Indice

1. NUOVI SOCI

Hanno aderito al CLUSIT le seguenti organizzazioni:

- DAM Sistemi (Reggio Emilia)
- Crovella Paolo (Casalborgone - TO)
- Electrolux Italia (Porcia - PN)
- Ingenia Direct (Conversano - BA)
- OWASP Foundation (Columbia - USA).

2. NOTIZIE DALL'ENISA

ENISA ha presentato la prima mappa dei 106 CERT (Computer Emergency Response Team) in Europa, in occasione di uno workshop il 13 e 14 Dicembre a Brussels. In Italia sono stati identificati 9 fra i 106 presenti in Europa.

Per l'aggiornamento di questo inventario dei CERT Europei, ENISA ha costituito un gruppo di lavoro specifico di esperti che forniranno ad ENISA tra le altre cose:

- la validazione dell'inventario stesso

- contatti dettagliati con i CERT

- la struttura organizzativa, le funzioni, le condizioni di partecipazione a diverse associazioni, ecc.

- una analisi delle lacune su base geografica e per area di business nelle zone non coperte dai CERT od organizzazioni simili

- raccomandazioni per il miglioramento della collaborazione tra i CERT.

La mappa e l'inventario dei 106 CERT sono rispettivamente:

www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_map.pdf

www.enisa.eu.int/doc/pdf/deliverables/enisa_cert.pdf

È disponibile l'edizione di dicembre 2005 dell'ENISA Quarterly. In questo numero particolarmente ricco di informazioni, vi segnaliamo, in particolare, gli articoli:

- sulle patch di sicurezza, che mette in luce quanto sia costoso effettuare le patch secondo le strategie usuali e propone una strategia più "economica"

- su alcuni aspetti "economici" della sicurezza e sulla nascita di un nuovo campo di approfondimento: la "security economics"

- sulle attività Europee in tema di standardizzazione della sicurezza.

Chiunque fosse interessato a ricevere l'ENISA Quarterly direttamente dall'ENISA può sottoscrivere l'abbonamento (gratuito, ovviamente) spedendo una email all'indirizzo press@enisa.eu.int, scrivendo nel Subject dell'email la parola "Subscribe".

(Fonte: Daniele Perucchini, ENISA Liaison Officer)

3. CYBERCRIME

Il laboratorio sul Phishing ci avverte che negli USA viene segnalata una nuova tipologia di attacco.

Viene indirizzata una email ad un apposito ufficio di una Istituzione, o di un Ente, contenente una richiesta di informazioni su un associato o su un operatore rilevante, riportando - ad esempio - l'indirizzo web di questi.

Onde poter rispondere, l'addetto dell'Ente si collega a detto sito e, nel far ciò, permette che un trojan venga scaricato sul suo computer.

A quanto sembra, il software criminale raccoglierà opportune informazioni (user, password, nome del computer, nome dell'utilizzatore, indirizzo IP, ecc.), aprirà una porta del computer, e, presumibilmente, invierà dette informazioni al cracker. Possiamo ipotizzare che questi, raccolte più informazioni possibili, proceda poi a valutare/predisporre un possibile attacco all'Ente preso di mira.

Il laboratorio non ha avuto modo di entrare in possesso del software trojan, né di avere - al momento - ulteriori notizie.

L'esperienza acquisita recentemente con una variante di SOBER, ha permesso di appurare che i trojan sono "migliorati" in "cattiveria", eseguendo una serie di manomissioni sul computer infettato che rendono difficile accertare e rimuovere, una volta scoperto, detto "malware" (ad esempio, disabilitano la funzionalità "regedit").

Si può quindi ipotizzare, per analogia, che la nuova minaccia si basi su questi assunti (in alternativa l'uno con l'altro):

- Il browser del computer preso di mira non è stato aggiornato con le ultime protezioni (patch);

- Il browser accetta che siano scaricati/eseguiti Active X;

- L'utilizzatore accetta di scaricare sul computer un file dal sito, giudicandolo innocuo.

Peggiora la situazione il mancato aggiornamento dell'antivirus o la mancata attivazione del personal firewall sul computer.

In conclusione, a quanto sembra anche da altre recenti notizie (consultare l'articolo all'indirizzo: www.cuispa.org/announc_12_14_05_1.html), l'attacco criminale si fa più "mirato".

Ciò significa che i criminali preparano l'attacco ad una istituzione e tendono l'esca, vanno a fare "phishing" su determinate utenze di quell'Ente.

Una volta raccolti nomi e cognomi, indirizzi internet ed altri dati personali dei dipendenti di un'azienda, quale sarà la mossa successiva?

Facciamo un'ipotesi. Se i criminali dovessero scoprire che un dipendente è pedofilo (gli trovano le foto sul computer), la mossa successiva potrebbe essere quella di contattarlo per ricattarlo. Per esempio, per chiedergli un qualche favore in cambio del silenzio? A quali seri rischi potremmo già oggi essere esposti?

Crediamo doveroso che ogni azienda faccia una seria riflessione sul suo livello di possibile esposizione ad attacchi di questo tipo e sensibilizzi il personale in tal senso. E' necessario che le aziende si rendano conto che il presidio "estremo" contro gli attacchi, costituito dalla mancata conoscenza all'esterno della propria organizzazione e delle proprie procedure, può rivelarsi superabile con estrema facilità e che, in molti casi, l'unica realistica difesa è quella di investire sulla formazione del personale.

Occorre rendere edotti i dipendenti dei rischi possibili (bastano poche ore) e soprattutto far leva sul fatto che, forse per semplice ignoranza, alcuni comportamenti possono rivelarsi a rischio per loro e per l'azienda.

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

4. STUDIO (ISC)²/IDC sulla forza lavoro nel settore della Sicurezza Informatica

Secondo lo studio sponsorizzato da (ISC)²®, i Professionisti del settore della Sicurezza Informatica stanno acquisendo sempre maggiore influenza a livello di Consiglio di Amministrazione.

Consigli di Amministrazione, CEO e CISO/CSO hanno sempre maggiori responsabilità in termini di strategie relative alla sicurezza informatica e alla gestione dei rischi.

In particolare:

- Quasi il 21% (29% nell'EMEA) degli intervistati, rispetto al 12% (16,9% nell'EMEA) nel 2004, ha affermato che il suo CEO è ora il responsabile al più alto livello della sicurezza, mentre gli intervistati per i quali il consiglio di amministrazione è ora responsabile al più alto livello della sicurezza è aumentato di circa il 6% dal 2,5% nel 2004. Gli intervistati della regione EMEA hanno rilevato la più alta incidenza di responsabilità riposta in ultima analisi presso il consiglio di amministrazione, corrispondente al 10,75% in generale e all'11,5% per i paesi dell'Europa occidentale.

- In tutte le regioni, le organizzazioni spendono in media oltre il 43% del loro budget per la sicurezza informatica in personale, istruzione e formazione. In generale, gli intervistati prevedono che, nel prossimo anno, il loro livello di istruzione e formazione aumenterà del 22%.

- I professionisti auspicano una ulteriore formazione nelle aree della business continuity (50,5% a livello mondiale, 50,6% nell'EMEA), del computer forensic (50,3% a livello mondiale, 42,86% nell'EMEA) e della gestione dei rischi (48% a livello mondiale, 51,29% nell'EMEA), aspetti questi che hanno tutti registrato una domanda superiore a quella indicata nel 2004. Nelle regioni al di fuori delle Americhe, i professionisti della sicurezza considerano la certificazione ISO/IEC 17799 quale loro massima priorità in termini di ulteriore formazione sulla sicurezza (53,9% nell'EMEA).

- Oltre il 60% degli intervistati (62,2 % nell'EMEA) ha indicato che sua intenzione conseguire almeno un certificato in sicurezza informatica nei prossimi 12 mesi. Quasi un quarto, ovvero il 23,3%, degli intervistati nell'EMEA rispetto al 5,9% degli intervistati nelle Americhe, ha affermato che la politica aziendale richiede l'ottenimento di certificazioni.

- Un maggior numero di individui ha affermato di aver conseguito un Master o equivalente - il 42% nell'EMEA, rispetto al 32% nel 2004. Nelle Americhe, il numero è aumentato al 34% dal 28% registrato nel 2004. L'11% dei professionisti della sicurezza informatica di tutto il mondo (6% nell'EMEA) ha affermato di aver conseguito un dottorato o diploma equivalente.

Questo studio conferma le positive prospettive di mercato per i professionisti nel settore della sicurezza informatica. IDC prevede che il numero dei professionisti della sicurezza, in tutto il mondo, nel 2005 sia di 1,4 milioni, un incremento del 9% (8,8% nell'EMEA) rispetto al 2004. Questa cifra è destinata a superare 1,9 milioni entro il 2009, rappresentando un tasso composto di crescita annua dell'8,5% (7,9% nell'EMEA) dal 2004 al 2009.

Lo studio e' disponibile su www.clusit.it/isc2/ISC2_IDC_2005_study.pdf

5. SEGNALAZIONE DOCUMENTI

L'Ing. Daniele Perucchini, Responsabile della sezione "Promozione della cultura della sicurezza ICT e comunicazione" dell'OCSI, ci ha segnalato due interessanti documenti:

1. la versione in inglese del "National Plan for Information Infrastructure Protection" elaborato dal Ministero degli Interni della Germania (disponibile all'indirizzo www.bmi.bund.de/cln_028/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2005/08/Information__Infrastructure__en.html)

2. il GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION presentato l'11 novembre 2005 dalla Commissione Europea (disponibile all'indirizzo: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0576en01.pdf).

Questo secondo documento fa parte di una serie di iniziative dell'EU finalizzate a combattere il terrorismo. L'elenco completo della documentazione si trova all'indirizzo http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc_criminal_terrorism_en.htm.

Segnaliamo un interessante documento sui Virus Informatici, elaborato dai colleghi del CLUSIF. Per ora il documento è disponibile solo in francese, all'indirizzo

www.clusif.asso.fr/fr/production/ouvrages/pdf/VirusInformatiques.pdf

6. NOTIZIE DA FEDERCOMIN

Il 30 novembre 2005 è stato presentato il terzo numero dell'Osservatorio semestrale della Società dell'Informazione, realizzato dal Dipartimento per l'Innovazione e le Tecnologie e Federcomin con la partecipazione di AITech-Assinform e Asstel, che analizza semestralmente lo stato e le dinamiche di utilizzo di nuove tecnologie da parte delle imprese, dei cittadini e della Pubblica Amministrazione.

L'Osservatorio è uno strumento di monitoraggio della domanda e dell'utilizzo delle tecnologie. I dati elaborati rappresentano il risultato di analisi condotte da

diversi istituti di ricerche (IDC, Italmedia Consulting, Nielsen//NetRatings) seguendo ed ampliando i parametri del Piano eEurope 2005.

Riportiamo alcuni dati significativi emersi dal secondo numero dell'Osservatorio, aggiornati generalmente a giugno 2005:

* Il settore ICT in Italia: crescita trainata dalle TLC *

Le variazioni percentuali del mercato ICT tra il primo semestre 2005 e quello 2004 indicano una crescita stimata da Assinform intorno al 2,1%, con il settore delle TLC a fare da traino (+2,9%), a fronte di un settore dell'Informatica che stenta ad uscire da un periodo di sostanziale stabilità (+0,4%). Le stime identificano come volano della crescita il mondo consumer (innovazioni di prodotto nell'intrattenimento domestico, offerta di contenuti digitali multi-piattaforma, nuove tecnologie in campo televisivo); risultano invece ancora deboli gli investimenti in innovazione tecnologica da parte delle aziende.

* I cittadini e l'innovazione tecnologica: 16 milioni di utenti UMTS nel 2006 *

Il 58% delle famiglie italiane è dotato di un PC (la crescita è di due punti percentuali rispetto all'anno precedente) ed il 43% accede ad Internet (un punto percentuale in più). Grande impulso ha avuto la telefonia di terza generazione, grazie alla sempre più ampia copertura del territorio ed alla crescente offerta di servizi a valore aggiunto. Si stima che a fine 2005 saranno più di 8 milioni gli utenti UMTS in Italia, più del triplo rispetto al 2004. Le previsioni per il 2006 indicano una ulteriore forte crescita (quasi 16 milioni di utenti).

* Le imprese ed Internet: connesse la quasi totalità delle grandi imprese *

Nel primo semestre 2005 il numero delle aziende con accesso a Internet è cresciuto fino alla quasi totalità delle grandi imprese e ad oltre il 50% delle PMI. Si tratta di un risultato molto importante, in quanto l'allargamento del numero di imprese connesse in rete permette all'intero sistema economico di godere dei benefici derivanti dalle relazioni on-line che si sviluppano con l'accesso a Internet: tra azienda e fornitori, con i clienti più importanti, con le banche e la Pubblica Amministrazione.

* La sicurezza on-line: in crescita il fenomeno del phishing *

La percentuale di aziende dotate di almeno due sistemi di difesa è cresciuto significativamente tra il 2004 e il 2005 e coinvolge ora più di 3/4 delle aziende che accedono a Internet, incluse le aziende più piccole. Fra i cittadini un navigatore su quattro sostiene di aver riscontrato problemi di sicurezza come virus o violazione dei dati personali: un dato in crescita di 3,3 punti percentuali rispetto al 2004. Così il 77,9% degli utenti web si è dotato di misure di sicurezza per proteggere il PC, un incremento di 14 punti percentuali.

Nell'ultimo anno è risultato in crescita il fenomeno del phishing (tecnica fraudolenta per carpire dati sensibili ai navigatori via e-mail), mentre è in calo quello che porta l'utilizzatore di Internet a fronteggiare inaspettatamente contenuti indesiderati od offensivi (è occorso al 28,3% dei navigatori, 3,2 punti percentuali in meno rispetto a un anno fa).

* e-Government: 11,6 milioni di cittadini contattano la PA *

Secondo una ricerca dell'Unione Europea sui servizi di Pubblica Amministrazione disponibili on-line, l'Italia è situata all'ottavo posto in Europa, con 10 servizi su 20 totalmente disponibili on-line. Dal 2001 al 2004 l'Italia è salita dal dodicesimo all'ottavo posto tra i Paesi UE a 18, con un incremento di 38 punti percentuali, e un aumento di sette servizi totalmente disponibili online.

La grande impresa mostra maggiore attitudine a contattare la PA (87%): la percentuale scende al 32% per le PMI.

Un numero crescente di cittadini decide di interfacciarsi con la PA direttamente on-line: nel secondo trimestre 2005 sono stati 11,6 milioni, 1,2 milioni in più rispetto al quarto trimestre 2004 (+12%) e 1,5 milioni in più rispetto allo stesso periodo del 2004 (+15%).

I siti della PA più visitati dagli italiani sono quelli dei Ministeri, della Comunità Europea e delle Amministrazioni locali, delle organizzazioni sindacali, dei

principali Enti pubblici e Istituzioni politiche, e il sito della Gazzetta Ufficiale per la consultazione dei bandi di concorso. Nel complesso gli utenti si reputano

soddisfatti dell'offerta attuale (60,4% degli utilizzatori intervistati sul totale).

* e-Learning: il 35% della grandi aziende lo utilizza *

Si registra un'interessante crescita nel ricorso a applicazioni di e-Learning: a giugno 2005 più del 35% della grandi aziende utilizzava strumenti di e-Learning

(le PMI si fermano al 5%). Secondo i dati del Ministero dell'Istruzione il processo di digitalizzazione delle scuole italiane ha portato nel 2005 il rapporto tra allievi e personal computer a 1 computer ogni 10 studenti, rapporto migliorato rispetto al 2004 (era di 1 a 11) e più efficiente rispetto alla media europea (che è di 1 a 13). Nel 2005 il 99% delle scuole italiane ha la connessione a Internet, l'86% accede con la banda larga, il 65% è cablato. Il 75% degli Istituti è anche dotato di un proprio sito Web.

Si mantiene bassa la percentuale di individui che ricorrono ad Internet con scopi di formazione ed istruzione: sul totale degli utilizzatori di Internet maggiori

di 14 anni, il 54,1% dichiara di ricercare on-line informazioni su argomenti di studio o lavoro, ma solo il 3,1% segue corsi di formazione on-line.

* e-Health: in aumento le prenotazioni on-line *

Il 12,8% degli utilizzatori di Internet maggiori di 14 anni dichiara di navigare per acquisire informazioni in materia sanitaria. Il dato, che indica un fenomeno

ancora circoscritto, è in crescita rispetto al 2004 (+3,4 punti percentuali) ed evidenzia una consuetudine soprattutto femminile.

Gli ospedali che permettono di prenotare una visita on line raggiungono il 10% del totale (12% nel Sud).

* e-Business: 6,1% è Il peso del commercio elettronico sul fatturato delle imprese (2004) *

Stabile risulta il rapporto on-line tra le aziende e il sistema bancario: l'utilizzo di servizi di e-Banking non cresce significativamente e continua a interessare

soprattutto le aziende di medio-grandi dimensioni (85%).

Fra i cittadini il 12,7% degli utilizzatori Internet maggiori di 14 anni dichiara di ordinare o acquistare beni e servizi on-line, una quota quasi raddoppiata

rispetto al 2004.

Al sito www.federcomin.it è disponibile un Summary della ricerca.

(Fonte: Federcomin Mail n. 37)

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