Autore: Raoul Chiesa - *Agosto 1999*

“Legalita’ “ e “non legalita’ ”

PARTE PRIMA:

LEGALITA’

Se questo inizio può lasciar perplessi, la spiegazione che segue - alquanto curiosa - non aiuterà certo ad avere un’immediata e chiara visione dell’accaduto.
Alla fine del 1998 una macchina ospitata (in hosting) presso la mia azienda è stata oggetto di attacchi e violazioni, unitamente ad alterazioni del contenuto delle sue pagine web.
Questa “moda” di modificare le home page dei siti, importanti o completamente sconosciuti, è un’usanza recente nel vasto panorama di stili e modi di fare dell’ “hacking”.

Le singolari conseguenze di tale fatto sono state molteplici:

io, ex-hacker ed oggi security manager, sono stato bucato da un altro hacker.
l’ex-hacker era divertito e contento della cosa.
l’attuale legislazione italiana non solo punisce chi entra abusivamente in un sistema “protetto” ma anche chi non denuncia gli attacchi subiti.

Il risultato, ***estremamente curioso*** , è che un imprenditore per nulla arrabbiato, anzi desideroso di conoscere l’hacker e la tecnica utilizzata, si trova costretto a fare ciò che non vuole fare: sporgere denuncia.

Ho così scoperto ed “apprezzato” - in chiaro senso ironico - la lentezza della burocrazia italiana e la scarsa competenza delle autorità addette. L’unica alternativa che avevo era quella di informarmi da solo sulle normative, sulle leggi e sulle loro interpretazioni da parte dei GIP (giudice per le indagini preliminari) e dei PM (pubblico ministero).

Quella che segue è una serie di riflessioni personali. Non intendo fare la parte dell’esperto legale perchè non sono né un avvocato, né un giurista. Esprimo semplicemente il mio parere, avendo avuto la duplice possibilità di riconoscermi nelle parti dell’hacker e dell’azienda chiamate in causa e di venire così a conoscenza del “modus-operandi” italiano.

I: “Vorrei non sporgere... ma devo”.

Il fatto che io abbia deciso di occuparmi professionalmente di sicurezza informatica ha come chiara conseguenza l’esistenza di un’attività commerciale. Avere una società comporta il rispetto di una serie di normative e di vincoli, che possono essere sia fiscali che legali e, in entrambi i casi, ricadere sul civile o sul penale.
La violazione effettuata dall’hacking in oggetto ha coinvolto diverse aziende, e nello specifico i siti di alcuni nostri Clienti.
Questo fatto ha generato tutta una serie di considerazioni:

La prima è che una Società che è stata violata ha l’obbligo di denunciare l’accaduto al fine di salvaguardare i propri diritti.

La seconda è che i Clienti della Società violata sono stati lesi, con il rischio di perderci sia dal punto di vista economico che di immagine.

Risultato è che se l’amministratore di una Società non denuncia un episodio di alterazione o modifica del proprio sistema informativo, incorre in sanzioni penali; allo stesso modo, omettendo la denuncia, l’amministratore è colpevole di non aver protetto sufficientemente i propri sistemi informativi.
Il motivo di questo controsenso lo si può estrapolare dall’interpretazione della legge 675/97 sulla privacy, all’articolo 15 che obbliga chi tratta dati personali ad adottare dei criteri minimi di protezione. Questi criteri minimi attualmente esistono a livello di bozza e si attende la loro pubblicazione per luglio o settembre. I criteri di ispirazione però sono già noti: i “Common Criteria” che non sono altro che la fusione della normativa “ITSEC” europea e degli “Orange Books” statunitensi.
Nel momento in cui scrivo so che si svolgerà un incontro dei G8 verso luglio con l’obiettivo di approvare questi nuovi criteri. Nel frattempo però in Italia è stata definita una ISO sull’argomento che entrerà in vigore entro la fine di quest’anno.
Nel caso in cui un sistema non protetto viene violato esiste attualmente l’ipotesi di reato penale con una pena detentiva che va fino a due anni se non vi è stato “nocumento” per terzi (quindi se non vi è il danneggiamento di terze parti) e sino a 3 anni se invece qualcuno ne paga le conseguenze (utilizzo di dati “rubati” per danneggiamento a terzi, o utilizzo del sistema violato come base di partenza o “ponte” per attacchi verso altri sistemi informativi). Chi viene perseguito penalmente perché ha la responsabilità giuridica dei dati è quindi in

primo luogo ***l'amministratore*** della società e, in secondo luogo e solo se e' presente, il ***responsabile della sicurezza.*** In conclusione quindi, la famigerata legge sulla privacy tratta decisamente a fondo i sistemi informativi e la sicurezza informatica!

Per tornare al caso in questione, non denunciando un episodio di hacking, ci troviamo di fronte a due eventualità ben diverse:

1) Il sistema non era protetto a sufficienza (o non lo era affatto, come spesso accade) e l'azienda nemmeno si è accorta di essere stata "bucata";

2) L'azienda si è accorta dell'intrusione ma omette di sporgere denuncia: in questo caso si diventa automaticamente complici e si pagano le conseguenze delle azioni di hacking effettuate dalla propria macchina.

II: "Sporgo"

Naturale conseguenza di tutto quanto detto sopra è chiaramente lo sporgere denuncia. La Polizia Italiana ha iniziato e, credo, terminato, la creazione e l'addestramento di una nuova sezione specifica per i crimini informatici. Questa divisione, amichevolmente chiamata "Escopost" è nata dall' "unione" del "Servizio Polizia Postale e delle Telecomunicazioni" (Polizia delle Telecomunicazioni) e il "Nucleo Operativo di Polizia delle Telecomunicazioni" (N.O.P.T. - nato nel luglio del 1996 nell'ambito dell'Ispettorato di Pubblica Sicurezza presso il Ministero delle Comunicazioni).

Escopost, a differenza delle sezioni precedenti, ha una sede in ogni principale capoluogo italiano (in totale sono 19 Compartimenti e 76 Sezioni) e condivide gli uffici con le stazioni di Polizia Postale .

Essendo a conoscenza di questa divisione, ho pensato di telefonare direttamente alla Escopost della mia città, per non perdere tempo e non fare perdere tempo, evitando di contattare i normali commissariati di polizia.
Purtroppo, mi aspettavo un'immediata competenza ed invece ho dovuto spiegare ad un paio di persone cos'era un'"hacking ai nostri server web" prima di essere dirottato sull'interno giusto... Preso l'appuntamento, mi recavo giorni dopo presso gli uffici Escopost accompagnato dal nostro sistemista.

Durante il colloquio telefonico con gli ispettori, si era convenuto di effettuare una copia fisica (un mirror) dell'hard disk dove risiedevano i log di sistema e le copie delle pagine HTML modificate. "Si era convenuto" significa che o si faceva così, o si dava l'hard disk originale (fermando i siti di alcune decine di Clienti) oppure ancora si stampavano e firmavano tonnellate cartacee di log file e stampe video.

Naturalmente il costo dell'hard disk da 6.4 GB è stato a carico nostro e non sappiamo se ci verrà mai restituito.

La stesura della denuncia ha avuto dei risvolti decisamente comici, spesso dovuti alla non conoscenza dei termini informatici, tecnici o in lingua inglese. C'è poi anche stata una dilatazione nei tempi per me stremante, dovuta alla capacità mia e di ogni informatico di digitare velocemente contrapposta alla lentezza di battitura del rappresentante delle Forze dell'Ordine (pensateci...è snervante).

III: "Attendo"

Dopo lo svolgimento di questa allegra e fremente deposizione non rimaneva null'altro da fare che attendere.

Attendere che la Escopost richiedesse sia ad Interbusiness (gestore delle linee dati implicate) che TIN (gestore della rete di accesso utilizzata) i log di connessione, le corrispondenze con User ID's e clienti effettivi, i riscontri di orari e date Interbusiness e TIN. L'assurdità sta anche nell'aver fatto due richieste a due aziende entrambe di proprietà di un unico "padrone"(Telecom Italia), per un controllo incrociato...

Attendere che "il consulente" analizzasse l'hard disk da noi "spontaneamente" dato.

Attendere che si nominasse un GIP e che lo stesso desse disposizioni.

Nel frattempo però il mio "ego hacker" (così chiamato per distinguerlo da quello che opera nella veste di imprenditore) era rispuntato: analizzavo le copie in nostro possesso dei log di sistema, giravo sulle chat, ircavo (irco da quasi 10 anni, ogni tanto mi chiedo quando smetterò..) e cercavo di capire.
Sono convinto che in Rete esistano una moltitudine di regole non dette, di abitudini e modi di fare, così come delle "etichette" non scritte. Questa mia personale convinzione mi porta ad interpretare il chattare ed Irc come una validissima fonte di pareri, idee, informazioni.
Dopo alcuni giorni di pensieri, confronti ed "indagini" (spinte da semplice curiosità ed ammirazione), avevo individuato la zona da dove sicuramente il mio "amico" aveva chiamato e probabilmente chi era.

IV: GIP

L'Escopost ci richiama per "chiarimenti". Ritorniamo. Il GIP che ha esaminato la denuncia vuole delle precisazioni e le dichiarazioni da parte delle varie persone implicate: questo significa riferire le stesse cose della volta precedente... in modo un po' più frettoloso. Apprendo che i miei Clienti, chiamati in causa come parti lese, dovranno subire questa procedura: ripetere e confermare quello che abbiamo già detto.

FINE PRIMA PARTE

PARTE SECONDA

ILLEGALITA': L'OPERAZIONE ICE-TRAP

Ice Trap fu chiamata così a causa di un "newbie" , tale Ice Mc, un ragazzino siciliano che avrebbe fatto meglio a non toccare mai un modem in vita sua e che entrò nel sistema informatico di una multinazionale (tra le holding della quale figurava anche, oltre ai principali marchi conosciuti dal mass-market, la più importante fabbrica italiana di gelati.... anche da qui il nome dato all'operazione). Io ero già entrato in quel sistema ed aveva una caratteristica particolare: era connesso sia alla rete X.25 italiana (Itapac) che a quella americana (SprintNet). Io entravo dagli Usa ed evitavo problemi di tracciamento, Ice entrava da Itapac: fu tracciato, identificato e la sua utenza telefonica fu messa sotto controllo. Questo avveniva nei primi mesi del 1995 o forse prima. Io continuavo ad essere presente su quei sistemi, vedevo Ice Mc commettere errori ma non feci nulla. E' necessario spiegare che, normalmente, quando un hacker entra in un sistema lo protegge, lo "fa suo" per evitare che altri hacker entrino, o causino allarmi tentando di entrare, oppure facciano danni per incapacità, segnalando quindi la loro presenza ai responsabili della sicurezza.
I sistemi interni alla rete della multinazionale nei quali giravamo, sia io che Ice Mc, non erano protetti ed il proteggerli avrebbe significato vietarne l'accesso anche agli utenti regolari. Quindi non li protessi per impedire l'accesso ad Ice Mc e mi feci i fatti miei. Nel frattempo, monitorando l'utenza di Ice Mc, la S.C.O. ***(Sezione Centrale Operativa Polizia di Stato per Crimini Informatici ed Economici)*** **scoprì che esistevano gli hackers italiani.**

Questo accadde perché Ice Mc si sentiva con un amico siciliano (il quale ebbe anni dopo ruoli organizzativi nel primo Hack.it meeting del '98 a Firenze , il quale, a sua volta, si sentiva con un altro di Roma... quello di Roma telefonava a me e io ero in contatto con un altro ancora... così piano piano ci identificarono tutti.
Le "sviste" da parte nostra furono sicuramente il parlare in chiaro dai cellulari, il passare le nottate a fare hacking e discutere al telefono (via box , carta o clonazioni) sempre tra di noi: un gruppetto di 3-4 persone, abbastanza pazze, che adoravano le reti, i sistemi mainframe, scoprivano Internet (...o meglio la sua prima diffusione in Italia tramite i centri di ricerca, le università e le multinazionali), vedevano nascere il W3 , iniziavano a capire il browsing con Mosaic e scorrazzavano tutta la notte sui vari sistemi informatici.
Parallelamente alla prima ondata di intercettazioni in Sicilia ci fu una serie di episodi di hacking "di alto livello" perpetrati da alcuni di noi verso istituzioni federali, compagnie telefoniche, banche, centri di controllo logico e strategico, in vari Paesi del mondo e da vari Paesi del mondo, su svariati tipi di reti. Da parte nostra non c'era nessuna intenzione "malevola", era soltanto la classica "sfida" che spinge ogni hacker a fare quello che fa.

Io e Nexus6 "bucammo" la GTE ed entrammo in tutta la loro rete. Avevamo accesso ai sistemi di controllo dell'utenza telefonica urbana, cellulare, satellitare, dati (X.25 e Internet), carte telefoniche, pager (cerca persone), numeri riservati, PBX ...qualunque cosa. Dopo molti mesi avvertimmo la GTE degli attacchi effettuati e dei bug presenti e chiedemmo, molto ingenuamente, se avevano bisogno di un aiuto. I "signori" della GTE cercarono in tutti i modi di avere i nostri dati, ci invitarono persino a Miami per un colloquio, con viaggio aereo e soggiorno pagato. Meno male che c'è sempre un sesto senso..... Mesi dopo, in seguito all'arresto e a tutti gli enormi problemi che ne seguirono, scoprii che la GTE era pronta, unitamente all'FBI, ad attenderci all'aeroporto con mandati di arresto e richieste di estradizione internazionale già pronti. Grazie a loro posso "vantarmi" di aver ricevuto una richiesta di estradizione verso gli States, per mia enorme fortuna rifiutata dal Governo Italiano.

Dopo questo episodio successe che:
- l'FBI si mise a cercare un tale "nobody" (mio nickname all'epoca), di nazionalità sconosciuta, per una serie di hacking fatti su varie reti americane;
- l'FBI diramò il comunicato tramite Interpol alle Polizie informatiche mondiali;
- la Francia, tramite i propri Servizi segreti (!) denunciò attacchi a sistemi sulla rete Transpac provenienti da Israele e ...si vociferava di un certo "nobody";
- Israele abbastanza risentita, negò ogni accusa e, anzi, accusò la Francia di procedere con attacchi verso i suoi sistemi informatici;
- la Criminalpol ricevette i dispacci delle varie Polizie europee e dell'Interpol, collegò "nobody" a Raoul, ed ecco che iniziò tutta la vicenda.

Ma la goccia finale fu l'hacking a Bankitalia....entrammo e poi lasciammo un avvertimento dicendo a Bankitalia che i loro sistemi non erano sicuri. Oltre a Bankitalia furono violati circa 50 sistemi appartenenti alle più svariate realtà industriali e commerciali: la cosa fece arrabbiare molte persone. Ma non ***riflettere....***

Per complicare ancora di più la cosa, agli hackers implicati nell'inchiesta e nell'operazione, furono associati personaggi "strani"....per farvi meglio comprendere, cito uno stralcio dell'intervista fatta da Felice Marra :

"...F: Mi pare di ricordare che, nell'inchiesta, voi siate stati accomunati con gente che nulla aveva a che fare con l'hackeraggio ma, piuttosto, con la delinquenza comune...
Te lo chiedo perché quando si parla di operazione Ice-Trap si parla di clonazione di cellulari ad esempio. Voi avevate qualche cosa a che fare con queste operazioni?

R: Credo sia necessaria una spiegazione: quando si fa hacking è normale non pagare le telefonate, le connessioni ecc. e questo lo si fa, non per commettere un reato, ma per non essere rintracciati. L'esigenza di non lasciare tracce si traduce - per forza di cose - nell'utilizzo non autorizzato di varie risorse, e questo di per sé è un reato. Dopo l'Operazione Ice Trap fu chiaro che nel giro si era insinuato qualcuno che le carte telefoniche internazionali, piuttosto che i numeri seriali per clonare i telefoni Tacs o altro, le aveva reperite ed usate.

F: E chi era questo "qualcuno"?

R: Delinquenti, come li definisco io, che gravitavano - e tutt'ora gravitano - attorno al mondo dell'hacking, spesso conquistando la fiducia dei più ingenui o dei piu' stupidi.

F: In quanti foste arrestati?

R: Nell'inchiesta Ice Trap ci furono 7 arresti ma, solo 3 erano gli "hacker" veri.

F: E gli altri, chi erano?

R: Gli altri erano un'accozzaglia di tipi loschi: svizzeri, danesi, extracomunitari e italiani, che nulla avevano a che fare con l'hacking, se non perché avevano utilizzato le loro conoscenze nel mondo degli hackers a scopo di lucro..."

Questa, in breve, è la storia dell'Operazione Ice Trap.

FINE SECONDA PARTE

PARTE TERZA

ILLEGALITA': "Imputato ai sensi degli articoli…"

I capi d'accusa sono riportati in originale, così come presenti nella richiesta di rinvio a giudizio presentata dal Giudice per le Indagini Preliminari e dai due Pubblici Ministeri della Procura della Repubblica di Roma, il 12 luglio 1996.

1) "del delitto di cui all'art. 416 c.p.; per essersi associati tra loro allo scopo di commettere più delitti contro il patrimonio e la persona, mediante frodi telematiche e intrusioni illecite in reti e sistemi informativi pubblici e privati. In Roma, denuncie del febbraio 1995 e date successive in Milano, Venezia, Torino e altrove, fino alla data odierna". ***(12 dicembre 1996, N.d.A.)***

Premesso che, come ho spiegato nella seconda parte di questo articolo, le persone con le quali "mi sono associato allo scopo di commettere più delitti contro il patrimonio e la persona" nemmeno le conosco, in questa accusa si commette un grossolano errore: si confondono le intrusioni nei sistemi informativi - intesi come atti di hacking o "frode informatica /telematica" - con l'inserimento su reti di telecomunicazioni telefoniche in seguito a clonazioni di apparecchiature radiomobili e cellulari. Ora, risulta ovvio che se uso un cellulare il segnale emesso viaggia sulla rete telefonica, sia essa radiomobile o cellulare; è altrettanto ovvio che se clono un cellulare il concetto non cambia, paga semplicemente un altro, ma io continuo ad essere sempre sulla stessa rete telefonica. Nel mio caso non c'è stata intrusione illecita ma clonazione, che nulla ha a che fare con l'hacking.

2) "del delitto di cui agli artt. 110. 81 cpv, 617 quater, comma 4, n. 1 C.P.; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso, fraudolentemente intercettando comunicazioni relative a sistemi informatici o intercorrenti tra più sistemi, acquisivano codici attinenti a carte di credito di circuiti Sprintnet, Global Italia, Global Communication International Phone Card, AT&T, Visa International e Master Card".

Il reato di "associazione a delinquere... in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso" è stato inserito in ogni singolo capo d'accusa.

La Global Italia e la Global Communication non sono mai state violate o intercettate e non è stato utilizzato alcun tipo di sistema informatico per ottenere le carte di credito telefoniche emesse da queste Società. Ogni carta di credito nasce da un algoritmo matematico. Quello delle Global era estremamente semplice e l'enorme tecnologia utilizzata per ottenere tale algoritmo consisté nell'acquistare in una tabaccheria quattro carte Global, sequenziali, analizzare i quattro numeri di carta di credito e con una normalissima calcolatrice ottenere l'algoritmo. Mi sembra di trovarmi di fronte ad un sistema non protetto dal proprietario....ma chiaramente la Global non è stata accusata di nulla.

I numeri delle carte telefoniche Sprint ed AT&T venivano invece fornite dai simpatici operatori americani delle compagnie telefoniche, i quali ricevevano in cambio dei verdi a fruscianti dollari USA. Anche in questo caso non c'è stato nessun atto di hacking. Anche in questo caso il sottoscritto non c'entra (non ho mai comprato una carta di credito rubata in vita mia), ma è stato condannato ugualmente.

Le carte Visa e Mastercard hanno una storia più divertente: qui la "tecnologia" menzionata nell'accusa consisteva nel far "trashing", vale a dire in parole più semplici rovistare nei bidoni della spazzatura di fronte a banche o centri commerciali e negozi, al fine di trovare le ricevute dell'acquisto (buttate via dal titolare!), con sopra scritto il numero di carta di credito, l'intestatario e la scadenza. Queste carte venivano poi utilizzate per la creazione di account per servizi a valore aggiunto quali, ad esempio, Bix e Compuserve in USA.
Non sono un avvocato ma non credo che rovistare tra la spazzatura sia reato...

Non dimentichiamo poi che l'articolo 617 quater C.P. recita "….la fraudolenta intercettazione, l'impedimento o l'interruzione di comunicazioni relative a sistemi informatici e telematici…..": fatico ad associare a queste frasi i bidoni della spazzatura e gli algoritmi da bambini dell'asilo...

3) "del delitto di cui agli artt. 110, 81 cpv, 617 quinquies, C.P.; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso, installavano illecitamente apparecchiature atte ad intercettare o interrompere

comunicazioni relative a sistemi informatici o telematici, o intercorrenti tra più sistemi".

L'articolo 617 quinquies del codice di procedura penale, oltre a punire con la ***reclusione da uno a quattro anni*** pone aggravanti in situazioni particolari: se il reato è commesso da un pubblico ufficiale, da un operatore del sistema o da un investigatore privato (reclusione fino a cinque anni).

Penalizzare l'operatore del sistema fa capire che si sta parlando di sistemi informatici. E' quindi ovvio che, nel momento in cui si fa hacking, si installino software, applicazioni ed utility atte a nascondere la nostra presenza nel sistema. Dov'è la confusione ? Nel chiamare "apparecchiature" poche righe di codice di programmazione, nel confondere tools di protezione (divento invisibile per non far risultare la mia presenza nel sistema) con tools per "interrompere comunicazioni"...Se interrompo le comunicazioni (linee dati) di quel sistema, come faccio a rimanere collegato su di esso ?!?

4) "del delitto di cui agli artt. 110 81 cpv, 615 quinquies, C.P.; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso, si trasmettevano comunicazioni e si consegnavano programmi informatici da loro stessi prodotti, allo scopo di interrompere o comunque alterare il normale funzionamento dei sistemi informatici e telematici aggrediti.

Nel mondo degli hacker è prassi scambiare informazioni: password, accessi, indirizzi di rete, conoscenze, programmi ed utility.
Un hacker non "fa qualcosa allo scopo di interrompere o alterare il normale funzionamento dei sistemi informatici e telematici aggrediti"..... Un hacker ***ama*** la macchina che ha violato, la protegge, la rispetta: non interromperebbe mai le connessioni ed i suoi servizi. Inutile dire che non furono interrotte connessioni ai sistemi informatici violati nell'operazione Ice Trap, se non dai proprietari e system manager stessi che - non sapendo che non era affatto necessario - pensarono bene di spegnere i server attaccati...con conseguente interruzione dei servizi e delle comunicazioni, arrecando indubbiamente danno agli utenti del sistema e dei servizi da esso erogati.

5) "del delitto di cui agli artt. 110 81 cpv, 648 comma 1, 61 n.2, C.P.; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso ed al fine di trarne un profitto, ricevevano apparecchiature informatiche, telematiche ed apparecchi telefonici provenienti da delitti di furto consumato in danno di persone rimaste, allo stato, non identificate. Con l'aggravante di aver commesso il reato per consumare il delitto di cui al capo seguente".

I pc e in generale l'hardware che ho utilizzato nel corso degli anni l'ho sempre acquistato o "barattato" in cambio di lavori e consulenze: i delitti in oggetto sono stati commessi da persone a me accomunate nelle fasi processuali ma che in realtà neanche conoscevo. Il reato però l'ho dovuto accettare ugualmente ("obbligo di patteggiamento uguale per tutti, o così o niente"...impose il PM).

6) "del delitto di cui agli artt. 110 81 cpv, 615 ter, C.P.; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso, e dopo aver commesso il reato di cui al capo precedente, si introducevano abusivamente nel sistema della Telecom nel quale permanevano contro la tacita volontà di esclusione dell'Azienda, al fine di effettuare attività di clonazione di apparecchiature telefoniche cellulari".
Fatti denunciati in Roma dal febbraio all'ottobre 1995.

Letta così, l'accusa sembra voler dire che uno o più hacker si sono introdotti nel sistema informatico della Telecom Italia e dallo stesso hanno prelevato informazioni adatte a clonare apparecchiature cellulari.

In realtà quello che è successo si traduce semplicemente nella clonazione di telefoni cellulari e l'utilizzo degli stessi a carico di utenze differenti. Credo vi sia una bella differenza..

7) "del delitto di cui agli artt. 110 81 cpv, 640 ter, comma 2, C.P.; perché in concorso tra loro e nelle circostanze precisate nei singoli capi di imputazione, intervenendo senza diritto su dati, informazioni contenute nei sistemi informatici e telematici di Enti Pubblici procuravano a se medesimi e a terzi ingiusto profitto consistente nell'acquisizione dei dati medesimi nella possibilità di riutilizzare apparecchiature illecitamente attivate, con conseguente danno agli Enti stessi, ravvisabile altresì nella forzata interruzione di attività in quei settori aggrediti".
Fatti denunciati in Roma dal febbraio all'ottobre 1995.

Dalla lettura si deduce che gli hacker sopra accusati, non contenti, utilizzavano i dati contenuti nel sistema informatico Telecom per trarne profitto. In realtà si continua a parlare di extracomunitari che intercettavano numeri seriali di cellulari E-TACS al fine di clonarli e rivendere le telefonate a loro connazionali. Non riesco ad immaginarmi a vendere telefonate in Africa ad extracomunitari...

8) "del delitto di cui agli artt. 110 81 cpv, 615 quater C.P. in relazione all'art. 617, quater, comma 4, n.2; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso, al fine di procurare a se stessi profitto economico e di arrecare danno a terzi, si procuravano, si comunicavano e consegnavano codici, parole chiave ed altri mezzi idonei all'accesso in sistemi informatici e telematici protetti da misure di sicurezza, e facenti capo al Consiglio Nazionale delle Ricerche, all'Ente Nazionale di Energia Alternativa, alle Università di Venezia e di Siena".

"Sistema informatico" e "sistema telematico"....questa è una grande assurdità ripetuta in molti capi d'imputazione. Un sistema informatico diventa telematico nel momento stesso in cui viene connesso in rete ma rimane chiaramente un sistema informatico. Non sono due entità distinte, separate logicamente e fisicamente l'una dall'altra... la telematica è un'implementazione al sistema informatico, che in questo modo può "parlare" con altri sistemi e utenti remoti.

9) “del delitto di cui agli artt. 110 81 cpv, 615 ter, C.P.; perché in concorso tra loro e con più azioni esecutive del medesimo disegno criminoso, si introducevano abusivamente nei sistemi informatici, protetti da misure di sicurezza, facenti capo alle società Unilever, Sprintnet della Sprint International Corporation, Comm 2000”. Fatti denunciati in Roma dal febbraio all’ottobre 1995.

I punti 9 e 10 illustrano gli unici reati dei quali mi sento colpevole: ***hacking*** . Ho fatto hacking ma ne ho pagato le conseguenze perché sono stato arrestato e processato. Ma sono stato obbligato a pagare anche per reati da me non commessi e questo lo reputo grave, molto grave...

10) “del delitto di cui all’art. 615 ter, comma 3 C.P.; perché abusivamente si introducevano nel sistema informativo della Banca d’Italia, protetto da misure di sicurezza, e vi si mantenevano contro la volontà tacita dell’Istituto...” Roma, nel giugno 1995.

Quest’ultimo commento racchiude in sé la principale carenza delle normative giuridiche italiane contro i crimini informatici - l’interpretazione delle accuse, dei fatti accaduti, delle sequenze di hacking e del ***modus operandi*** dell’hacker - unita ad una sfacciata ignoranza per tutto ciò che riguarda informatica, telematica, sicurezza dei dati.

Si è voluto prendere l’esempio dell’hacking a Bankitalia perché è quello che meglio rappresenta le molteplici variabili che possono esistere in un episodio di hacking e che meglio fa comprendere le tante inesattezze ed errori di procedura commessi.

L’hacking a Bankitalia

Raoul Chiesa, io, accusato e condannato in base ai sopra citati articoli del codice di procedura penale; uno di questi recita: "accusato di aver violato un sistema informatico protetto".

Se un sistema informatico è protetto da misure di sicurezza:
1) non ci entro
2) se è protetto con dovute barriere ed io ci sono entrato, allora sono colpevole, perché quelle barriere mi hanno avvertito di trovarmi di fronte a un sistema informatico il cui accesso è vietato se non autorizzati.

Il sistema violato in ***bankitalia.it*** e per il quale sono stato condannato (insieme ad altri sistemi) era un IBM Aix 3.2 con sistema Unix.

Se ci sono entrato:
1) non era protetto
2) non c’è stata nessuna barriera, avvertimento, divieto se non la richiesta di login/password .

Mi si potrebbe dire: “ecco, sei stato condannato perché hai utilizzato login/password abusive.” Ipotizziamo che ci fosse una login ROSSI con la password ROSSI. Io credo che sarei stato colpevole se avessi indovinato una password del tipo “RGEw76zX|” perché mi sarei impegnato moltissimo e quindi avrei avuto l’intenzione di violare quel sistema.

Questa era però un’ipotesi... in realtà io non ho mai immesso login o password... non ce ne è stato bisogno perché c’era un bug .

Fate molta attenzione a quanto segue.
la IBM, casa produttrice del sistema adoperato in Bankitalia, sbagliò la procedura di login sugli UNIX IBM AIX versione 3.0 e 3.2.

Dando il comando ***"rlogin -f root"*** da un'altra macchina Unix connessa ad Internet gli Unix IBM AIX versione 3.0 e 3.2 sbagliavano **perché non chiedevano la password!** Quello che succedeva dopo aver digitato il comando era ritrovarsi root (quindi super-utente con privilegi massimi sulla macchina) senza aver toccato alcun tasto, senza aver lanciato alcun programma, senza aver indovinato alcuna password....senza nulla di nulla!

La IBM annunciò il suo bug ovunque così come le maggiori organizzazioni di sicurezza, profit e non profit. Il bug stesso era vecchio e quindi molto conosciuto, specie per gli “addetti al settore” (sistemisti, responsabili sicurezza, consulenti dell’I.T).
La IBM distribuiva gratuitamente i patch per questi sistemi operativi.
La funzione del system manager è quella di informarsi (è pagato per questo) ed applicare i patch . Inoltre, enti come Bankitalia (così come tanti altri) hanno contratti con IBM, Digital, ecc. ...come mai nessuno dei consulenti esterni di queste multinazionali effettuò il patch di quel bug?

Riassumiamo dunque i fatti:

Mi accusano, denunciano e condannano per aver fatto hacking.

Mi sequestrano e vietano la restituzione di un hard disk con due 2 anni della mia vita (hacking, lettere, appunti, ricordi, software...) perché su quell'hard disk c’è "il corpo del reato", ovvero la descrizione del bug in questione.

Questo bug e' pubblicato ovunque su Internet. Non l'ho rubato alla IBM ma l’ho scaricato dal CERT (Computer Emergency Reponse Team).

Migliaia di siti internet riportano quel bug.

Bankitalia mi chiede i danni (!) economici.

Devo pagare le spese processuali in quanto sono stato obbligato dai PM a patteggiare e a non andare in discussione processuale con relativo dibattimento (pagando di tasca mia consulenti e periti incapaci !).

.....Pensate ancora che la colpa sia tutta degli hackers ?

FINE
