo, purtroppo, ad una riduzione drastica dei tempi fra rivelazione di un nuovo "bug" e diffusione di un virus che lo sfrutta.

Su quest'ultimo aspetto, andrebbe aperto un dibattito, in quanto l'unico rimedio al momento noto, è quello di diffondere rapidamente una nuova patch, non appena questa si renda disponibile.

Tutto ciò, rendendo impossibile l'esecuzione di adeguati test dei pacchetti software da distribuire, può comportare malfunzionamenti dei sistemi a livello locale, ossia in filiale e negli uffici di Direzione.

Si profila quindi, a nostro avviso, l'esigenza di:

- ridurre il numero di pacchetti software presenti sui server e client;

- rafforzare il controllo sulla gestione delle password di amministratore, introducendo, possibilmente, un ulteriore strumento di autenticazione per queste figure che sono, chiaramente, quelle in grado di installare software e creare cartelle sui computer (ci riferiamo, ad esempio, all'introduzione nell'uso dei "token");

- esercitare un più stretto controllo sugli addetti alle installazioni di hardware e software (quante volte sono stati loro la fonte di guai?);

- fare estrema attenzione a quanto viene attuato in momenti in cui i controlli si attenuano o vengono eliminati; ci riferiamo, ad esempio, a quelle occasioni nelle quali tutti gli addetti interessati devono intervenire con urgenza per ripristinare una situazione di disservizio; in questi casi, il manuale di ripristino non basta, ma serve una adeguata sorveglianza;

- attuare uno stretto controllo sui software che vengono installati e, ancora meglio, adottare una politica severa nei confronti delle unità organizzative che installano software senza autorizzazione da parte della Funzione Aziendale competente.

Per quanto riguarda l'ultimo punto, ci risulta che alcune banche negli USA hanno adottato questa tecnica: hanno assegnato un codice di priorità ad ogni utente dell'Help Desk e a tutti gli utenti che hanno un software non autorizzato sul computer viene assegnata la priorità più bassa. Sembra che questa iniziativa funzioni!

Se ci riferiamo agli attacchi ai nostri clienti, interni ed esterni, tesi alla cattura di informazioni relative al loro accesso in rete (e non solo), possiamo al momento ipotizzare le seguenti azioni:

- insistere perché le Associazioni consumatori sensibilizzino gli utenti di computer, che accedono in rete, ad avere maggiori accortezze e a dotarsi di contromisure minime, quali i software antivirus e personal firewall; (in questa direzione si inserisce la nostra iniziativa con Adiconsum);

- investire ulteriormente nella sensibilizzazione di tutto il personale ai pericoli che oramai possono presentarsi, coinvolgendoli nella comprensione delle possibili contromisure, affinché le facciano proprie;

- tra le tecniche di sensibilizzazione alla sicurezza, usare la Intranet, il giornale aziendale, ed ogni altra occasione per raccontare alcuni episodi tratti dai giornali specializzati (ci risulta che il primo ad accorgersi di un attacco di phishing ad un grande gruppo spagnolo fu proprio un dipendente: ciò conferma l'importanza del coinvolgimento di tutti);

- incrementare la sicurezza dei sistemi di home banking, adottando certificati digitali o "token";

- dato che oramai sempre più frequentemente vengono realizzati siti uguali in tutto per tutto a quelli delle banche, eseguire periodiche scansioni delle pagine web contenenti parole chiave uguali a quelle dei propri siti di home banking.

Per maggiori dettagli:

http://www.kommersant.com/page.asp?id=475549
http://www.finextra.com/fullstory.asp?id=11879
http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,93247,00.html
http://news.bbc.co.uk/2/hi/technology/3633167.stm
http://www.theregister.co.uk/2004/04/20/babel_fish_worm/
http://sify.com/news_info/fullstory.php?id=13442609
http://news.netcraft.com/archives/2004/06/02/phishing_worm_installs_trojan_without_trickery.html
***Fonte**: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Informatica*

5. COMPUTER CRIME: Case studies

Proseguiamo l'analisi di alcune casistiche di frodi perpetrate via computer.

Questa volta alleghiamo alcuni casi avvenuti negli States e i cui autori sono stati oggetto di incriminazione negli ultimi sei mesi.

Come si può notare, una delle tecniche più usate appare quella dei programmi chiamati "trojan", capaci di lavorare sul computer di terzi in modo da fornire informazioni preziose al criminale.

Se,da una parte, una attenta riflessione riguardo a chi è stato colpito ed agli autori (teniamo conto che siamo negli USA, dove esistono da tempo leggi assai severe, una forte sensibilizzazione ed organismi pubblici molto attrezzati nella individuazione e repressione di queste tipologie di reati) non può non preoccuparci per cosa attenderci anche in Italia nel prossimo futuro, dall'altra non possiamo non sottolineare un nuovo caso di spionaggio industriale ed un caso (il n.7) in cui l'autore del crimine ha sfruttato le conoscenze acquisite dall'essere l'amministratore dei server di un'azienda collegata per ragioni di business.

A questo proposito domandiamoci: quanti di noi hanno aziende collegate via rete per varie ragioni? Per manutenzione? Per sviluppo software?

Quante informazioni riesce ad ottenere il CIO di un'azienda o l'amministratore dei server?

Nel caso n.7, tra l'altro, il Tribunale competente segnala che il danno è stato stimato in 5,8 milioni di dollari!

Il vecchio adagio recita: "fidarsi è bene, ma non fidarsi…".

1- maggio 2004

Tale Sabathia, approfittando della sua mansione di addetta alla fatturazione passiva, ha emesso oltre 100 assegni circolari, per un totale di 875.000 US$, intestandoli a se stessa e ad altri amici.

Aveva celato l'operazione dietro falsi pagamenti, a fornitori, alterando il registro degli assegni emessi.

2- maggio 2004

Mr. Dinh è stato condannato a tre anni di prigione per aver eseguito operazioni di trading in nome e per conto di un ignaro cittadino; l'hacker era riuscito ad accedere al computer malgrado fosse protetto. Dopo aver catturato informazioni vitali, ha eseguito una serie di operazioni di acquisto di "opzioni put" onde ottenerne un beneficio per se stesso.

La tecnica usata è consistita nell'attirare l'ignaro ad un sito da lui costruito e quindi ad infettare il computer con un programma trojan. La scusa era consistita nel chiedere agli investitori di alcune banche il parere su un nuovo sistema di trading on line.

3- febbraio 2004

Andrew, già amministratore di server presso una nota Corporation, due settimane dopo essere stato dimesso, si è connesso alla rete aziendale ed ha cancellato diversi file critici. Del caso si è occupata l'FBI.

Non è stata rivelata la stima della perdita subita dall'azienda.

4- febbraio 2004

Emmet e Demarcus, due giovani impiegati, di due diverse società (impresa assicuratrice una, e nota costruttrice di hardware, l'altra), sono comparsi davanti al giudice per aver acceduto, tramite il computer aziendale, all'archivio delle carte di credito di una nota Società. Sono ritenuti colpevoli di avere anche aperto delle linee di credito con le informazioni rubate.

Le aziende datrici di lavoro hanno ampiamente collaborato con la Electronic Crime Task Force dei servizi segreti americani.

5- febbraio 2004.

Il CEO di una azienda americana e due suoi collaboratori sono stati incriminati per aver acceduto al sistema informatico di una azienda concorrente per catturare informazioni relative alle condizioni praticate.

Per far ciò, i tre sono riusciti a carpire i codici di accesso e le password di alcuni dipendenti dell'azienda concorrente.

Non è stata rivelata la stima della perdita subita dall'azienda.

Le indagini sono state portate avanti dall'FBI.

6- gennaio 2004.

Jerome, 24 anni, è stato riconosciuto colpevole di aver catturato i codici di accesso degli utenti di eBay e Qualcomm e di avere interrotto l'operatività di tali aziende.

Il giovane ha usato programmi trojan per entrare nei sistemi delle citate società.

Non sono state fornite indicazioni relativamente alla perdita economica subita.

Le indagini sono state condotte dall'FBI.

7- dicembre 2003.

Daniel, di anni 25, è stato incriminato per essere riuscito a catturare informazioni relative alle carte di credito di clienti di una azienda che gestisce informazioni per conto di Società emittenti carte di credito, banche, aziende industriali, ecc.

Ha potuto far ciò approfittando del collegamento telematico esistente fra la società colpita e quella per la quale lavorava in qualità di amministratore di server.

Il danno subito dall'azienda colpita è stato stimato in 5,8 milioni di dollari.

L'indagine è stata condotta da apposite squadre dei servizi segreti e dell'FBI.

***Fonte**: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Informatica*

6. L'IGNORANZA INFORMATICA: IL COSTO NELLA SANITA

Lo scorso 18 giugno AICA e SDA Bocconi hanno presentato il rapporto "L'ignoranza informatica: il costo nella Sanità", con l'obiettivo di valutare , il più possibile in termini quantitativi, il costo che il "non sapere" informatico comporta per la collettività. Lo scorso anno la ricerca si era rivolta al mondo del lavoro in generale, e aveva messo in evidenza come lo scotto pagato dall'economia nazionale per tale ignoranza risultasse dell'ordine dei 15 miliardi di euro annui. In questa seconda indagine ci si è focalizzati su un'area di grande rilevanza sociale, la Sanità.

La ricerca risponde a tre interrogativi:

1. Quale è il ruolo dell'informatica nella Sanità in Italia?

2. Quale è il costo dell'ignoranza informatica?

3. Quali sono i benefici della formazione informatica?

In talia la spesa per le prestazioni sanitarie nel 2001 è stata dell'ordine di 100 miliardi di euro. Tre quarti di tale importo è stato sostenuto dallo Stato ed il rimanente 25% è stato pagato dai privati. In termini macroeconomici il settore dei servizi sanitari in Italia dà lavoro a circa 1.280.000 persone, ovvero impiega il 4,6% della forza lavoro diaponibile nel nostro paese, mentre le sue attività economiche rappresentano l'8% del PIL italiano.

La spesa informatica nel settore della sanità italiana ammonta ad oltre 600 milioni di euro l'anno. Tale importo lappresenta lo 0,59% della spesa sanitaria.

Il livello di informatizzazione di questo settore è enormemente lontano rispetto a quello della finanza o dell'industria, an che se è evidente il vantaggio che una maggiore informatizzazione potrebbe determinare sia per i processi amministrativi che per quelli clinici. Nei paesi europei più forti l'inc idenza della spesa informatica rispetto alla spesa sanitaria ammonterebbe al 2%.

La formazione informatica è un tema chiave del rapporto curato da AICA e SDA Bocconi. Di conseguenza lo è anche quello dell'alfabetizzazione informatica. Solo nell'ultimo anno è aumentato di circa il 70% il numero di coloro che in Italia hanno investito in percorsi formativi e programmi di certificazione delle competenze, anche se poi si vede che è quasi sempre il singolo a farsi carico dell'impegno economico e di tempo necessario per acquisire le competenze (74% dei casi).

Anche in ambito pubblico si è ancora lontani dal considerare l'alfabetizzazione informatica strumento di efficienza ed una conferma viene dal rapporto sul settore della sanità.

Dalla ricerca risulta che nella Aziende Sanitarie Locali e Ospedaliere la percentuale degli addetti che si avvalgono per il loro lavoro dell'informatica, tipicamente PC e Internet, varia

dal 49 al 35%, secondo la dimensione dell'azienda. In tali strutture si è stimato che attualmente quasi 340.000 persone usano l'informatica per necessità di lavoro, ma circa 200.000 di queste non hanno una solida preparazione al riguardo e necessitano di interventi formativi IT.

La ricerca ha inoltre verificato che l'utenza informatica attuale è costituita in gran parte da personale amministrativo.

Per qunto riguarda invece i medici di medicina generale (medici di base) un'indagine campione ha mostrato che il 76% usa strumenti informatici ed un altro 7% intende farlo quanto prima. È comunque da sottolineare che circa l'80% dei medici di base ha dichiarato di non essere stato "alfabetizzato"all'uso di strumenti informatici, non ha cioè acquisito quelle competenze di base richieste ad un utente non specialista.

Gli intervistati, sia medici di base che personale medico ospedaliero ha affermato di perdere tempo, nella propria attività, per superare difficoltà nell'uso dell'informatica. Dai dati raccolti si è giunti alla conclusione che il costo della improduttività (tempo perso) ammomta per l'intero sistema sanitario (pubblico e privato) a oltre 850 milioni di euro l'anno. Tale importo rappresenta largamente il totale della spesa informatica dell'intero settore sanitario e potrebbe facilmente aumentare per effetto di una diffusione di tecnologie digitali a tassi superiori di quelli dell'alfabetizzazione, andando ad impattare anche sull'esito del programma "Sanità elettronica". In pratica, il "non sapere"informatico potrebbe pregiudicare il passo di progetti innovativi, che vedono un'evoluzione del rapporto cittadino/struttura sanitaria.

Dopo aver esaminato alcune esperienze effettuate in altri paesi, la ricerca mostra che adeguati percorsi formativi potrebbero portare ad un incremento di produttività complessivo pari al 2,7% della spesa informatica sanitaria italiana.

Un test effettuato presso l'Ospedale di Legnano ha portato a stimare che l'effetto di una formazione informatica porterebbe ad un incremento di produttività, per l'intero settore sanitario italiano, del valore di 1,905 miliardi di euro, oltre ad una riduzione di costi compreso tra i 675 euro l'anno pro-capite per il personale medico e 218 per il personale tecnico. In totale il ritorno annuale della formazione informatica nel settore sanitario sarebbe di 2,156 miliardi di euro l'anno.

***Fonte**: il presente articolo è stato ripreso dagli atti del convegno tenutosi il 18 giugno 2004, presso l'Università L. Bocconi di Milano.*

7. MASTER

CEFRIEL e MIP Politecnico di Milano, rispettivamente centro di eccellenza ICT e business school del Politecnico di Milano, lanciano la 3a edizione del Corso di Alta Formazione in Information Security Management: ISM. Il corso, della durata di 200 ore, ha una formula part-time, con frequenza venerdì e sabato, ogni 15 gg.. L'inizio è previsto per Settembre 2004, con due edizioni che si svolgeranno parallelamente a Milano e Roma. I destinatari sono responsabili di sistemi informativi e di reti, specialisti e consulenti nel campo della gestione in outsourcing di reti e sistemi informativi.

Per ulteriori informazioni: www.securman.it

Il Dipartimento di Informatica dell'Università di Roma "La Sapienza" ha istituito il Master di I livello in "Sicurezza dei Sistemi e delle Reti informatiche per l'impresa e la Pubblica Amministrazione" (scadenza presentazione domande: 15 settembre 2004). Il corso è rivolto soprattutto a coloro che già operano nel settore informatico, presso aziende private o la Pubblica Amministrazione ed intendono completare e potenziare la loro formazione, senza interrompere la propria attività lavorativa e si svolge prevalentemente nei giorni di venerdì e sabato. Il Master è aperto, previa selezione, a tutti i possessori di una Laurea (almeno di primo livello) in Informatica, Fisica, Ingegneria, Matematica, Statistica, nonché i possessori di una Laurea in altre discipline, che abbiano una comprovata esperienza lavorativa pluriennale nel campo dell'informatica. Per ulteriori informazioni: www.clusit.it/vetrina_soci/uniroma.pdf e http://security.di.uniroma1.it/master/

Si sta per concludere la parte di teoria del "Master in Telecomunicazioni, VII ed." organizzato da IFOA. Obiettivo del corso è stato quello di formare esperti che si occupino della progettazione, amministrazione e gestione di reti fisse, reti wireless e sistemi radiomobili, con competenze sia di IT che di Network Security. Gli allievi del Master saranno disponibili per tirocini formativi (completamente gratuiti per l'azienda), della durata di 12 settimane, nelle aziende del settore ICT , a partire dalla fine di Luglio o da Settembre. Le aziende interessate possono contattare Micaela Pecorari al n° 0522 329340 o via mail ict2@ifoa.it

8. ULTIME NOTIZIE

28.06.04

Malicious code sono stati rilevati in questi giorni sulle home page di importanti siti web. Si tratta di motori di ricerca, di istituzioni finanziarie, di aste on line e di siti che fanno comparazione di prezzi. Tramite questi siti viene propagato del codice Javascript, che infetta le macchine che impiegano Internet Explorer. I malcapitati navigatori, senza volerlo, scaricano il codice maligno, che è collegato a un'immagine o a un grafico. Una volta lanciato il codice maligno, il trojan collega le macchine infettate ad uno o più IP, localizzati nel Nord America o in Russia, con uno sniffer intercetta le battute sulla tastiera e da ultimo apre una porta che può utilizzare per prendere il controllo della macchina o inviare dello spam.

25.06.04

RSA Security ha presentato il suo studio annuale sulla sicurezza delle reti Wi-Fi. Lo studio, inizialmente focalizzato su Londra, è stato esteso a Parigi, Francoforte e Milano. Lo studio mostra che le reti di Milano sono le meno sicure d'Europa.

leggi la notizia su
http://key4biz.metsviluppo.it/index.jsp?notizia=144677&urlChiamata=visNotizia.jsp

9. EVENTI SICUREZZA (Tutti i dettagli sulle manifestazioni sono disponibili sul sito CLUSIT alla voce EVENTI)

6-9 luglio 2004, Torino
Corso per la certificazione professionale OPSA

10 luglio 2004, Roma
Esame di certificazione CISSP

13 luglio 2004, Roma
SEMINARIO CLUSIT - "Principi di crittografia"

27-30 luglio 2004, Torino
Corso per la certificazione professionale OPST

21 settembre 2004, Milano
SEMINARIO CLUSIT - "Voice-over-IP"

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