Indice

1. NUOVI SOCI

Hanno aderito al CLUSIT le seguenti organizzazioni:

- Aditinet Consulting (Milano),
- Innovation Blue (Padova)

2. CONSULTAZIONE PUBBLICA SUI CONTENUTI ON LINE NEL MERCATO UNICO EUROPEO

La Commissione apre una consultazione pCONSULTAZIONE PUBBLICA SUI CONTENUTI ON LINE NEL MERCATO UNICO EUROPEOubblica sui"Contenuti on line nel mercato unico europeo"

La consultazione pubblica "Contenuti on line nel mercato unico europeo" lanciata oggi, 28 luglio, dalla Commissione intende preparare il terreno per un vero mercato unico europeo per la fornitura dei contenuti on line. La Commissione intende incoraggiare lo sviluppo di modelli aziendali innovativi e promuovere la fornitura transfrontaliera di diversi servizi riguardanti contenuti on line. La Commissione vuole inoltre appurare in che modo le tecnologie e le apparecchiature europee possano avere successo nei mercati creativi dei contenuti on line. I contributi a questa consultazione aiuteranno ad elaborare una Comunicazione della Commissione sui contenuti on line, che dovrebbe essere adottata a fine anno. Il termine per le risposte è il 13 ottobre 2006.

La creazione di un mercato unico aperto e competitivo per i contenuti on line è uno degli obiettivi principali dell'iniziativa della UE "i2010 - Una società europea dell'informazione per la crescita e l'occupazione", varata dalla Commissione il 1° giugno 2005

(cfr.IP/05/643http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/643&format=HTML&aged=1&language=EN&guiLanguage=en).

Nel luglio 2005, i leader delle industrie del settore delle ICT e dei media avevano convenuto di collaborare con la Commissione in merito ad un Programma per lo sviluppo dell'economia digitale europea, nel quale si dava priorità alla promozione dei mercati dei contenuti dei media tramite una valida tutela dei diritti, efficaci procedure di licenza e l'incoraggiamento dell'uso legittimo dei contenuti

(cfr.IP/05/900http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/900&format=HTML&aged=1&language=EN&guiLanguage=en).

La consultazione sui contenuti on line varata oggi serve altresì a conoscere i pareri delle parti interessate sulle iniziative di autoregolamentazione quali la

Carta del film on line, a valutare se quest'ultima possa essere utilizzata come modello per iniziative analoghe in altri settori di contenuti on line e se siano richieste misure di regolamentazione a livello UE per garantire il completamento di un vero mercato UE senza frontiere per i contenuti on line.

La consultazione avviata oggi fa seguito ad iniziative precedenti della Commissione volte allo sviluppo di un mercato unico europeo per la fornitura dei servizi musicali on line.

(cfr.IP/05/1261http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/1261&format=HTML&aged=1&language=EN&guiLanguage=en).

Ulteriori informazioni sulla consultazione pubblica e sul documento di consultazione sono disponibili all'indirizzo:

http://ec.europa.eu/comm/avpolicy/other_actions/content_online/index_en.htm.

Fonte: FEDERCOMIN - www.federcomin.it

3. CYBERCRIME

Insiders.

Ci è pervenuta notizia che, tra le aziende che sono state oggetto di una recente ispezione nell'ambito di una indagine sullo scambio di materiale pedo-pornografico, vi sono anche un paio di banche italiane.

In base alle notizie in nostro possesso, coinvolti sono dei dipendenti che, consci della carenza nelle misure di sicurezza interne, hanno usato il computer dell'azienda per i loschi traffici illeciti.

Il fatto ha colto impreparate le aziende che ,a quanto sembra, non sono state in grado di fornire tutte le informazioni richieste; non sappiamo, quindi, ora a quali conseguenze andranno incontro.

Siccome purtroppo non si tratta di casi isolati, desideriamo ricordare ai colleghi che si occupano di Sicurezza che, oltre a far sì che ci siano gli opportuni controlli ed evidenze di "chi fa che cosa", siano operati anche interventi di sensibilizzazione del personale, quali: pubblicare e diffondere le "policy di sicurezza", informare il personale dell'azienda dei rischi nei quali incorre chi viola la legge mediante corsi tarati sull'azienda, ecc..

Phishing.

Su alcuni siti è stata ripresa la notizia di un attacco alla clientela che usa le "One Time Password".

Il Cliente verrebbe indotto (come è oramai usanza) a connettersi ad un sito simile a quello della propria banca e qui gli verrebbe chiesto di digitare tutti i dati in suo possesso.

A questo punto il criminale (che deve quindi essere in linea tutto il tempo) rapidamente accede al vero sito, per cercare di ricavare informazioni utili o, nel peggiore dei casi, per dirottare fondi su altri conti.

Non entriamo nel merito di questa nuova tecnica (non è questa la sede), ma ci limitiamo a fare delle semplici considerazioni, anche alla luce della recente indagine condotta da ICAA e sponsorizzata da ISCOM, SYMANTEC ed ANSSAIF.

Ricordiamo che il 5% dei Clienti, che riceve una email di "phishing", va a curiosare sul sito che gli viene indicato dalla email truffaldina. Ciò, malgrado gli avvertimenti che la stampa, la Polizia e le banche continuano a fare.

Dato che il 39% degli intervistati ha dichiarato di avere sfiducia nei sistemi di home banking, trading on line, ecc., bisogna che i media, e non solo loro (ci

riferiamo ad esempio alle Associazioni dei Consumatori, ma anche alle Pubbliche Istituzioni), intensifichino l'azione di sensibilizzazione dei cittadini.

Con l'occasione segnaliamo che la Polizia di Stato mette a disposizione dei cittadini un modulo per le richieste di chiarimento in merito ai crimini informatici, nell'apposito sito.

Potrebbe essere opportuno ricordarlo ai Clienti che accedono ai siti di Home Banking, anche mediante un semplice richiamo al sito del Ministero: www.commissariatodips.it.

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

4. LA GESTIONE DELLA FULL DISCLOSURE

Riportiamo un articolo dell'Avv. Andrea Monti, socio fondatore e membro del CD Clusit, tratto dal secondo numero di ICTLEX BRIEFS (www.ictlex.com - Note legali: www.ictlex.com/?page_id=8).

IL CONCETTO IN SINTESI

- La full disclosure è la scelta compiuta da chi ricerca vulnerabilità di sistemi operativi e applicazioni, di renderne integralmente noti i risultati.
- A seconda della tipologia delle informazioni rilasciate e delle tempistiche adottate, si possono configurare diversi livelli di responsabilità per lo scopritore dei bug.
- La scoperta di una vulnerabilità causata da una grave negligenza del produttore può provocare, a carico di quest'ultimo, l'apertura di procedimenti penali e l'attivazione di class action.
- Prima di rendere integralmente nota una vulnerabilità è opportuna segnalarla al produttore del software e alle forze di polizia.

ILCONCETTO IN TEORIA

1. La definizione

Il termine full disclosure indica la scelta "filosofica" di un programmatore o sistemista che decide rendere liberamente e gratuitamente disponibili le informazioni su vulnerabilità o difetti di progettazione/implementazione rinvenuti analizzando un dato software senza avere accesso al relativo codice sorgente.

2. Full disclosure e penetration-test abusivi

Come si è accennato nel numero precedente, la ricerca di vulnerabilità è inconciliabilmente diversa dall'eseguire penetration test non richiesti su sistemi di terze parti. Non rientra, quindi, nell'ambito della full disclosure il tentativo di "bucare" un server per poi vendere la soluzione alla vittima. Questo si chiama "estorsione" ed è un comportamento sanzionato gravemente dal codice penale.

3. Le responsabilità del bug hunter

Venendo al merito specifico delle responsabilità legate alla full disclosure è necessario distinguere due ambiti. Il primo riguarda le condizioni che rendono questa attività lecita. Nella misura in cui la ricerca è compiuta rispettando la legge sul diritto d'autore (e in particolare le limitazioni sul reverse engineering), essa non è automaticamente illegale.

Quando invece il bug hunter decide di mettere in circolazione la "ricetta" per costruire l'exploit (il software che consente di sfruttare concretamente la vulnerabilità), o addirittura l'exploit stesso, le cose possono essere diverse. Non è infatti la stessa cosa diffondere subito il dettaglio di una vulnerabilità e senza avere dato al produttore il tempo di predisporre un rimedio, o invece segnalare il

problema e attendere un periodo di tempo ragionevole prima di rendere pubblica la notizia.

Dal punto di vista tecnico ognuna delle scelte di cui sopra ha una sua giustificazione. Ma in termini di responsabilità quantomeno civilisitica le differenze ci sono e sono anche sostanziali. Pertanto è teoricamente possibile che il bug hunter possa essere portato in causa per rispondere dei danni che ha provocato, anche se non volontariamente, con la messa in circolazione del risultato dei suoi studi.

4. Le responsabilità dei produttori del software difettoso

La scoperta di una vulnerabilità - specie se collegata all'esistenza di funzioni non documentate (cioè "nascoste" dal produttore) - è fonte di una precisa responsabilità giuridica anche per chi ha realizzato e diffuso il software difettoso. Le clausole delle licenze d'uso che esonerano il produttore da qualsiasi responsabilità sono, infatti, nulle. La legge italiana stabilisce in proposito che le limitazioni contrattuali di responsabilità non valgono in caso di "dolo" (cioè di bug noto al produttore, ma da questi nascosto ai clienti) e di "colpa grave" (difetto ignoto anche al produttore, per sua negligenza o imperizia non scusabile).

Nonostante le gravi responsabilità dell'industria del software nella creazione di una infrastruttura di comunicazione geneticamente compromessa, i proprietari dei prodotti di cui si è scoperta la vulnerabilità non vedono di buon occhio l'attività di ricerca delle vulnerabilità. E, pur essendo a volte costretti a "fare buon viso a cattivo gioco", sono sempre in attesa dell'occasione per agire legalmente contro lo scopritore del bug.

Di regola, questo accade con l'invio di una lettera di cease and desist, con la quale gli avvocati dell'azienda intimano al ricercatore di cessare ogni attività di studio su un certo programma, di rimuovere ogni informazione eventualmente diffusa, e di evitare anche solo di parlare dei prodotti dell'azienda "parte lesa".

E' anche vero, tuttavia, che gli stessi produttori conoscono bene gli effetti di un'azione legale. Con particolare riferimento all'inevitabile pubblicazione di informazioni anche relative al modo in cui (non) è stato collaudato il software o l'apparato e che sarebbe meglio non far circolare. Il che potrebbe trasformarli da "carnefici" in "vittime" di azioni giudiziarie (come class action o, nei casi più gravi, addirittura procedimenti penali).

5. Conclusioni

Benchè (non sempre) ispirata da "buoni sentimenti" la full disclosure assoluta, che non tiene conto delle conseguenze della diffusione indiscriminata di determinate informazioni, può essere fonte di responsabilità per danni a carico dello scopritore di bug. E' sicuramente preferibile, e dal punto di vista giuridico più coerente, adottare una procedura di diffusione graduale delle informazioni. In primo luogo dovrebbe essere avvisato l'autore del software e, se la vulnerabilità è critica, anche le forze di polizia (Nucleo anticrimine tecnologico della Guardia di finanza, oppure Polizia delle comunicazioni). Solo successivamente, quando è stata rilasciata la patch o il produttore del software non ha inteso realizzarla, si potrebbe procedere alla diffusione pubblica della notizia e del relativo codice informatico. Perché o la falla è stata chiusa, o in caso di inerzia della software house, il pubblico ha diritto di sapere.

IL CONCETTO IN PRATICA

- Nell'attività di bug hunting è essenziale poter dimostrare di non avere violato diritti di proprietà intellettuale.
- Se si decide di rendere pubblica la scoperta del bug sarebbe opportuno contattare innanzi tutto il proprietario del software.
- Bisogna evitare, a qualsiasi costo, che il contatto di cui al punto precedente venga scambiato per un tentativo di estorsione.

5. US NATIONAL INFRASTRUCTURE PROTECTION PLAN

L'ISCOM ci segnala che è stato rilasciato il National Infrastructure Protection Plan 2006. Il documento è disponibile all'indirizzo:

www.dhs.gov/dhspublic/interweb/assetlibrary/NIPP_Plan.pdf

Per chi fosse interessato in particolare all'Homeland Security, consigliamo la consultazione del sito www.dhs.gov, dove troverete diverso materiale.

6. CLUSIT.EU

Abbiamo il piacere di segnalare che finalmente, dopo una procedura abbastanza complessa, oltre ai domini **clusit.it** e **clusit.org**, e' stato registrato anche il dominio **clusit.eu** dell'associazione: www.clusit.eu

7. NOTIZIE DAI SOCI

Segnaliamo la disponibilità di uno studente universitario a svolgere, quanto prima, uno stage oppure una tesi presso una societa' che operi nell'ambito della Sicurezza Informatica. Il richiedente sta terminando il Corso di Laurea Quinquennale in Informatica presso l'Universita' Statale di Milano.

Le aziende interessate possono scrivere a info@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