RIFLESSIONI PERSONALI SUL TEMA "**FINANZA ED HACKING**"

di: Raoul Chiesa, Divisione Sicurezza Dati @ Mediaservice.net Srl, IT
per: CLUSIT, Italia

Release: 1. Data: 28/06/2002

INDICE

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

1 INTRODUZIONE

Il matrimonio, tutto sommato recente, tra la prima fase rivoluzionaria chiamata *Information Technology* (I.T.) e le telecomunicazioni, ha portato alla nascita dell'I.C.T., *Information & Communication Technology*: il risultato sta avendo un sempre più forte impatto su moltissimi aspetti della nostra vita e sulle abitudini della "persona comune". L'I.C.T. gestisce oramai le comunicazioni - oggi espresse attraverso la telefonia fissa, mobile, le procedure bancarie interne e rivolte all'utenza finale, la gestione ed il controllo del traffico aereo, etc… - a 360 gradi.

I nuovi rischi apportati dall'enorme diffusione della tecnologia trasmissiva dei dati nei confronti dell'economia ("The New Economy", come viene chiamata) sono incredibilmente pericolosi, spesso *enormi*, non previsti o ipotizzati dai canoni standard di difesa: tutto ciò si traduce in una profonda insicurezza dei sistemi informatici, sia che essi siano bancari o, peggio, governativi.

Quello che si vuole far capire ai lettori in questo contesto è l'estremo pericolo rappresentato da un esperto di reti informatiche malintenzionato (leggasi "attacker", *cracker* o *malicious hacker*) ed i danni che egli potrebbe causare in un mercato specifico, azionario o obbligazionario.

Prima di proseguire credo sia molto importante *definire* il termine **hacker**: l'hacking è, da sempre, una filosofia di vita, uno stile, una logica mentale. Il termine originario nasce nei laboratori del M.I.T., nei primi anni '60; hacker sono stati i fondatori ed i primi utilizzatori di Arpanet, la rete che divenne poi, evolvendosi, la dorsale dell'attuale Internet, la "mamma" di tutte le reti. Hacker era, nel senso più completo e nobile del termine, Linus Torvalds, inventore di un sistema operativo(Linux) che oggi, di fatto, sta rivoluzionando il mercato; hacker sono stati i promotori del progetto **GNU** (http://www.gnu.org), per il quale oggi possiamo parlare di freeware, di **Open Source** ed **Open Software (**http://www.opensource.org), movimenti e filosofie di pensiero ed economiche i quali hanno permesso ad una piccola azienda come la Netscape Communication Inc./USA (http://www.netscape.com) di diventare il colosso che era sino a poco tempo fa, scegliendo in una delicatissima fase di espansione sul mercato la strada del Free Software prima e dell'Open Source poi per il proprio browser…

Dal lato dell'economia capiamo quindi, con questi pochi esempi, come le diverse generazioni hacker abbiano sempre dato la svolta decisiva ad una serie di evoluzioni e rivoluzioni informatiche, con forti impatti sui mercati economici e sulla vita sociale dei singoli individui.

Ho ritenuto una soluzione ottimale per rappresentare il problema svolgere una ricerca selezionando alcuni case study conosciuti a livello mondiale ed individuando - dato il mio passato e le mie conoscenze – alcuni "eventi" per lo più sconosciuti. Analizzeremo dunque i problemi collegati all'hacking su sistemi informatici bancari, il pericolo degli "insider" (attacchi dall'interno), i rischi insiti nel "trading on-line" e nei circuiti di carte di credito.

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

Sottolineo ancora, per maggior chiarezza, quanto sia raro che un hacker, nel senso puro del termine, sposi la criminalità: esiste però il serio pericolo - denunciato recentemente da famosi esponenti dello Stato italiano, non ultimo il Tenente Colonnello della Guardia di Finanza Umberto Rapetto - che hacker "deviati" accettino le richieste e gli alti profitti di una criminalità organizzata, con rischi ben chiari ed immaginabili.

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

2 CASE STUDIES

Il problema delle "banche virtuali" (fornitura di servizi bancari on-line) è scindibile in tre differenti problematiche: da un lato il **rischio di intrusioni**, che comporta l'assoluta deficienza di garanzie sul tipo di riservatezza e sicurezza nelle transazioni, dall'altro, l'enorme rischio di inaffidabilità dell'Istituto Bancario, spesso in questi episodi criminali mero **"specchietto per le allodole"**, così come vedremo in un caso di esempio; infine il gravissimo flagello del **"money laundering"**, vale a dire il riciclo di denaro sporco.

2.1 Banche virtuali e soldi facili: 1994, the European Union Bank (EUB)

I° Case History. "Banche virtuali e soldi facili": 1994, The European Union Bank (EUB).

Più o meno in quel periodo questo "istituto bancario" aprì la sua sede virtuale nelle isole Antigua, Caraibi. Una fortissima campagna pubblicitaria che la presentava come la prima banca esistente su Internet, la quale offriva tassi di interesse incredibilmente bassi e garanzie di massima riservatezza: questo era l'EUB.
In realtà dietro l'istituto troviamo due cittadini dell'ex Unione Sovietica, con un "background tecnico" di tutto rispetto:

- Alexander Konanykhine, finanziere fuggito dalla Russia nei primi anni '90, con l'accusa di aver frodato 8 milioni di USD da una banca di sua fondazione, ricercato negli Stati Uniti per immigrazione clandestina;
- Mikhail Khodorkovsky, proprietario della banca Menatep così come della Yukos Oil, la seconda compagnia petrolifera più importante in Russia, citato dalla stampa statunitense come uno dei 200 uomini più ricchi al mondo [1]

Nell'agosto del 1997 le autorità di Antigua emisero un "fraud alert", vale a dire un documento dove ufficialmente si riconosceva il pericolo di frodi bancarie da parte della EUB. Pochi giorni prima, però, i due proprietari avevano chiuso "baracca e burattini", licenziando i pochi dipendenti, facendo sparire il sito web della banca e i relativi soldi versati dagli ignari Clienti della banca…Le autorità non rivelarono mai l'entità del danno, ma è verosimile ipotizzare siano stati frodati 10 milioni di USD ai danni di persone ignare e, sicuramente, troppo avventate…

***

[1] The Village Voice, 16/9/1997

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

2.2 Il furto da un milione di dollari: riflessioni sulle politiche bancarie

II° Case History. "Il furto di 1 milione di dollari": riflessioni sulle politiche bancarie

Accennavo però prima al grande problema dell'intrusione nei sistemi bancari: lo schema che segue rende l'idea, più di mille parole, su cosa queste intrusioni possono comportare ad una banca di *piccole dimensioni*.

Ipotesi: furto di un milione di dollari da una piccola banca operante *online*	
Tipo di spesa	**Costo (dollari)**
Rimborso del denaro rubato dai conti bancari (ad esempio, 1.000 dollari per 1.000 conti)	1.000.000
Sospensione dell'operatività in rete per 48 ore per la revisione del proprio sistema di sicurezza (2 milioni per ora)	96.000.000
Controllo di emergenza sui conti bancari (250.000) per verificare quali di essi sono stati colpiti dall'attacco	1.000.000
Danni di immagine	6.000.000
Aumento dei premi assicurativi per la copertura delle frodi	5.000.000
Perdita di 10.000 conti a favore di banche concorrenti (250 dollari per conto)	2.500.000
Totale	**111.500.000**

Fonte: Forrester Research, "Expenses associated with electronic crime are high", in *The Industry Standard*, 21 settembre 1998.

Dal mio punto di vista uno dei freni all'innalzamento dei livello di I.T. Security nelle banche - sia che si parli di servizi di E-commerce e Trading on-line, sia che si parli di sicurezza verso i classici servizi forniti da una comune banca - consiste nella *non comunicazione* e *non diffusione* delle truffe subite da parte degli Istituti stessi. Mancando dunque una certa tipologia di casi, è difficile creare una *casistica esaustiva*, così come immaginare o capire cosa la criminalità (ed insisto, si tratta di criminali, non di hacker) stia facendo ed in quale direzione stia andando.

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

L'eccessiva ma logica riservatezza del mondo bancario si sta rivelando un'arma a doppio taglio, che oggi va a scapito delle banche stesse: il semplice dato di fatto della "non fiducia" dimostrata dagli istituti di credito italiani e, in taluni casini, europei, nei confronti di ex-hacker che hanno voluto mettere a frutto la loro preziosa esperienza avviando, spesso con successo, regolari attività di consulenza e servizi nel campo della security (caso sperimentato direttamente dal sottoscritto, che oggi si occupa professionalmente di sicurezza informatica) rischia di fare perdere loro la concreta visione delle cose aumentando, nel contempo, il gap tra questa realtà ed i veri pericoli di intrusione ed accessi non autorizzati.

In altre occasioni ho avuto come interlocutori Clienti (italiani), i quali non hanno posto preconcetti di base nei confronti del sottoscritto e del mio team, ma hanno scelto la strada più logica: ascoltiamoli e vediamo se hanno veramente qualcosa di rivoluzionario ed innovativo da proporci. Così è stato, ed oggi ci troviamo a dialogare ed offrire la nostra esperienza a Clienti che, solo 10 anni fa, non avrebbero certamente scelto di affidare la sicurezza dei loro sistemi informatici a realtà come la nostra.

Evidenzio come negli Stati Uniti questa sia oramai una consuetudine, un'usanza assimilata e comune, e come famosi gruppi hacker (ancora una volta, "hacking" inteso come *filosofia*, non come il "corsaro" con la benda sull'occhio che ruba carte di credito…) quali i L0PHT (http://www.l0pht.com) oggi siano divenuti una multinazionale (http://@stake.com) che annovera tra i propri Clienti una forte percentuale delle realtà presenti in "Fortune Top 500" USA, dimostrando a pieno titolo la loro riconosciuta affidabilità e professionalità: questo per il semplice e banale motivo per cui non vi è persona migliore di un ladro per verificare la sicurezza di una cassaforte…L'ha capito anche il governo americano, il quale ha nominato *The Mudge*, storico fondatore dell'hackers group, quale consulente ufficiale per la sicurezza informatica del proprio paese.

***

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

2.3 La new economy ed i mass-media: il pericolo della "perdita di fiducia" ed il panico globale; i casi Fineco On-line e Servizi Interbancari

III° Case History. "La new economy ed i mass-media": il pericolo della "perdita di fiducia" ed il panico globale; i casi Fineco On-line e Servizi Interbancari.

Come illustrai nell'articolo "La bolla di sapone che ha sconvolto il mondo: e cosa succede se gli hacker arrivano davvero" (pubblicato da **Internos Editore**, http://www.internos.it/archivio/rc12.html, e da **Apogeo Editore** http://www.apogeonline.com/riflessi/art_171.htm), un primo serio pericolo è la forte amplificazione che riscuotono argomenti quali l'hacking, le intrusioni, le truffe e la mancanza di sicurezza in Rete.

Voglio portare come esempio due casi, due "bolle di sapone", che hanno veramente portato preoccupazioni e paure, spesso totalmente infondate, tralasciando così, volutamente, i casi sensazionalistici riguardanti gli attacchi a Yahoo.com ed Amazon.com avvenuti i primi mesi del 2000. Mi riferisco ai casi **Fineco On-line** (http://www.fineco.it) e **Servizi Interbancari**, due esempi "made in Italy"

2.3.1 Fineco On-line

Fineco On-line parte agli inizi del 2000 con un'enorme campagna pubblicitaria: possiamo dire che il successo del termine "new economy", nel nostro Paese, sia merito loro. Il primo problema è la visione, allarmistica secondo il mio punto di vista, di tanti italiani che giocano a fare i broker, da casa propria ed a qualunque ora, interpretando però quello che è il mercato borsistico come un "gioco d'azzardo" on-line.
Il secondo problema è rappresentato dalla sicurezza del sistema informatico e comunicativo. In questo contesto non tecnico ritengo fuori luogo commentare le scelte operative effettuate e quindi mi limito al "dovere di cronaca".

Il 3 febbraio **Fineco On-line SIM**, società del gruppo Bipop-Carire che raggruppa le attività di trading on-line, ha "inavvertitamente inviato, tramite un mailing list dati, riservati di clienti" che aderiscono al loro servizio di transazioni borsistiche on-line. In pratica questo significa che su un mailing list del servizio di trading on-line sono circolati messaggi contenenti dati personali, comprensivi di riferimenti bancari, riguardanti alcuni dei clienti abbonati al servizio.
Prima si è parlato di possibile sequestro del server (a che scopo poi ? In questi anni nulla è stato imparato? Esistono i backup e rappresentano la soluzione migliore..), per passare, poi, direttamente a sdrammatizzare l'accaduto, spiegando che "i dati inviati xxx sono solo dati generici xxx".
Ammettiamo pure la veridicità di quest'informazione, ma se per caso quel modulo dati fosse stato di un altro tipo, i dati sensibili sarebbero usciti fuori e magari sarebbe stato sufficiente spingere il mouse un pochino più in su per selezionare un altro file...

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

Quello che segue è il comunicato apparso sul sito di informazione deandreis.it (http://www.deandreis.it/p.asp?i=30562):

03/02/00 - News - Roma - Definire imbarazzante quanto accaduto nelle scorse ore a FINECO è quantomeno riduttivo. Uno dei principali servizi di trading online italiani si trova infatti nell'occhio del ciclone perché dati personali e riferimenti bancari di numerosi utenti sono girati pubblicamente su una mailing list dedicata.
Va detto che la mailing list è aperta ai numerosi utenti del servizio e lo scambio di molte email "compromettenti" è stato originato da un primo messaggio di un cliente, messaggio indirizzato alla mailing list ("per errore", secondo FINECO). Nella pioggia di email generate dal buco nella sicurezza gli utenti, tra l'altro, hanno denunciato con forza l'inefficienza complessiva del servizio.
Di fronte a questi eventi il Centro Servizi Legali, come richiesto da uno degli utenti FINECO, ha immediatamente presentato alla magistratura competente denuncia civile e penale, con richiesta conseguente di danni e di sequestro del server dell'azienda.
Alle proteste dell'utente, che ha poi deciso di intraprendere l'azione giudiziaria, finora da FINECO è pervenuta soltanto una mail firmata dal direttore generale della società. Un messaggio nel quale si sostiene che l'azienda "NON ha direttamente distribuito dati personali, ma, attraverso la propria lista di distribuzione, ha INVOLONTARIAMENTE e PER POCHI MINUTI diffuso messaggi tra gli utenti". Una lettera nella quale si afferma tra l'altro che "l'episodio (...) può essere ricondotto ad una situazione particolare e non invece ad una leggerezza". Una risposta stigmatizzata dai legali secondo cui "si ammette il grave errore commesso tentando una puerile giustificazione tecnicamente non accettabile".
Dinanzi ad una palese violazione della riservatezza dei dati finanziari, della privacy dei dati personali, dinanzi alla divulgazione di numeri di conto corrente e loro ubicazione, la risposta della FINECO ha indubbiamente caratteristiche di inaspettata superficialità.
In un momento nel quale con l'hacking ai server Visa, ammessi dalla stessa azienda, con gli scandali delle transazioni online denunciati ripetutamente da MSNBC, l'e-commerce e il business online sono "sfidati" come mai prima, la reazione della FINECO appare ancora più "disastrosa" perché non sembra prendere in serissima considerazione l'intera problematica della sicurezza che appare, al contrario, ampiamente sottovalutata.

Ben tre mesi prima il sistema del **Nasdaq** fu violato, rendendo così possibile agli intrusi variare in tempo reale il valore delle azioni, oggetto delle transazioni borsistiche. Tutto ciò che rimane di questo attacco è una frase che recita più o meno: “potremmo cambiare i valori azionari di alcuni titoli e fare speculazione: *invece vi lasciamo questo messaggio e torniamo ad impacchettare hambuger al Mac Donald’s*...”

Risulta quindi ovvio, al di là del livello di pericolosità dell’accaduto, quanto le ripercussioni e le amplificazioni al problema – sia da parte dei mass-media che da parte degli addetti ai settori toccati come gli esponenti del mondo bancario e del trading nonché di quello tipicamente *underground* o degli utilizzatori finali dei servizi– siano spesso eccessive, causando conseguentemente instabilità a livello di mercato. Questo è uno dei prezzi, a parer mio, della globalizzazione, in un mercato come quello borsistico che dipende fortemente dagli Stati Uniti e nel quale i “segnali di allarme” non sono più controllabili o gestibili come prima. Arriva allora il rischio dell’aggiotaggio, della falsificazione delle informazioni, con il chiaro ed unico scopo di creare destabilizzazione ed effettuare speculazioni in “real time”.

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

2.3.2 Servizi Interbancari

Il secondo caso riguarda la Servizi Interbancari: nel 1999 un gruppo di "hacker" inglesi ha interpellato la VISA europea con l'obiettivo di ricattare la società, asserendo di essere in possesso di migliaia di numero di carte di credito e chiedendo così un'altissima cifra per non diffondere questi codici.
I primi risultati si sono visti immediatamente e seguono anche in questo caso il percorso di Fineco On-line: destabilizzazione del mercato piuttosto che eventuale calo borsistico delle società implicate, disinformazione verso gli utenti finali ed i consumatori dei servizi, perdita di fiducia da parte degli stessi nei confronti dell'erogatore.

La Servizi Interbancari ha subito lanciato un allarme, avvertendo di "non utilizzare le carte di credito sulla Rete Internet" (niente di più sbagliato), per poi venire a sapere che, a quanto pare, era tutto una "grossa bufala", o un ottimo soffocamento della notizia. Il risultato comunque è che, stando a sondaggi del febbraio 2000, il 70% degli italiani ha paura ad utilizzare Internet, non ha fiducia nella sicurezza dei sistemi e giudica "inaffidabili" i servizi attualmente disponibili. E' dunque rimasta una traccia ben definita nella mentalità comune dei clienti o possibili clienti del servizio.

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

3 CONCLUSIONI

I rischi della diffusione ed evoluzione delle tecnologie informatiche e delle comunicazioni, in particolare nel settore finanziario, sono di diversa natura ed in ogni caso elevatissimi. Le aree interessate ed i relativi pericoli sono identificabili come segue:

- Commercio on-line
- Circuiti di carte di credito
- Paradisi fiscali "virtuali" ("cyber-paradisi")
- Istituti bancari privati e pubblici (banche on-line)
- Organi di controllo delle operazioni bancarie
- Organi di controllo delle operazioni borsistiche
- Transazioni bancarie "bank to bank" (Wire transfer quali: SWIFT, Fedwire, ACH)
- Transazioni bancarie "bank to end-user" (Home Banking, Web Banking)
- Riciclo di denaro tramite casinò on-line o siti pornografici a pagamento, utilizzando paesi offshore come base tecnico-logistica
- Attacchi dall'esterno (hacking)
- Utilizzo abusivo dall'interno (insider)
- Trading on-line (dal lato "hacking" può corrispondere ad un'interruzione del servizio con conseguente inaccessibilità allo stesso da parte dei clienti, o infiltrazioni e modifiche ai listini cambi o alle transazioni, diffusione di informazioni riservate, etc..)
- Trading on-line (dal lato "abuso della Rete", ad esempio utilizzando l'amplificazione che la stessa offre al fine di diffondere false notizie con ampio risalto, ed ottenere il conseguente rialzo o calo del valore delle azioni della società target)
- Fisco telematico
- Commercialisti che utilizzino l'invio telematico al Ministero delle Finanze
- Servizi amministrativi dello Stato on-line

oltre a

- Spionaggio industriale (grandi aziende)
- Spionaggio militare e/o governativo (archivi di Stato)
- PMI
- …….

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

Internet non è un "pericolo obbligato", è anzi una rete di comunicazioni che sta cambiando completamente le opportunità di business e di commercio, a livello mondiale.
Da un lato abbiamo carenze e mal interpretazioni legislative, le quali non aiutano e sono spesso troppo complicate, dall'altro ci troviamo di fronte al serio pericolo che hacker altamente capaci sposino la causa della criminalità organizzata e dello spionaggio industriale o governativo ad alto livello: il rimedio deciso negli Stati Uniti in questi ultimi anni è quello dell'utilizzo di queste persone per migliorare la sicurezza dei sistemi governativi, bancari e delle società multinazionali.
In Italia questa soluzione sta iniziando ad essere presa in seria considerazione tramite le prime proposte avanzate da alcuni responsabili statali ed esperti in sicurezza informatica; in Germania ed in Olanda da alcuni anni i clienti di noti ex-hacker sono importanti aziende a livello nazionale; in Oriente l'intero sistema di e-commerce tailandese è stato realizzato da una società locale, fondata da due ex hacker, un francese ed un serbo.

Le soluzioni sono classificabili nel seguente ordine logico di svolgimento:

1. effettuare un'attenta e profonda analisi dei rischi, esistenti o ipotizzabili, di quella che è la "nuova finanza digitale" (limitandosi dunque ad analizzare questo lato della problematica), al fine di identificarne i punti deboli e le possibili soluzioni;
2. istituire gruppi di studio altamente qualificati per l'analisi delle problematiche e la definizioni delle soluzioni;
3. affidarsi a chi veramente sa e conosce la Rete ed i relativi pro e contro, a chi conosce le realtà tecnologiche della nuova generazione così come le risorse *underground*: in altre parole, al mondo hacking che ha deciso di farne una seria e qualificata professione;
4. svolgere attente verifiche della solidità informatica, sul fronte sicurezza a 360°, nei settori toccati da questi nuovi fenomeni: ciò può avvenire "interfacciando" i gruppi di studio (teorici) con consulenti specializzati (pratici), al fine di analizzare e prevedere ogni tipologia e logica di attacco;
5. presidiare continuamente i sistemi con una nuova mentalità verso le possibilità di attacco(*aggressive defense*) ;
6. comprendere le realtà della rivoluzione tecnologica attualmente in corso e regolarsi di conseguenza, evitando di limitarsi ad una visione *locale* o attuale: la tecnologia corre, i piani di aggiornamento teorici e pratici e le previsioni devono essere futuristiche oggi per poter poi divenire concrete nell'immediato futuro economico.

Raoul Chiesa
*Chief Technical Officer, @ MediaService.net Srl (Italia) - **D.S.D. D**ivisione **S**icurezza **D**ati*
Socio Fondatore e Membro del Consiglio Direttivo di CLUSIT – Associazione Italiana per la Sicurezza Informatica

4 L'AUTORE

Raoul Chiesa nasce a Torino il 3/7/73: è uno dei primi hacker d'Italia.

All'età di 13 anni comincia, con il *nickname* Nobody, il suo pellegrinaggio attraverso le reti informatiche e dopo una serie di eclatanti intrusioni in grossi Enti ed Istituzioni - tra le quali Bankitalia, IBM e AT&T - la sua fama, già vasta nella comunità hacker europea, è riconosciuta e suggellata dalle autorità internazionali.

Nel 1997 fonda la MediaService ed oggi, a capo della @ MediaService.net, si occupa oramai da anni di sicurezza informatica ad alto livello, insieme ad un selezionato team di tecnici ed esperti, con collaborazioni internazionali. Istituti di Ricerca e Multinazionali si avvalgono della sua collaborazione, senza contare il suo riconosciuto e singolare impegno in un'opera di diplomazia tecnologica, con la quale mira a promuovere una seria coesistenza tra il più genuino spirito hacker e l'IT Security nel nostro Paese.

Oggi @ MediaService.net guarda all'esempio americano dei L0pht, dove la voglia di cultura informatica e perfezionamento continuo della sicurezza informatica sono i pilastri di un'azienda con una mission ed una visione completamente nuova, vendor-independent ed aperta verso la filosofia Open Source. Con questi principi è nata la D.S.D., la Divisione Sicurezza Dati dell'azienda.

Il suo modello è l'hacker "etico" (ethical hacker): nelle interviste televisive, così in quelle concesse ai principali quotidiani nazionali (La Stampa, Il Sole 24 Ore, Repubblica, il Messaggero) ed ai periodici specializzati e non (Computer Facile, Max, Panorama, l'Espresso), si dichiara fedele allo spirito e agli obblighi morali dell'"hacking" più genuino, difendendo la sete di conoscenza e non l'attacco gratuito e dannoso ai sistemi informatici.

In quest'ottica è intervenuto come relatore a svariati convegni: "L'hacker e il magistrato" (Pescara 1998), "L'hacker e la legge" (Ciampino), "Pirateria Informatica" (Futur Show, Bologna, 1999) e ha organizzato inoltre, in collaborazione con l'Unione Industriale di Torino, "Imprese e Sicurezza Informatica" (Torino 1999) e partecipato all'ultimo convegno "New Economy, Nuova Editoria" presso il Salone del Libro di Torino (maggio 2000), confermando il suo costante impegno mirato all'evoluzione continua ed allo sviluppo della I.C.T. (*Information & Communication Technology*) Security nella sua più naturale applicazione: la protezione dei dati "sensibili" delle imprese.

Scrive articoli sul controllo e lo sviluppo di Internet, pubblicati da riviste on-line tra cui Internos.it, Apogeonline.com, Affari Italiani, Mondadori My Tech e PC Magazine Italia, convinto dell'importanza di diffondere cultura **in** e **sulla** Rete, tramite una continua e sempre maggiore *informazione su tutto quello che gravita intorno ad essa*, con un occhio di riguardo alla vulnerabilità dei sistemi informatici ed alle continue evoluzioni tecnologiche, anche segno di cambiamento dei tempi.

Sede legale: Via Schierano, 21 – 10064 Pinerolo (TO) - P.IVA 08006220019
Uffici: Via Raffaele Cadorna, 47 - 10137 Torino (Italy)
Tel. +39 011 3272100 - Fax +39 011 3246497
mailto:info@mediaservice.net http://@mediaservice.net

Cura rubriche on-line e cartacee ed ha tenuto lezioni di specializzazione e partecipato a conferenze per le Università di Trento (Transcrime, Centro Interdipartimentale di Ricerca sulla Criminalità Transnazionale dell'Università di Trento), Milano (D.S.I. Dipartimento di Scienza dell'Informazione), Cosenza, Torino, Biella, Pisa, Bologna.

E' membro del Comitato Direttivo del CLUSIT (Associazione Italiana per la Sicurezza Informatica, http://www.clusit.it) dalla fondazione dell'Associazione con carica sino al dicembre 2002 e docente al Master in Sicurezza Informatica del Dipartimento di Scienze dell'Informazione presso l'Università di Milano.

Nel 2001 è tra i fondatori, insieme a Marco Ivaldi aka Raptor e Fabio Pietrosanti aka Naif di ITBH, Italian Black Hats Association (http://www.blackhats.it).
Blackhats.it è una comunità di ricerca sorta spontaneamente, formata da un gruppo dieci persone: hackers, esperti di security, alcuni che lavorano nel mondo dell'I.T., altri impegnati come ricercatori.
Professionisti della sicurezza informatica, con forti legami al mondo underground ed alla filosofia hacker, che si dedicano a migliorare la sicurezza della rete Internet. Lo fanno per proprio conto e con risorse proprie, dedicando il tempo personale a questa passione.
Altre figure si aggiungeranno nel tempo, in quanto Blackhats.it è una comunità aperta a tutti coloro i quali vedono l'I.T. Security da punti di vista differenti dai canoni standard, lontano dai legami e dagli obblighi commerciali e vicino alla filosofia Open Source.

L'autore è raggiungibile ai seguenti indirizzi E-mail:

raoul.chiesa@mediaservice.net (Aziendale)
rchiesa@clusit.it (Clusit)
raoul@raoul.EU.org (Personale)
nobody@blackhats.it (ITBH)

PGP Fingerprint: 17E3 CF8C BDE9 E5A3 2ED7 97BB 31F9 60FA