Indice

1. NUOVI SOCI

Recentemente hanno aderito al CLUSIT le seguenti organizzazioni:

- ALASCOM Services (Milano),
- ALISAT (Raffadali - AG),
- CETIF-Centro di Tecnologie Informatiche e Finanziarie (Milano),
- CREDIT SUISSE (Milano),
- EPICURO Servizi (Roma),
- ERNST & YOUNG Financial-Business Advisors (Milano),
- Fondazione Ugo Bordoni (Roma)
- LAMPERTZ Italia (Monza),
- LISCOM (Busto Arsizio),
- LUCENT Technologies Italia (Roma),
- ORCOM (Petralia Soprana - PA),
- P.D.C.A. (Roma),
- SIES (Carbonera - TV),
- Università di Parma - Centro di Calcolo Elettronico (Parma).

2. INFOSECURITY ITALIA 2005: DATI FINALI

Sono stati 5.000 i visitatori di Infosecurity Italia 2005, la principale manifestazione fieristica del settore, che si è svolta dal 9 all'11 febbraio alla Fiera di Milano. I dati dettagliati sono disponibili su:

www.infosecurity.it/upload/I%20dati%20finali%20di%20Infosecurity,%20Storage%20Expo%20Italia%20e%20Documation%202005.pdf

Clusit, partner scientifico di Infosecurity, ringrazia tutti coloro che hanno collaborato al buon esito della manifestazione: visitatori, relatori, espositori e organizzatori. Invitiamo già da ora tutti i partecipanti a inviarci commenti, suggerimenti, e critiche, in particolare sulla parte convegnistica, onde poter preparare al meglio la prossima edizione, che si svolgerà dal 22 al 24 febbraio 2006, nel padiglione 17 di Fiera Milano.

3. COMPUTER CRIME

CYBER CRIME. FINANCIAL CRIME SECTOR REPORT

La Financial Services Authority ha pubblicato una sua indagine sullo stato dei rischi nel campo dell' Information Security (IS), per quanto attiene la gestione dei dati elettronici. Sono state interpellate e visitate sia banche che assicurazioni, broker, che gestori di fondi, per un totale di 18 aziende, di cui 6 con meno di 100 addetti, 7 con meno di 10.000 addetti, e 5 con più di 10.000 addetti.

L'aumento nell'uso dell'Outsourcing e di tecniche di furto d'identità, quali il "phishing", hanno indotto la FSA a portare avanti una revisione strutturata dei rischi di Information Security (IS).

Ciò ai fini di fornire informazioni utili al management delle aziende e non, precisa l'Authority, in base alla sezione 157 del "Financial Services and markets Act".

Infatti, ribadisce la FSA, in linea con la responsabilità del senior management nella gestione ed il controllo dei rischi, i dirigenti e senior managers devono mettere in atto tutte le opportune contromisure per fronteggiare i possibili crimini. Ed essi sono responsabili di fornire una efficace direzione in azienda per promuovere una cultura anti-frode ("In line with the FSA's principle of senior management responsibility for risk management and controls, firm's directors and senior managers are responsible for countering the crimes Information Security risks can give rise to. And they are responsible for providing an effective lead within a firm to promote an anti-fraud culture.").

LE PRINCIPALI CONCLUSIONI DELL'INDAGINE

* Le aziende potrebbero essere più attiVe:

  - nella gestione dei rischi di IS piuttosto che reagire agli eventi,

  - nel proteggere meglio i beni propri e dei loro clienti nei riguardi dei rischi derivanti da attività fraudolente.

* Mentre le aziende più grandi sembra stiano facendo qualche progresso, le piccole e medie continuano a sopportare rischi seri e sostanziali (".continue to carry more serious and substantial Information Security risks").

* Molte aziende ritengono di avere adeguati investimenti, ma ancora subiscono violazioni di sicurezza. Altre hanno incrementato i loro investimenti a seguito di attacchi, perdite economiche o la scoperta di vulnerabilità.

* Le aziende devono essere a conoscenza del continuo mutare in complessità delle minacce e devono eseguire le opportune verifiche e prepararsi a fronteggiarle ("firms need to be aware of the ever-changing complexities of current Information Security threat")

* Il management delle aziende non ha sempre aggiornato le policy di IS per fronteggiare i rischi derivanti dalle nuove tecnologie, e le procedure di controllo non vengono sviluppate finché le policy non sono state aggiornate.

* L'emergere di nuove minacce è servita a ricordare al management che devono proteggere i beni loro e dei propri clienti sia da pericoli interni che esterni.

* L'educazione dei clienti è particolarmente importante nel caso di attacchi quali quelli di "phishing".

* Un ruolo importante lo ricopre l'aggiornamento tempestivo delle "patch".

* Mentre l'Outsourcing ha il vantaggio di ridurre i costi, le aziende intervistate hanno ammesso che la loro priorità è quella di avere un controllo diretto sui processi critici.

* Sono poche le aziende che hanno sistemi efficienti di alert e di intrusion detection a causa di mancanza di expertise tecnica al proprio interno.

* Mentre nuovi rischi stanno emergendo, la FSA conclude la sua indagine segnalando che le aziende sono tuttora esposte alle minacce più tradizionali, in quanto non sono ancora ampiamente adottate adeguate strutture di IS, con ciò includendo la gestione dei rischi. Le aziende non hanno sufficientemente investito nei controlli; ad esempio, ancora sussistono sistemi legacy con una struttura di controllo povera. A titolo esemplificativo, la FSA segnala:

- l'incapacità di dimostrare come i rischi vengono identificati e gestiti;

- il non corretto peso dato alla formazione del personale, non tenendo conto che lo staff è importante per il controllo e la mitigazione dei rischi di IS;
- i rischi insiti nella carente gestione degli utenti, specialmente nel garantire un' adeguata separazione dei compiti fra utenti e tecnici.

NUOVE TECNICHE DI CYBER CRIME.

A quanto ci risulta, la tecnica conosciuta come "phishing", usata dai criminali per catturare informazioni personali utili a compiere frodi, è ancora frequente, ma comincia a farsi strada l'ipotesi che abbia fatto "il suo tempo".

E' quindi lecito domandarsi, se dietro l'angolo c'è qualche nuova tecnica e se questa è in abbandono.

Il laboratorio ANSSAIF sul "phishing" ci risponde.

Domanda: Il "phishing" tende a scomparire come tecnica criminale?

Risposta: Innanzitutto nessuna tecnica criminale è mai scomparsa. Casomai si è ridotta, si è specializzata, ma è sempre valida.

Pensiamo, ad esempio, alla tecnica per la cattura del contenuto di una banda magnetica di una carta di credito. Finché questo meccanismo non sarà totalmente soppiantato dalle carte a microchip, la copia del contenuto di una carta di credito è oramai di una semplicità tale da indurre anche piccoli criminali alla duplicazione dei contenuti. Questo tipo di frode è vecchissima. Infatti, la tecnica di copiare la banda magnetica, tramite un apposito apparecchio, posto ad esempio nella manica di un cameriere, risale al team del noto boss Lucky Luciano. Ciò avveniva quindi un bel po' di anni fa!

Domanda: cosa dobbiamo aspettarci a breve come nuova tecnica criminale?

Risposta: Per rispondere adeguatamente dobbiamo fare una premessa.

La cattura dei dati personali, eseguita ai fini di operare per nome e per conto di un ignaro consumatore, è uno dei principali fini delle bande criminali. Il furto di identità è sempre più frequente, più drammatico, sotto certi aspetti, per le possibili implicazioni per chi ne è vittima (ad esempio: chiusura di affidamenti; denunce; processi penali; ecc.); l'accesso virtuale alle risorse economiche lo rende ancora più "appetibile".

Come sappiamo, il furto d'identità, nella sua modalità più classica, si può svolgere in vario modo. Dalla raccolta di dati personali, leggendo la posta ed i documenti gettati nella spazzatura, al furto del portafoglio, alla raccolta di dati importanti mediante contatti con familiari, o con lo stesso soggetto, spacciandosi per un funzionario di un'azienda finanziaria o della Pubblica Amministrazione (esempio: impiegato del Comune, INPS, ecc.). I recenti continui "buchi" di sicurezza dei prodotti software, non eliminabili in toto per gli eventuali costi proibitivi per il fornitore, danno la possibilità di eseguire fondamentalmente due tipologie di operazioni:

1- installare un piccolo programma, di poche istruzioni, che cattura quanto il possessore del computer digita sulla tastiera e lo invia al criminale;

2- dirottare l'utente su un sito appositamente creato per catturargli informazioni personali, ovvero, per installargli il programma "trojan" menzionato al punto 1.

La seconda tipologia è quella che prevediamo in aumento. La potremmo chiamare "shifting", oppure, in italiano, "dirottamento". Ciò quindi deve indurre i "navigatori" su Internet a fare grande attenzione quando accedono ai siti (bisogna essere fortemente sospettosi).

Ma ciò non basta. Tutti devono sapere che, se non sono installati sul computer opportuni software di alerting e difesa, non è difficile catturare informazioni dal disco fisso (nome, indirizzo, ecc.). Vi sono aziende che, pur avendo installato un antivirus su tutti i computer, non hanno attivato la funzione di personal firewall, disponibile con lo stesso prodotto. Probabilmente per ragioni di costo. Domanda: sono stati valutati i rischi? E' stata fatta un'analisi costi/benefici? Se viene catturata la password di un amministratore di sicurezza, che danno l'azienda può subire?

I dati in nostro possesso parlano di milioni di euro.

DIGITAL RIGHT MANAGEMENT E SPYWARE

Fra le più recenti tecniche di "phishing" o, se vogliamo, di "shifting", segnaliamo quella utilizzata da alcuni hackers che mettono a disposizione dei video (probabilmente a contenuto.diciamo.interessante.), la cui visione può essere assicurata se viene scaricata la relativa licenza.

La licenza viene letta dall'utente e, contemporaneamente, vengono scaricati sul computer tutta una serie di programmini atti a spiare quanto eseguito dall'utente e utili a dirottare l'utente su siti appositamente creati dal criminale per catturare informazioni. Chiaramente il personal firewall, qualora installato, è stato disattivato dall'utente, in quanto il file video altrimenti non sarebbe stato possibile scaricarlo.

Il laboratorio di Phishing ci ricorda che, molte volte, è prassi dare invio senza leggere il messaggio che ci appare: ciò è estremamennte pericoloso, perchè, così facendo, si autorizza un terzo ad operare sul nostro computer!

(Fonte: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria. www.anssaif.it)

4. POSTA CERTIFICATA

CdM: via libera definitivo alla "posta elettronica certificata"

L'Italia è tra i primi Paesi al mondo a disporre della posta elettronica certificata. L'invio e la ricezione e-mail ha infatti completo valore legale, come una ricevuta di ricezione, proprio come avviene per la tradizionale raccomandata con avviso di ricevimento rispetto alla lettera con affrancatura ordinaria. Su proposta di Lucio Stanca, ministro per l'Innovazione e le Tecnologie, il Consiglio dei Ministri ha approvato in via definitiva il Dpr che, come ha spiegato lo stesso Ministro, "disciplina l'utilizzo della posta elettronica certificata non solo nei rapporti che cittadini ed imprese intrattengono con la Pubblica amministrazione, ma anche nelle relazioni tra uffici pubblici, come pure tra privati".

(Tratto dalla newsletter N.89 del Ministro per l'Innovazione e le Tecnologie)

Il comunicato stampa è disponibile su:

www.innovazione.gov.it/ita/comunicati/2005_01_28.shtml

5. CONSULTAZIONE UNIONE EUROPEA

L'Unione Europea ha avviato tre consultazioni on-line per le quali attende commenti da parte di tutti gli interessati su argomenti relativi a sicurezza e privacy.

Gli argomenti sono:

- Data protection issues related to intellectual property rights
- Data protection issues related to RFID technology
- Videosurveillance.

Coloro che avessero interesse a partecipare possono inviare i propri commenti per email direttamente all'Unione Europea entro il 31 MARZO 2005.

Tutte le informazioni e le modalità di partecipazione sono disponibili presso:

http://europa.eu.int/comm/internal_market/privacy/workingroup/consultations/consultation_en.htm

6. PREMIO CLUSIT PER LA MIGLIORE TESI UNIVERSITARIA IN SICUREZZA INFORMATICA

È stato istituito un premio (di 1.000 euro per il 2005), che ricompenserà ogni anno la migliore tesi universitaria in sicurezza informatica.

Le tesi saranno valutate da una giuria mista, composta da esperti del Clusit, del mondo accademico e delle aziende del settore.

L'iniziativa è legata alla creazione di un portale, all'interno del sito web dell'associazione, per la raccolta e la proposta di tesi in sicurezza informatica, e servirà di riferimento per aziende, docenti e studenti.

7. GRUPPO DI LAVORO FEDERCOMIN SU RFID

FEDERCOMIN ha lanciato un Gruppo di Lavoro sulle applicazioni della tecnologia RFID.

CLUSIT partecipa al Gruppo di Lavoro, per le problematiche relative alla sicurezza e alla Privacy.

Non mancheremo di tenere informati i nostri lettori sul seguito dell'iniziativa.

8. SEMINARI CLUSIT DI MARZO

SEMINARIO CLUSIT Sicurezza VLAN e LAN
ROMA 15 marzo 2005

Sono aperte le iscrizioni.

Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form_2004.pdf

Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

1 - Introduzione
Modello OSI
Standard Ethernet
Standard VLAN (802.1q)
ARP
2 - Principi di funzionamento degli apparati di livello 2
CAM table
Address Learning
Autoconfigurazione : DHCP
3 - Attacchi e Contromisure
CAM Table e CAM Overflow (DEMO)
ARP Poisoning, Gratuitous ARP (DEMO)
VLAN Hopping
Switch Port Stealing (DEMO)
Spanning Tree Protocol (STP)

DHCP Spoofing
4 - Conclusioni
Encryption
802.1x e Admission Control
Best Practices
Questions and Answers

Agenda:

- Registrazione: 13,50
- Inizio Seminario: 14,10
- Fine lavori: 18,10

Docenti: Marco Valleri, Marco Misitano
Luogo: Centro di formazione Percorsi Srl - Viale Manzoni 22

SEMINARIO CLUSIT RFID
MILANO 22 marzo 2005

Sono aperte le iscrizioni.
Il modulo per registrarsi: www.clusit.it/edu/reg_sem_form_2004.pdf
Per i Soci Clusit la partecipazione è gratuita*

PROGRAMMA

1 - Cosa sono, loro storia, utilizzi
Che cos'è RFID
La storia del RFID: dalla Seconda Guerra Mondiale a Walmart
I transponder sulle cose e i transponder sulla persona
Dal RFID alla Ubiquitous Society
2 - I vari tipi di transponder
Transponder passivi, semiattivi e attivi
Transponder magnetici e elettrici
Le frequenze del RFID
Convergenza tra M2M e RFID: il caso Zigbee
3 - Architetture Software e sicurezza
Il modello ISO/OSI del RFID
L'architettura degli standard ISO ed EPC: similitudini, differenze e convergenze
Riservatezza, Integrità ed autenticità
La sicurezza informatica: dall'immobiliser al Mifare ed oltre
Metodi per garantire la scelta di privacy dell'utente
4 - Applicazioni del RFID
Il settore dell'auto: dalla produzione all'accesso autostradale
I servizi di ticketing (on net/off net): da Dolomiti Skipass a Calipso
Monetica: principi ed applicazioni
Sicurezza informatica: costi/benefici
I beni di largo consumo: dai pallet ai prodotti finiti
Un'esperienza diretta: il magazzino di parti di ricambio di Inet

Agenda:

- Registrazione: 13,50
- Inizio Seminario: 14,10

- Fine lavori: 18,10

Docenti: Luigi Battezzati, Stefano Quintarelli
Luogo: StarHotel Splendido - Viale Andrea Doria, 4

*Condizioni e modalità di iscrizione per Soci e non soci su www.clusit.it/edu
Per ogni informazione chiedere a edu@clusit.it

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

15 marzo 2005, Roma
Seminario CLUSIT - "Sicurezza VLAN"

21-23 marzo 2005, Parigi
16° EUROSEC - Forum Européen de la Sécurité des Systèmes d'Information

22 marzo 2005, Milano
Seminario CLUSIT - "RFID"

31 marzo 2005, Milano
Corso di certificazione OPST

5-6 aprile 2005, Scandicci (FI)
ISA Server...The Firewall

12 aprile 2005, Roma
Seminario CLUSIT - "RFID"

17-20 aprile 2005, Copenhagen
ASIS International European Conference

18 aprile 2005, Roma
Corso di certificazione OPST

19 aprile 2005, Milano
Seminario CLUSIT - "Digital Right Management"

26 aprile 2005, Lugano
Convegno CLUSIS/CLUSIT al Lugano Communication Forum

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