Crimini informatici e crimini giornalistici

Sbatti l'*hacker* in prima pagina

Il crimine tecnologico è una ghiotta occasione per titoli sensazionali e pezzi «di colore». Ma bisogna smetterla di fornire notizie esagerate, se non addirittura false, e di esaltare i giovani pirati telematici. L'opinione del sostituto procuratore Giuseppe Corasaniti, in prima linea contro il computer crime

di Manlio Cammarata

Notizie di cronaca, 4 giugno: «Catturato il pirata che entrò nei computer della Banca di Italia»: il fatto merita titoli di scatola, intere pagine di giornali con servizi e interviste. Ma a chi conosce un po' fatti e misfatti del ciberspazio italiano capisce subito che è una «bufala», come si dice a Roma.

Prima di tutto perché nessuno ha mai violato, che si sappia, i computer del *bunker* della Banca d'Italia. Il 30 settembre dell'anno scorso qualcuno lasciò un messaggio firmato «Falange armata» in un server collegato a Internet, ma del tutto separato dal sistema informativo dell'istituto di emissione. In secondo luogo perché la stessa «Falange armata» molto probabilmente è un'altra «bufala», per quanto riguarda le azioni telematiche. Riflettiamo un attimo. Arriva un messaggio che dice: ho la parola chiave per entrare nel tuo sistema. La risposta è semplice: e allora, perché non la usi, se vuoi spaventarmi? Poi, nel dubbio, sai che ti dico? Che io la cambio, la parola chiave... Se il terrorismo fosse fatto solo di questi messaggi potremmo dormire sonni tranquilli. In realtà continuo a chiedermi se siano più pericolosi *hacker* e *cracker*, o certi amministratori di sistema che continuano a usare password come «Pippo», «sysadmin» o la data di nascita del primo figlio.

Andiamo avanti. 5 giugno: Contrordine, il pirata non è lui! Il sostituto procuratore Giuseppe Corasaniti, il noto *hackerbuster* della Pretura circondariale di Roma, fa sapere che si è già occupato del giovane siracusano all'inizio dell'operazione «Ice Trap» (vedi MCmicrocomputer n. 159, febbraio '96), ma che era risultato estraneo alla vicenda della Falange armata. Che cosa resta?

Restano i giornali che trattano i delinquenti telematici come divi, con tanto di interviste, riciclano notizie vecchie di sei mesi «sette arrestati per l'assalto a Bankitalia» e si diffondono in inquietanti dietrologismi (lo pseudonimo del pirata di Siracusa era «Ice», perché aveva violato il computer di una fabbrica di gelati, ma l'operazione della Procura di Roma contro la Falange telematica era chiamata in codice «Ice Trap», e allora chi manovrava il ragazzo?); resta il fatto che ci sono sistemi, come quello di Matera usato per le incursioni telematiche, assolutamente insicuri; resta l'alzataccia del vostro cronista, buttato giù dal letto a un'ora antelucana per spiegare agli assonnati ascoltatori di «Unomattina» fatti e misfatti del ciberspazio. Soprattutto resta un ragazzo che da una parte viene descritto come un pericoloso terrorista e dall'altra viene mitizzato come «il genietto della telematica» (*Il Messaggero*) o «il re dei baby-hackers» (*la Repubblica*). Ed è difficile dire quale sia l'aspetto più grave, perché l'esposizione al pubblico ludibrio viola i diritti della persona, mentre l'esaltazione stimola comportamenti imitativi.

Ma il problema è serio

Centocinquantamila tentativi di violazione dei sistemi del Pentagono negli ultimi anni: lo ha detto il presidente Clinton, annunciando la costituzione di una speciale *task force* per combattere il crimine telematico. La cifra forse non è alta, se si pensa al successo di film come «War Games» e dei suoi epigoni e se si considera il numero di ragazzini americani e non che dispongono di PC e modem. Ma comunque fa impressione. Il problema è se uno solo di questi assalti è riuscito, se qualcuno è riuscito a leggere informazioni riservate o a danneggiare qualcosa. E, soprattutto se il sistema è adeguatamente protetto. Questo è il punto fondamentale.

Si deve considerare che oggi l'intera struttura della società mondiale funziona grazie ai prodotti delle tecnologie dell'informazione. Trasporti, difesa, sanità, protezione civile, commercio, finanza, persino la distribuzione dei tagliandi milionari del «Gratta e vinci» nostrano sono governati da computer e da reti telematiche. La vulnerabilità dei sistemi mette a rischio tutto l'assetto socio-ecomico dei paesi industrializzati, e non solo di questi.

Dunque la parola d'ordine deve essere «sicurezza». I sistemi devono essere protetti con tutti i mezzi oggi disponibili, passivi e attivi. La sicurezza passiva è quella che deriva dalla ricerca sistematica e dalla conseguente chiusura di tutti i «buchi» potenziali; quella attiva è data dall'adozione e dalla gestione intelligente di tutte le difese logiche e fisiche che è ragionevole impiegare, anche se a volte possono complicare la vita degli utilizzatori. E qui torniamo al vecchio discorso della «cultura della sicurezza», che va dalla struttura delle password alla loro conservazione, alle sanzioni per chi, all'interno di un'organizzazione, lascia in giro la


PIRATI INFORMATICI

I giudici Corsaniti e Saviotti: il giovane siracusano denunciato non firmò l'intrusione

Contrordine, non è "Ice" il pirata di Bankitalia

Per l'assalto telematico incriminati a Roma 7 "hacker"

CRONACHE ITALIANE

tt'anni, terrore di Bankitalia

i Siracusa violava computer super-protetti firmandosi "Falange Armata"

IL CRIMINE CORRE SUL FILO

Quattro cyber-gang ricattano gli istituti di credito

PIRATI INFORMATICI

Armato di tastiera e telefono navigò via Internet fino al bersaglio e si firmò "Falange armata"

Ha 17 anni il re dei baby-hackers

Uno studente violò il computer nel bunker della Banca d'Italia

BANCA D'ITALIA

L'IDENTIKIT

"Sono un pericolo, in Italia provocano danni per 100 miliardi"

sua «chiave» o non la cambia entro scadenze prestabilite.

Poi occorrono leggi che rendano obbligatoria l'adozione di misure minime di sicurezza, come l'identificazione degli utenti dei sistemi telematici, della quale molte volte abbiamo parlato. Ma qui siamo in alto mare, se pensiamo all'ultima trovata commerciale di Telecom Italia Mobile, che offre una card del tutto anonima per utilizzare i telefonini GSM (si veda l'editoriale di Paolo Nuti del mese scorso): sai che pacchia per mafiosi, trafficanti di droga e malfattori di ogni genere, se gli inquirenti non sanno chi intercettare! E c'è la legge 547/93, che punisce chi si intrufola in un sistema «protetto da misure di sicurezza», ma non punisce l'omissione delle misure stesse, che in molti casi può costituire un pericolo anche per i terzi, i cui dati siano archiviati in un sistema troppo vulnerabile. Sempre a proposito della legge 547/93, si dovrebbero aggiungere norme procedurali che con-

Il comunicato di ALCEI

ALCEI, l'Associazione per la Libera Comunicazione Elettronica Interattiva, ha commentato le cronache del 4 giugno con un comunicato diffuso via Internet, che vale la pena di riportare integralmente.

COMUNICATO STAMPA 5 giugno 1996

Un anno fa vi fu un grande clamore intorno alla presunta aggressione telematica ai danni dell'agenzia ADN Kronos e che, alla luce dei fatti, si era poi rivelato essere un episodio privo di consistenza. Tra l'altro, in quell'occasione, nessuno si era preoccupato di rendere note all'opinione pubblica le conclusioni degli inquirenti. Adesso giunge la notizia dell'individuazione di «IceMc», uno studente di diciassette anni, quale presunto responsabile di una serie imprecisata di accessi abusivi perpetrati in punti isolati e mal protetti delle reti telematiche. Soliti titoli a pagina intera, informazione scarsa, la notizia, così come presentata risulta risibile.

Il fatto, che poteva costituire l'occasione per una riflessione seria sui temi della libertà nella rete, ha purtroppo ceduto il passo ancora una volta alla «vena» sensazionalistica e superficiale che ha caratterizzato trasversalmente la quasi totalità dei mezzi di informazione.

Vi sono giornalisti seri e competenti che con pazienza scrivono articoli validi e pur avendo un'ottima conoscenza delle problematiche reali delle reti di calcolatori e della comunicazione elettronica continuano ad essere relegati sulla stampa specializzata o entro spazi ridottissimi.

Non manca dunque l'intelligenza ma la volontà che essa venga impiegata per dare informazione di qualità, e questo ci preoccupa molto più di quanto la rete telematica preoccupi i lettori. Con o senza innocui quanto pittoreschi «hacker».

ALCEI, l'Associazione per la Libera Comunicazione Elettronica Interattiva si dispiace di dover denunciare ancora una volta questo approccio distorto che non tiene conto dei reali problemi e distoglie l'attenzione del pubblico da quelle che sono le infinite opportunità culturali, sociali ed economiche che si sviluppano intorno alla rete.

Come sempre ALCEI è a disposizione di chi voglia maggiori informazioni sull'argomento:

alcei@alcei.sublink.org

http:// www.nexus.it/alcei

Credo che siano opportuni tre «distinguo». Primo: l'assalto telematico all'ADN Kronos non è stato «un episodio privo di consistenza», come afferma ALCEI, ma un atto abbastanza grave, chiunque sia stato il suo autore (la Falange armata, vera o sedicente, o forse qualche «interno», come spesso accade in questi casi). Secondo: la «riflessione sulla libertà della rete» deve considerare anche il diritto di essere protetti da intrusioni indebite. Terzo: un hacker potrà anche essere «pittoresco», è una questione di punti di vista, ma non è mai innocuo, proprio perché viola i diritti degli altri. È una persona che commette un atto illecito, penalmente perseguibile (nei casi meno gravi) ai sensi degli articoli 615-ter e 615-quater del codice penale. Dunque è un delinquente.

(Manlio Cammarata)

sentano alla magistratura di disporre intercettazioni e «tracciamenti» in tempi brevissimi, assicurando anche la disponibilità delle apparecchiature necessarie (si veda in queste pagine l'intervista al PM Corasaniti).

Soprattutto è necessario rendersi conto che gli *hacker* non sono i giovani eroi romantici del nostro tempo. La violazione di un sistema telematico protetto è sempre un crimine, il cui autore deve essere punito. È vero che, come afferma ancora Corasaniti, bisogna distinguere tra le motivazioni di un ragazzino che vuole misurare e dimostrare la propria abilità, e quelle di un delinquente adulto che compie deliberatamente atti illeciti, a scopo di lucro, terrorismo o altro. L'integrità dei sistemi informativi e delle reti di telecomunicazioni è un bene troppo importante, che deve essere difeso anche contro comportamenti che possono rientrare nel novero delle «ragazzate». Dunque bisogna smetterla di presentare i giovani delinquenti tecnologici come geni o eroi. Il magistrato potrà forse essere un po' più indulgente contro il violatore di fabbriche di gelati e severissimo nei confronti del vero delinquente telematico, ma il giornalista

Hackerbuster: la parola a Corasaniti

Al sostituto procuratore presso la Pretura circondariale di Roma Giuseppe Corasaniti, dotato di una vasta preparazione informatica, vengono affidate le indagini più delicate che hanno per oggetto episodi di computer crime, intercettazioni, duplicazione abusiva di software. Gli ho chiesto di commentare i recenti fatti di cronaca

Dottor Corasaniti, a che punto siamo con le indagini sugli hacker di casa nostra, la Falange telematica e tutto il resto? Dai titoli dei giornali sembra che sia scoppiato il finimondo, ma poi gli articoli non dicono niente di nuovo.

Giuseppe Corasaniti.

Per quanto riguarda la «Falange», se ne occupa il collega Saviotti e quindi mi è difficile rispondere. Per quanto riguarda l'operazione «Ice Trap», condotta da me, siamo al lavoro. Stiamo visionando tutto il materiale intercettato, e la cosa naturalmente richiede un certo tempo, anche sotto il profilo tecnico. Posso dire che per la prima volta abbiamo sperimentato attrezzature sicuramente all'avanguardia in Europa, e le abbiamo sperimentate attraverso il Servizio centrale operativo della Polizia di Stato. Questa operazione dei Carabinieri, francamente, mi lascia perplesso. Non sono come sono arrivati al ragazzo di Siracusa, non vorrei che tutto sia nato da una fonte confidenziale. Le indagini in materia di criminalità informatica non si basano su fonti confidenziali o su dichiarazioni, si basano su riscontri oggettivi. Sono indagini semplici, se si vuole, ma richiedono una certa abilità tecnologica e anche una discreta dose di fortuna, probabilmente. Ma dal punto di vista dei riscontri, poi, sono chiarissime.

Nella nostra indagine ci siamo trovati di fronte a un'organizzazione strutturata, al punto che per la prima volta è stata contestata l'associazione a delinquere per la commissione di questi reati, e non mi pare una cosa da poco. I giornali parlano di sette persone, ma in realtà il numero è molto più elevato, perché complessivamente i soggetti che ho identificato sono ventisei, fra cui le sette con posizioni particolarmente serie, già valutate dalla Procura presso il Tribunale e per le quali sono stati anche emessi i provvedimenti cautelari di cui abbiamo parlato a suo tempo (*il «carcere virtuale», arresti domiciliari senza linea telefonica, si veda MCmicrocomputer n. 159, ndr*).

Dunque «sbatti l'hacker in prima pagina», ma non è lui...

Il nucleo più pericoloso dei criminali informatici era nel Nord Italia. Si tratta di persone che hanno una grande capacità criminale e che sfruttano bene le attività illecite da punto di vista economico. Ovviamente si tratta di maggiorenni. Non condivido quello che hanno fatto i giornali. L'uscita giornalistica probabilmente è avvenuta in coincidenza con l'annuncio di Clinton sulla forza di intervento rapido del Dipartimento della Giustizia degli Stati Uniti. Clinton ha ricordato che i tentativi di accesso al Pentagono negli ultimi anni sono stati centocinquantamila, e questo ha preoccupato l'opinione pubblica. Però l'*hacker*, soprattutto quando è un minorenne, non va né mitizzato né sbattuto in prima pagina. Perché è un ragazzo, e ogni ragazzo, soprattutto se si trova coinvolto in un illecito penale, merita assolutamente il rispetto della sua dignità: innanzitutto l'anonimato, anche se, quando

deve essere sempre rigoroso nei contenuti e nel modo di presentare le notizie, chiedendosi quali conseguenze certi messaggi possono avere su un pubblico immaturo e, a volte, con carenze educative non trascurabili.

Infine, ma non certo ultimo, resta l'aspetto della repressione. Qui sono stati fatti notevoli passi avanti dai tempi di «Fidobust» (ricordate l'azione della Procura di Pesaro, due anni fa, nella quale furono sequestrati persino i tappetini dei mouse?) e le forze di polizia in molti casi agiscono con maggiore competenza. A Genova è stata appena inaugurata una nuova scuola per la Polizia postale. Possiamo stare certi che, al di là dell'apparenza della denominazione, non passeranno certo il tempo a controllare la filigrana dei francobolli! Mentre la sezione Criminalità informatica del Servizio centrale operativo della Polizia di Stato viene potenziata e collegata al Ministero delle poste, con un'articolazione territoriale che consentirà interventi rapidi in tutta la Penisola. Insomma, stiamo per avere anche noi le «teste di cuoio» della tecnologia. È una buona notizia, ne riparleremo presto.

si tratta di una persona che vive in una piccola città, l'anonimato è molto ipotetico. L'atteggiamento deve essere né di mitizzare queste forme criminali, che sono forme criminali come tante altre, né di esaltarne l'azione dal punto di vista giornalistico. Indubbiamente si tratta di un'attività criminale che viene svolta in larga parte da ragazzi, ma per questo va studiata e bisogna anche comprenderne a fondo le motivazioni. Quando un minorenne si dedica a un'attività illecita, ha delle motivazioni, che sono di vita, che sono di conoscenza dei sistemi, che derivano anche dal gusto di violare i palazzi del potere. Sono motivazioni molto diverse da quelle di un criminale vero che fa questo tipo di attività a scopo di guadagno o per altri fini illeciti.

Bisogna porre molta attenzione, soprattutto da parte dei genitori, quando hanno in casa attrezzature di questo genere, anche perché ci sono stati molti casi di minorenni coinvolti in attività di duplicazione ben organizzata. Ci vuole ben poco a farla, e a volte è anche difficile il *discrimen* fra l'attività di duplicazione per gioco, fra amici, e l'attività di duplicazione che diventa una piccola attività commerciale illecita. Vedo come un rischio concreto lo sfruttamento di un minorenne, anche via modem, offrendogli possibilità di guadagno con la duplicazione del software. Abbiamo visto genitori che non si rendevano assolutamente conto di che cosa facevano i figli, e se li sono trovati sul giornale coinvolti in attività di pirateria informatica. Anche per questo è necessario cominciare a costruire una cultura del rispetto delle regole informatiche. Si parla tanto delle autostrade dell'informazione: questi ragazzi sanno guidare benissimo, però devono ancora imparare a rispettare le regole del codice della strada, che sono poste a salvaguardia della sicurezza di tutti.

In America sono state istituite le «teste di cuoio» telematiche. Anche in Italia mi sembra che si stia facendo qualcosa in questa direzione.

La novità è che il Servizio centrale operativo della Polizia di Stato viene praticamente diviso in due sezioni, la prima continua a occuparsi di criminalità economica, la seconda si occuperà solo di criminalità informatica e telefonica e avrà presso ogni ogni regione un compartimento di polizia appositamente dedicato, quindi qualificato. Il problema più urgente adesso è formare il personale e dotarlo di mezzi e strutture adeguate. Si deve andare verso una specializzazione sempre più spinta e credo che tutte le indagini sulla criminalità informatica dovrebbero essere concentrate nello SCO e nei compartimenti di Polizia postale, come sta avvenendo dappertutto in Europa. Un altro problema è che nelle recenti operazioni abbiamo sperimentato delle attrezzature molto sofisticate, che però forse sono già obsolete. Queste attrezzature non dovremmo acquistarle, dovremmo averle sempre nella disponibilità delle forze di Polizia e praticamente rinnovarle quasi ogni sei mesi. Perché la sfida della criminalità informatica, di cui ha parlato Clinton in questi giorni (e io condivido totalmente la sua visione) è questa: bisogna che le istituzioni giudiziarie e di polizia siano una spanna più in alto rispetto ai delinquenti. Qui siamo nella situazione in cui i delinquenti informatici hanno apparati di tutto rispetto e paragonabili a delle Ferrari, mentre ai nostri poliziotti anziché le Cinquecento stiamo incominciando a fornire macchine di media cilindrata. Fino a ora si è data la priorità alla repressione del traffico di droga e delle associazioni mafiose, ed è stata una scelta strategica inevitabile. Il problema è che proprio queste organizzazioni si stanno dotando di attrezzature, di mezzi, e stanno cominciando a investire in questi settori, soprattutto nella duplicazione del software e nel traffico di supporti audiovisivi contraffatti. Ovviamente hanno sempre più necessità di scambiare informazioni, di diffondere informazioni false e anche di trafficare in informazioni riservate che hanno un valore economico. Forse ci sono già dei fenomeni di killeraggio informatico, cioè di atti illeciti eseguiti su commissione, e probabilmente parte dei nostri «associati» svolgeva anche attività di questo genere. Occorrono quindi sia norme procedurali che ci consentano di intervenire con la necessaria tempestività, sia attrezzature allo stato dell'arte. Le «teste di cuoio» non è detto che debbano intervenire fisicamente, perché ci sono «agenti elettronici», già sperimentati, in grado di ricostruire in tempo reale i tracciati delle connessioni e cose del genere.

Senza una politica di questo tipo non possiamo pretendere di ottenere risultati significativi nella lotta al crimine informatico.