Indice

1. NUOVI SOCI

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

- Adobe Systems Italia (Agrate Brianza - MI),
- CAP System (Roma),
- Bitdefender.it (Genova),
- Interactive Net Business (Verona),
- Tecno Logic (Crema),
- Webegg (Milano),
- Work Plus (Scurelle - TN).

2. IL VALORE DELLA SICUREZZA DELLE INFORMAZIONI

Coloro che si occupano di sicurezza informatica all'interno delle aziende devono sempre più dimostrare quale sia il ritorno degli investimenti (ROI: Return On Investment) dei loro progetti, specialmente nella difficile situazione economica degli ultimi 18 mesi.

Purtroppo, la natura stessa delle attività di sicurezza informatica rende estremamente difficile qualunque proiezione finanziaria. Le aziende considerano il ROI come un indicatore finanziario (cioè come un ritorno finanziario quantificabile, ad una scadenza prevista, o come un'economia in termine di costi). La difficoltà, per la maggior perte degli investimenti in sicurezza, è che i ritorni finanziari (parte importante del ROI) sono molto difficili ed alle volte impossibili da prevedere.

Da un recente studio, realizzato da META Group risulta che, per un terzo dei responsabili della sicurezza in Germania, le perdite conseguenti ad incidenti informatici occorsi negli ultimi 24 mesi, sono rilevanti.

Anche se gli investimenti in sicurezza hanno effettivamente delle conseguenze finanziarie importanti, è molto difficile quantificarne i benefici in anticipo. Si possono utilizzare delle statistiche globali (ad esempio il costo medio degli attacchi) per fare una stima dei rischi di perdite potenziali, ma la natura estremamente diversificata delle singole situazioni aziendali, abbinata alla specificità di ogni attacco, portato in un determinato momento, rendono qualunque previsione estrememente approssimativa.

Giusticare gli investimenti in sicurezza tramite calcoli di ROI basati su ipotesi non sufficientemente realistiche, porta spesso a decisioni negative, relativamente alle domande di budget.

Per approfondire questa problematica, Bull ha sponsorizzato uno studio, realizzato da META Group.

Sono state realizzate interviste con i responsabili della sicurezza (Chief Information Security Officers) di grandi aziende (tra 9.500 e 70.000 dipendenti) in Germania, Francia, Italia, Spagna, Inghilterra e nei paesi scandinavi, in particolare nei settori: industria, finanza, telecomunicazioni e pubblica amministrazione. Ciò ha permesso di meglio comprendere il metodo utilizzato dalle grandi imprese europee per stabilire un rapporto tra il valore delle informazioni e la sicurezza IT.

Lo studio, dalla cui introduzione sono state prese e liberamente tradotte le considerazioni sopra riportate, è disponibile (previa registrazione) su
www.evidian.com/iwatch/surveys/meta2003.php (in inglese) o su
www.evidian.com/iwatch/surveys_fr/meta2003.php (in francese).

3. INSEDIAMENTO DEL COMITATO Internet@Minori

Il 10 marzo, alla presenza del Ministro delle Comunicazioni On. Maurizio Gasparri, si è insediato il Comitato Internet@Minori. Del Comitato, presieduto dal Prof. Danilo Bruschi, Presidente del CLUSIT, fanno parte i rappresentanti delle quattro associazioni firmatarie del Codice di autoregolamentazione (Federcomin, Aiip, Anfov e Assoprovider), delle Associazioni per la tutela dei Minori, del Consiglio Nazionale degli Utenti nonché del Ministero delle Comunicazioni e del Dipartimento per l'Innovazione e le Tecnologie.

4. LA CONVENZIONE SUL CYBER CRIME ENTRER IN VIGORE IL 1 LUGLIO 2004

La Convenzione sul cyber crime entrerà in vigore il 1° luglio 2004. Si tratta del primo trattato internazionale sulle infrazioni penali commesse attraverso internet o altre reti informatiche. Il trattato, adottato dal Consiglio Europeo nel novembre 2001, è il risultato di quattro anni di lavori, che hanno coinvolto 43 Paesi. Per l'entrata in vigore definitiva era necessaria la ratifica di almeno cinque Stati membri. Gli Stati che per primi hanno provveduto alla ratifica, e grazie ai quali è dunque possibile l'entrata in vigore della Convenzione, sono.....: la Croazia, l'Albania, l'Estonia, l'Ungheria e la Lituania...(!!!).

Il testo della Convenzione è disponibile su:

http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (in inglese)

http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm (in francese)

5. CYBER CRIME, VIRUS E TERRORISMO

Il "Computer Crime Research Center" sovietico, in un articolo firmato dal sig. Dmitri Kramarenko, riporta la notizia di un allarme, proveniente dall'america, di un presunto prossimo attacco su Internet ad opera di terroristi islamici. Asseriscono che i servizi europei sono stati avvertiti perché "...consequences of this attack can be compared with September 11 disaster. Terrorist aim at computer systems of large economical and financial centers of the West.".

Un altro membro del Centro di Ricerca, sig. Andrey Belousov, afferma che la brigata "Abu Nafsa", facente parte della rete di Al Qaeda, ha già colpito via Internet e si sta preparando a colpire gli USA.

Non sappiamo quanto ciò possa essere vero, però, dobbiamo ammetterlo, negli ultimi mesi si sta assistendo ad una sequenza di virus il cui scopo principale è la raccolta di informazioni dai computer (user, password, antivirus, ecc.) e la installazione di software affinché terzi possano prendere il possesso dei pc stessi. Seguono poi, a completare il quadro, virus del tipo "mass-mailing"; già abbiamo subito quelli che cancellano i file... In particolare, come segnalato da Symantec, la maggior parte degli attacchi da virus, cresciuti nel 2003 del 148%, hanno riguardato in prevalenza il settore finanziario.

I russi asseriscono che si stanno predisponendo nuove tipologie di virus, molto più disastrose. Onestamente non abbiamo al momento idea di come potrebbero essere i nuovi attacchi.

In base alle nostre conoscenza attuali, potremmo dire che al momento i virus sfruttano:

- i "bug" dei sistemi operativi,
- il mancato aggiornamento antivirus di tutti i server e posti di lavoro,
- l'ingenuità o superficialità degli utenti.

Da una nostra indagine presso alcuni gruppi tecnici che partecipano a "chat" ed a raduni con hacker di varie nazioni, alla nostra domanda "sono avvenute o stanno avvenendo delle modifiche strutturali rilevanti ai virus tali da far ritenere che l'affermazione russa abbia un possibile fondamento di verità", ci è stato risposto che:

1. l'utente del computer è talmente "sciocco" che non occorrono programmi sofisticati per convincerlo a scaricare sul computer una e-mail infetta;
2. i nuovi worm sono stati ingegnerizzati e sono divenuti più "leggeri"; infatti occupano mediamente un quinto dei byte che richiedevano fino a poco tempo fa;
3. i worm più recenti riescono a bloccare i servizi dell'antivirus e del personal firewall.

L'ultima informazione credo ci preoccupi non poco. Da questo punto di vista i computer portatili, anche se provvisti di antivirus e personal firewall possono essere un pericolo d'infezione più grave di quanto si potesse ritenere fino a poco tempo addietro.

Siccome bisogna ragionare sempre su cosa si deve fare, le principali linee di difesa ci appaiono al momento ancora quelle seguite fino ad oggi:

- esecuzione di programmi che controllino tutte le LAN e verifichino che i computer in rete siano dotati di antivirus: ciò attraverso una ricerca su tutto il "range" di indirizzi;
- Uitilizzo di sonde sulla rete per l'intercettazione di programmi non standard o "UFO".
- esecuzione di programmi che verifichino, almeno a livello giornaliero, che tutti i posti di lavoro in rete abbiano l'antivirus aggiornato; e che riverifichino le impostazioni degli antivirus.
- rendere disponibili, in una apposita cartella sul server locale, accedibile da un incaricato, il programma di "pulizia" di virus messo a disposizione dal proprio fornitore;
- provvedere alla distribuzione sui server e client delle patch al software di base; tale distribuzione deve essere eseguita con una priorità basata sulla gravità della segnalazione pervenuta dal fornitore (es: Microsoft Security Bulletin);
- divieto "fisico" di colloquio in LAN dei personal computer portatili privi di antivirus;
- normativa che proibisca l'accesso a "provider" di servizi di email utilizzando il computer dell'azienda (portatile o desktop);
- responsabilizzazione delle Società fornitrici, ai fini dei problemi di virus, nei confronti dei propri dipendenti che accedano alla rete LAN aziendale mediante computer portatili, inserendo, inoltre, clausole contrattuali di reindennizzo di danni provocati da eventuali virus introdotti da loro personale;
- monitoraggio costante delle segnalazioni di infezione onde comprendere nel più breve tempo possibile la fonte dell'infezione, natura, ecc.;
- sensibilizzazione del personale dell'azienda al problema dei virus, ad esempio attraverso notizie sulla Intranet aziendale e/o messaggi di avviso, onde tenere desta l'attenzione.

(Autore: Ing. Anthony Cecil Wright, socio CLUSIT e Presidente ANSSAIF [Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria])

6. NOTIZIE DA FEDERCOMIN

CONCLUSIONI DEL CONSIGLIO UE SULLO SVILUPPO DELLA SOCIETÀ DELL'INFORMAZIONE

Riunito sotto la presidenza di Dermot Ahern, il Consiglio trasporti e telecomunicazioni ha adottato, l'8 marzo, un insieme di conclusioni sullo sviluppo della Società dell'Informazione in un'Europa allargata. Dopo la valutazione dell'attuazione del programma eEurope 2005 e della situazione delle comunicazioni elettroniche in Europa, i ministri hanno esaminato le misure complementari auspicate dalla Commissione europea per lottare contro la proliferazione dello "spam". I ministri hanno inoltre avallato l'analisi della Commissione sul follow-up del Vertice mondiale sulla Società dell'informazione (WSIS).

DIRETTIVA CONTRO CONTRAFFAZIONE E PIRATERIA

Il Parlamento di Strasburgo ha approvato il 9 marzo in prima lettura la relazione di Janelly Fourtou (UDF) sul "rispetto dei diritti di proprietà intellettuale".

Presentata nel gennaio 2003 dalla Commissione, la proposta di direttiva completa la legislazione comunitaria sulla proprietà intellettuale, fissando norme comuni per sanzionare le frodi e le contraffazioni che si ispirano alle "migliori prassi " nazionali.

Riguardo al campo di applicazione, la proposta di direttiva prevede misure che devono essere applicate unicamente agli atti commessi su scala commerciale, fermo restando per gli Stati membri di applicarle nei confronti di altri atti, compresi quelli configurabili come concorrenza sleale o attività simili. La direttiva prevede altresì che le autorità possano procedere a sequestri cautelativi dei beni mobili ed immobili delle persone incriminate in casi di frode. Gli aventi diritto potranno così chiedere indennizzi per i mancati guadagni. La direttiva si applicherà a qualsiasi forma di contraffazione o pirateria: dei giocattoli, dei prodotti di lusso, delle medicine o, elemento controverso, questo, di musica, film ecc. Su indicazione del Consiglio, le sanzioni penali sono state eliminate. Il testo di compromesso si limita a stabilire che gli Stati membri dovranno fare il necessario al di fuori del diritto civile per perseguire gli autori delle frodi. Spetterà ai giudici applicare caso per caso sanzioni "proporzionate" all'infrazione.

"SAFER INTERNET PLUS"2005-2008

La Commissione europea ha presentato "Safer Internet Plus" 2005-2008, un nuovo programma per rendere Internet più sicuro per i minori. Il programma, che ha una dotazione di 50 milioni di euro, si propone di mettere a profitto tutto il lavoro effettuato nell'UE dal 1996 contro i contenuti illegali e dannosi su Internet. Gli orientamenti principali del programma sono: la lotta contro i contenuti illegali, il trattamento dei contenuti non richiesti e dannosi, la promozione di un ambiente più sicuro, la sensibilizzazione per un'informazione sistematica sulla sicurezza di Internet.

Il testo della proposta si trova al sito:
http://europa.eu.int/information_society/programmes/iap/index_en.htm

DECRETO LEGGE ANTIPIRATERIA

E' stato pubblicato sulla Gazzetta Ufficiale n. 69 del 23 marzo il decreto legge 22 marzo 2004, n. 72, recante "Interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo", il quale dispone nuove misure sanzionatorie per la tutela del diritto d'autore. La normativa prevede l'individuazione di fattispecie tipiche che consentono di colpire i comportamenti di coloro che scambiano file coperti dal diritto d'autore. In aggiunta alla sanzione penale per lo scambio su Internet di file protetti dal copyright fatto per fini commerciali, disposta dalla legge n. 633 del 1941, il decreto legge introduce una sanzione amministrativa pecuniaria (di euro 1.500) per lo scambio fatto per uso personale tramite i cosiddetti programmi di file sharing. E' previsto che il Dipartimento della pubblica sicurezza del Ministero dell'interno raccolga le segnalazioni di interesse per la prevenzione e la repressione delle violazioni. Il decreto legge impone precisi obblighi ai service provider, verso i quali sono previsti, in caso di violazione di tali adempimenti, sanzioni amministrative pecuniarie assai pesanti (da 50.000 a 250.000 euro). Il decreto legge non sembra rispecchiare quanto previsto dalla proposta di direttiva del Parlamento europeo e del Consiglio relativa alle misure e alle procedure volte ad assicurare il rispetto dei diritti di proprietà intellettuale, approvata lo scorso 9 marzo dal Parlamento europeo, che invece prevede sanzioni amministrative solo per gli atti commessi su scala commerciale.

Il disegno di legge di conversione del decreto legge è stato presentato alla Camera dei deputati (A.C. n.4833) ed è stato assegnato il 23 marzo in sede referente alla VII Commissione permanente (Cultura).

(Fonte: FEDERCOMIN MAIL n. 21)

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

7 aprile 2004, Lugano
Seminario CLUSIS/CLUSIT al Lugano Communication Forum

5-9 aprile 2004, Milano 3
Seminario di preparazione all'esame CISSP

6 maggio 2004, Padova - Webbit
"Sicurezza ed etica nella tutela dei dati personali". SEMINARIO CLUSIT

8 maggio 2004, Monza (MI)
Esame di certificazione CISSP

12-14 maggio 2004, Roma
Internet/Intranet: TCP/IP Network Security

21 maggio 2004, Lecce
Il rischio "accettato"

4 giugno 2004, Politecnico di Milano

"Tutelare l'azienda gestendo efficacemente la sicurezza informatica: dalle implicazioni tecniche alle responsabilità legali"

2° Seminario sulla sicurezza informatica, organizzato dall'Ordine degli Ingegneri della Provincia di Milano e da CLUSIT, in collaborazione con CEFRIEL, Cisco Systems e Politecnico di Milano.

23 giugno 2004, Milano

Web Security, 4ª edizione

Per cancellarsi dalla mailing-list inviare una e-mail a info@clusit.it
specificando nel Subject: REMOVE con l'indirizzo e-mail da eliminare

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