

anche se quella persona è davvero colpevole. La MPAA che mette fuori uso il computer di qualcuno perché ha il sospetto che stia copiando un film, commette un'azione sbagliata, anche nel caso il film sia stato effettivamente copiato. La vendetta è un sentimento basilare dell'animo umano, ma essa può diventare giustizia soltanto se è portata avanti dallo Stato.

Lo Stato ha sempre più motivi per essere imparziale. La RIAA ha inviato una lettera di sospensione ad un Internet provider richiedendo la rimozione di certi file che rappresentavano opere di George Harrison coperte da copyright. Uno dei file era "Portrait of Mrs. Harrison Williams 1943.jpg [Ritratto della signora Harrison Williams 1943]". La RIAA ha semplicemente cercato con Google la stringa "Harrison" ed ha iniziato a procedere contro chiunque compariva nei risultati della ricerca. Il vigilantismo è sbagliato perché il vigilante può avere torto. L'obiettivo di un sistema giuridico di Stato è la giustizia, l'obiettivo della RIAA era l'opportunismo.

I metodi di risposta agli attacchi funzionano praticamente nello stesso modo. Il concetto è questo: se un computer ci sta attaccando (inviandoci virus, agendo come zombie DDoS, ecc.) dovrebbe essere possibile renderlo forzatamente inattivo, oppure installargli una patch da remoto. Certo, una bella idea, in teoria, ma un'idea che si rivela essere legalmente e moralmente sbagliata.

Pensate di essere il proprietario di una casa, e il vostro vicino possiede un qualche aggeggio, collocato fuori da casa sua, che produce forti rumori, che fa parecchio baccano giorno e notte, a livelli che qualsiasi persona assennata lo definirebbe disturbo della quiete pubblica. Anche se fosse, non è legale da parte vostra occuparvi della faccenda e porre fine ai rumori di vostra iniziativa.

Distuggere la proprietà privata non è certo un rimedio accettato per mettere termine a una qualsiasi seccatura, anche se questa è fonte di reale disturbo nei vostri confronti. Quello che potete fare è: 1) chiamare la polizia e chiedere loro di far smettere i rumori, o di obbligare il vicino a farli smettere, oppure 2) denunciare il vicino, chiedere alla corte di intimargli di non usare quell'aggeggio finché non sia debitamente riparato o revisionato, e chiedere che vi siano riconosciuti i danni procurati da questo inconveniente. Il farsi giustizia da soli non è idea da tenere in considerazione, in nessun caso, non importa quanto si crede di aver ragione.

Qui si parla di legge, non di tecnologia, per cui la questione presenta tutta una serie di sfumature. Gli interessi in gioco nell'attacco originario, il tipo di proprietà, la libertà o la sicurezza personale compromesse dal contrattacco, il rischio di essere dalla parte del torto, e la disponibilità e l'efficacia di altre contromisure sono tutti fattori che servono per valutare che qualcosa sia moralmente o legalmente giusto oppure no. La legge proposta dalla RIAA è all'estremo, poiché il copyright è un interesse di proprietà limitata, e si corre il rischio di limitare illecitamente l'utilizzo del computer e di limitare la privacy e la sicurezza dell'utente. Un contrattacco che disabiliti un pericoloso worm che gira in Internet è un atto decisamente meno estremo. Ovviamente questo è qualcosa che dovrà essere stabilito da una corte.

Tornando indietro al 1789, la Dichiarazione dei Diritti dell'Uomo e del Cittadino sosteneva che "Nessun uomo può essere accusato, arrestato o detenuto se non nei casi determinati dalla Legge, e secondo le forme da essa prescritte. Quelli che procurano, spediscono, eseguono o fanno eseguire degli ordini arbitrari, devono essere puniti". E poi: "Presumendosi innocente ogni uomo sino a quando non sia stato dichiarato colpevole, se si ritiene indispensabile arrestarlo, ogni rigore non necessario per assicurarsi della sua persona deve essere severamente represso dalla Legge".

Non si dovrebbe permettere che gli interessi dei vari amministratori di sistemi su Internet, o gli interessi di compagnie come la Disney, abbiano la meglio su questi diritti.

Sulle "forze dell'ordine elettroniche":

<<http://www.foxnews.com/story/0,2933,64688,00.html>>

La promessa del neo-costituito Dipartimento per la Sicurezza Nazionale è quella di aumentare la sicurezza del nostro paese nei confronti del terrorismo. Purtroppo i risultati avranno, con ogni probabilità, un esito del tutto opposto. Centralizzare le responsabilità inerenti la sicurezza presenta l'inconveniente di rendere la nostra sicurezza ancor più fragile, grazie alla creazione di una comunanza di approcci e di un'uniformità di pensiero. A meno che il nuovo dipartimento non distribuisca la responsabilità e contemporaneamente centralizzi il coordinamento, esso non aumenterà la sicurezza del nostro paese. La sicurezza ha due evidenti verità, assai utili per questa discussione:

1) Le decisioni riguardanti la sicurezza devono essere prese il più vicino possibile al problema. Questo presenta diverse implicazioni: la protezione di potenziali bersagli terroristici dovrebbe essere compito di persone che abbiano competenza in merito a tali bersagli; le decisioni in merito al piazzamento di ordigni esplosivi dovrebbero essere prese dagli ufficiali stanziati nel territorio di guerra, non da Washington; le indagini federali dovrebbero essere approvate dal distretto dell'FBI più vicino al caso da investigare. Questo modo di procedere può dar luogo ad abusi, perciò è indispensabile che vi sia una supervisione competente. Ma è anche un metodo più solido, ed è il modo migliore perché la sicurezza funzioni.

2) L'analisi sulla sicurezza deve avvenire il più lontano possibile dalle fonti. Operare nell'intelligence significa anche saper trovare informazioni di un certo rilievo in mezzo a moltitudini di dati irrilevanti, per poi organizzare tutte quelle informazioni disparate in previsioni coerenti di ciò che potrebbe accadere in seguito. Sono necessarie persone in gamba che riescano a percepire le varie connessioni e che abbiano accesso alle informazioni attraverso svariate agenzie governative. Non può essere un campo limitato solo a specifiche entità come FBI, CIA, NSA o il nuovo Dipartimento per la Sicurezza Nazionale. Il disegno generale è molto più grande di ogni singola agenzia, e ognuna ha accesso solo ad una parte di questo disegno.

Ciò che consegue a queste due verità è che la sicurezza funzionerà meglio se è coordinata centralmente ma implementata in una modalità distribuita. Siamo maggiormente sicuri se ogni agenzia governativa implementa la propria sicurezza all'interno del proprio dipartimento, con differenti punti deboli e punti di forza. La nostra sicurezza diventa più robusta se più dipartimenti vengono a sovrapporsi l'un l'altro. A questo scopo è buona cosa che le istituzioni meglio fondate ed equipaggiate per difendere il nostro paese dal terrorismo (FBI, CIA, le organizzazioni militari di controspionaggio) non facciano parte di questo nuovo dipartimento.

Ma è importante che tutte queste organizzazioni comunichino fra loro, ed è questo il valore primario di un Dipartimento di Sicurezza Nazionale. Un'organizzazione dovrà essere l'unico centro di coordinamento ed analisi delle minacce e delle risposte terroristiche. Un'altra avrà il compito di occuparsi del "disegno generale", prendere decisioni e impostare regole di condotta in base ad esso.

Il corpo umano si difende mediante sistemi di sicurezza sovrapposti. Esso possiede un complesso sistema immunitario per combattere specificatamente una malattia, ma questa battaglia contro la malattia viene distribuita attraverso i vari organi e le varie cellule. Il nostro corpo possiede ogni genere di sistemi di sicurezza, a partire dalla pelle, che tiene alla larga elementi nocivi all'organismo, al fegato, che depura il sangue da certe sostanze pericolose, fino alle difese presenti nell'apparato digerente. Tutti questi sistemi e apparati svolgono i propri compiti in maniera diversa. Inoltre questi sistemi si intrecciano l'un l'altro e, entro certi limiti, possono venirsi in aiuto nel caso uno di essi non funzioni a dovere. Potrebbe sembrare ridondante e inefficiente, ma in realtà è un sistema solido, affidabile e sicuro. È grazie ad esso che siete vivi e state leggendo questo testo.

La metafora biologica è molto appropriata. È difficile difendersi dal terrorismo, perché esso sovverte le nostre istituzioni e pone le nostre libertà e possibilità contro di noi. Invade la nostra società, la avvelena e si diffonde al suo interno, e poi la attacca. È difficile da combattere, nello stesso modo in cui è difficile combattere il cancro. Se ci vogliamo difendere efficacemente dal

Windows. Non importa che strutturalmente sia o non sia sicuro: non vedo perché dovrei scegliere il bersaglio più noto.

Il libro di Kevin Mitnick, "The Art of Deception", è un'ottima lettura. Il primo capitolo, mancante perché tolto all'ultimo momento dall'editore, riguarda Internet. Esso narra la vita di Mitnick in qualità di hacker e fuggiasco, parla del suo arresto e del conseguente processo. È davvero molto interessante.

<<http://www.wired.com/news/culture/0,1284,56187,00.html>>
<<http://littlegreenguy.fateback.com/chapter1/Chapter%201%20-%20Banned%20Edition.doc>>

È stata crackcata la chiave a curva ellittica da 109 bit. Ho cercato di reperire stime di complessità in merito a questo crack. La migliore che ho trovato parla di "una grande quantità di potenza di calcolo che ha impegnato diecimila computer (PC per la maggior parte) 24 ore su 24 per 549 giorni". I sistemi attualmente operativi utilizzano chiavi a curva ellittica da 163 o più bit, per cui non lasciatevi allarmare da questo risultato.

<http://www.certicom.com/about/pr/02/021106_ecc_winner.html>

Sembra che le tastiere HP senza fili non abbiano alcuna autenticazione incorporata. Questo aneddoto racconta della tastiera di un utente usata per inviare ordini al computer di un altro utente, a 150 metri di distanza e oltrepassando varie mura.

<<http://www.aftenposten.no/english/local/article.jhtml?articleID=427668>>

Il NIST e la NSA hanno pubblicato i Common Criteria Protection Profiles (profili di protezione secondo i Common Criteria) per quanto concerne sistemi operativi, firewall, sistemi di rilevamento anti-intrusione, infrastrutture basate su token e chiavi pubbliche.

<http://www.gcn.com/vol1_no1/daily-updates/20373-1.html>

La legge della California richiede ora che le agenzie di commercio e governative segnalino tutti quei cyber-attacchi che possano aver compromesso l'integrità di informazioni confidenziali. Vi è una grande fuga di informazioni che potrebbero ostacolare un'indagine in corso, per cui non mi aspetto grossi cambiamenti.

<http://www.businessweek.com/technology/content/nov2002/tc20021111_2402.htm>

Storie di sabotaggi informatici:

<<http://www.techtv.com/cybercrime/viceonline/story/0,23008,3386967,00.html>>

Un articolo interessante su come sbagliare ad impostare la sicurezza sin dall'inizio: non capire a quale genere di problema un sistema di sicurezza dovrebbe far fronte. Dopo l'11 settembre, Ashcroft ha iniziato a far rispettare una regola che impone a chiunque non abbia la cittadinanza americana di notificare ogni cambio di residenza al governo federale. Negli uffici governativi sono pervenute schede di cambi di residenza nell'ordine di centinaia di migliaia. Non ci sono addetti del personale che inseriscano questi dati in un computer, e questi moduli giacciono archiviati in parecchie scatole. Ma anche se qualcuno inserisse i dati, che cosa cambierebbe? In che misura tutto questo risolverà i problemi legati alla sicurezza? Forse che un terrorista invierà una scheda quando cambierà residenza? Non credo proprio.

<http://www.ilw.com/lawyers/colum_article/articles/2002,1023-latour.shtm>

Abuso del DMCA. Wal-Mart ed altri commercianti al dettaglio stanno usando il DMCA per impedire che siti web dedicati ai consumatori pubblichino informazioni sui loro prezzi di vendita. Questo flagrante abuso del DMCA è un'ulteriore prova di quanto cattiva possa essere una legge.

<<http://www.nytimes.com/2002/11/21/technology/21COPY.html>>

<<http://www.theregister.co.uk/content/6/28223.html>>

<<http://www.wired.com/news/business/0,1367,56504,00.html>>

<<http://www.fatwallet.com/forums/messageview.cfm?catid=18&threadid=126042>>

pie di altezza in direzione del Nevada. Poi, da qualche parte sopra la zona a sudovest di Washington, abbassò le scale posteriori dell'aereo e si paracadutò. Non fu mai catturato, e ancora l'FBI non sa chi sia e se sia ancora vivo.

Questo tipo di attacco era nuovo. Era un modo di ragionare fuori dagli schemi. L'attacco sfruttava una vulnerabilità delle maglie del sistema di sicurezza: si spendono molte energie per rendere sicuri gli accessi ai voli e le uscite a terra, ma non si fa altrettanto in aria. (Si noti poi l'astuzia nella richiesta dei 4 paracadute. L'FBI fu così costretta a presumere che Dan Cooper potesse obbligare alcuni ostaggi a paracadutarsi insieme a lui, e non si poté rischiare di fornirgli dei paracadute finti). Cooper "barò" e sparì.

La sua impresa ha ispirato molti altri imitatori. Infatti, simili tentativi furono così numerosi che sui Boeing è stato installato un congegno chiamato Cooper Vane, che impedisce alle scale posteriori dell'aereo di aprirsi in volo.

N.B. Un ufficiale di polizia chiamò per sbaglio il dirottatore "D.B. Cooper": tale nome rimase, e diede origine ad un film e a una ballata.

** *** *****

Il crimine, ovvero la prossima grande novità di Internet

Credo che la prossima grande "tendenza" in fatto di sicurezza in Internet sarà il crimine. Non il genere di crimine un po' scialbo e fonte di qualche minima seccatura che abbiamo potuto vedere in questi anni. Non i virus, i trojan e gli attacchi DDoS, fatti a scopo ludico o per puro vanto. Nemmeno le epidemie che scuotono Internet nel giro di qualche ora e che causano milioni di dollari di danni. Parliamo di crimine, quello vero. Su Internet.

Il crimine in Internet non è una novità. Abbiamo tutti sentito di episodi isolati in cui due concorrenti violano le rispettive reti, o di hacker che penetrano nei network ed estorcono denaro a confusi amministratori di sistemi, o di spionaggio industriale, furto di identità, furto di numeri di carte di credito, rapine ai danni di banche e di altre istituzioni finanziarie. Però sono i vari Nimda e i vari attacchi root-name server che fanno notizia. Mentre ci stiamo a preoccupare di quelle minacce, i criminali agiscono indisturbati. Continuano a rubare denaro e altre cose che possono vendere in cambio di denaro. Continuano a rubare numeri di carte di credito e informazioni private per commettere frodi. Continuano a portare avanti lo spionaggio industriale. I criminali non cambiano, sono le tattiche ad essere nuove.

Prevedo che le persone inizieranno ad accorgersene. Le aziende hanno forti interessi a non divulgare i veri criminali che vengono commessi ai danni delle loro reti. La cattiva pubblicità che scaturisce dal rendere pubblico un attacco, spesso è più dannosa dell'attacco stesso. Ma i tempi stanno cambiando. Proprio quest'anno in California è passata una legge che -- pur con grosse scappatoie -- richiede alle aziende di rendere noti questi attacchi. Prevedo che saranno approvate altre simili leggi in futuro.

I criminali tendono a rimanere indietro rispetto alle tecnologie nell'ordine di 5-10 anni, ma alla fine imparano. Proprio come Willie Sutton, che rapinava le banche perché "è lì che ci sono i soldi", i criminali moderni attaccheranno le reti. Il valore si trova sempre più on-line che non in un caveau; modificare illegalmente un numero all'interno del database di una banca può essere molto più redditizio che non entrare in una banca brandendo un'arma da fuoco.

È difficile rilevare i veri criminali. Quando la vostra rete viene esaminata decine di volte al giorno dai vari script kiddies, l'unico vero criminale potrebbe penetrare senza venire scoperto. Presso Counterpane monitoriamo centinaia di reti contro eventuali attacchi. Il nostro compito più difficile, quel che ci assorbe la maggior parte del tempo, è identificare i veri criminali in mezzo

alle centinaia di hacker. Può essere un impiegato della stessa azienda che cerca di cambiare il proprio stipendio nel computer delle risorse umane. Può essere un gruppo di ladri che cercano di manipolare i conteggi del computer di una banca. Questo è il vero crimine nella rete, e quando riusciamo a catturare questa gente, i nostri clienti sono estasiati. Sempre più di frequente questo sarà l'ambito in cui le aziende investiranno il proprio denaro per salvaguardare la sicurezza informatica.

** *** ***** ***** ***** ***** ***** ***** ***** *****

Commenti dei lettori

Da: Anonimo

Oggetto: Sistemi di controllo incorporati - Crypto-Gram del 15 luglio 2002

Una prima stesura di questa mail è rimasta per mesi nel mio programma di posta. Dato che non ho notato simili commenti nei numeri successivi di Crypto-Gram, le mando ora il mio contributo.

Per quanto concerne le sue osservazioni sui sistemi di controllo incorporati, sono d'accordo che minacce quali ordigni esplosivi, germi, uragani e terremoti siano più frequenti degli hacker, ma questi sistemi presentano in ogni caso diverse problematiche di sicurezza.

Alcune osservazioni basate sull'esperienza personale (coordino la parte informatica di alcuni sistemi di gestione energetica per la ditta in cui lavoro):

- Questi sistemi stanno via via abbandonando le connessioni dirette a favore di comunicazioni basate su TCP/IP, dato che le istituzioni possono avvantaggiarsi di un'infrastruttura di rete già esistente invece di spendere un mucchio di soldi per creare e mantenere connessioni dirette dedicate. Se da una parte (si spera) verrà utilizzata una rete ad accesso ristretto per le varie apparecchiature, è altresì probabile che verrà creato un gateway verso Internet in modo che gli utenti (sia il personale addetto alla manutenzione, sia gli installatori) possano controllare le apparecchiature in remoto.

- Gli utilizzatori di questi sistemi stanno abbandonando i sistemi proprietari in favore di protocolli aperti quali LonMark (ovvero LonWorks, EcheLon), BACnet, ModBus over IP, ecc. Scordiamoci la sicurezza attraverso l'incomprensibilità.

- Chi ha progettato questi protocolli conosce bene i propri sistemi (allarmi antincendio, sistemi di riscaldamento/raffreddamento, misurazioni elettriche, ecc.) ma non ne sa molto di sicurezza di reti o di reti informatiche in generale. (Ricordo il sistema BACnet di un rivenditore che obbligava gli utenti stessi ad impostare la rete per creare i loro indirizzi MAC). L'unica sicurezza che possono implementare è un nome utente e password in chiaro.

- Stanno diffondendosi sempre più le interfacce basate su web (Java). Le istituzioni preferiscono questo approccio perché in questo modo si può accedere ai sistemi da qualsiasi computer dotato di browser web, invece che da un computer particolare dotato di software proprietario.

- Per le solite ragioni, quei sistemi progettati per avvantaggiarsi delle funzionalità di Internet Explorer sono molto diffusi. Basta immaginare di poter analizzare un problema dall'ufficio accanto invece di scendere nei sotterranei 50 piani più sotto, o di avere un impiantista che rimedia ad un problema direttamente dal suo ufficio invece di fare un sopralluogo a 100 dollari o più all'ora, e si potrà comprendere l'attrattiva di questo approccio. Naturalmente questo

significa che chiunque può avere accesso a tali sistemi. Un hacker non ha nemmeno bisogno di conoscere i protocolli, gli basta sapere il giusto sito web e la relativa password.

- Questi sistemi potrebbero utilizzare server web proprietari o poco noti, che non hanno lo stesso livello di collaudo e di verifica che hanno, per esempio, Apache o IIS.

- Spesso questi sistemi possiedono scarse strutture di accesso, o non le possiedono affatto, per cui diventa impossibile stabilire chi ha effettuato un accesso e quando, e che cosa ha tentato di fare.

- Le persone che utilizzano e curano questi sistemi giorno per giorno non ne sanno molto di informatica. Chi effettua regolari controlli sui computer, chi installa service pack o delle patch, chi esamina i resoconti, ecc.?

- La mia esperienza con alcuni impiantisti è che costoro sono abituati ad implementare questi sistemi su ogni tipo di connessione di rete su cui riescono a metter mano, e installano il software in un computer utilizzato dal personale addetto alla manutenzione. Sospetto che esistano molte istituzioni in cui il dipartimento di IT non è nemmeno al corrente dell'esistenza di tali sistemi sulle proprie reti.

- Allo stesso modo, gli impiantisti solitamente mandano qualcuno esperto in un determinato campo (climatizzatori, serrature elettroniche, allarmi antincendio) ma che sa poco o nulla riguardo all'impostazione o alla manutenzione di una macchina Windows NT o Linux.

- Spesso il personale addetto alla manutenzione prende decisioni in merito agli acquisti senza consultarsi con lo staff IT.

- Le richieste o i reclami presentati ai rivenditori in merito alla sicurezza dei loro sistemi o sono scomparse giù nel buco nero di "se ne occuperanno gli sviluppatori", o hanno generato risposte evasive da parte del personale addetto alle vendite.

- A questo si aggiunga il solito pressapochismo di utenti che scrivono le proprie password sulla scrivania, o che le condividono, o che utilizzano password semplici da indovinare, oppure rivenditori che si servono di una sola password per tutti i sistemi dei loro clienti, oppure password predefinite che non vengono mai modificate...

E questa è solo la punta dell'iceberg.

Da: "Christian Gruber" <cgruber@infotriever.com>

Oggetto: La strategia nazionale per rendere sicuro il Cyberspazio

Questa mia vuole essere una risposta ad una lettera comparsa sul numero di novembre di Crypto-Gram. In essa un lettore affermava che la protezione dei beni comuni sarebbe stata più efficace spartendo questi beni e suddividendoli in proprietà privata, così da "tenerli puliti" perché appunto sarebbero proprietà privata, e quindi si sarebbe incentivati a farlo, ma con un ammonimento: "la parte difficile è distribuire i beni comuni in 'pezzi' omogenei di proprietà, per assicurare che il maggior numero di persone possa ancora utilizzarli ad un prezzo equo".

Vi sono tre errori in questo assunto.

Il primo consiste nell'assunzione secondo cui le persone mantengono pulito e accessibile quel che è di loro proprietà. Io non strappo quasi mai le erbacce nel mio prato. Mia moglie è preda di attacchi allergici quando uso i pesticidi, e io non sono abbastanza tipo da aria aperta per prendermene cura personalmente. Siccome è mio, non mi metto ad estirpare i denti di leone. Lo faccio solamente quando ricevo sottili o aperte pressioni da parte dei vicini. Francamente

qui si tratta di pressioni esterne, che non hanno a che vedere con il possesso di proprietà. Si tratta dei miei vicini che difendono il bene comune rappresentato dalla bellezza del vicinato, combinato con il bene comune rappresentato dall'aria che condividiamo attraverso la quale volano i semi dei soffioni. Il mio pezzo di proprietà "privata" in se stesso non offre alcun incentivo o pressione per mantenerlo pulito, né da parte mia ho alcun incentivo per permettere che altri entrino nel mio prato, specialmente se devono lamentarsi per le erbacce. Per cui suddividere i "beni comuni" pare non abbia alcun vantaggio per l'uomo comune, ma è un grosso vantaggio personale, perché mi permette di possedere una proprietà della quale, più o meno, posso disporre a mio piacimento.

In secondo luogo, la frase "le leggi non funzionano" è palesemente ridicola. Se le leggi non funzionano, allora invito il lettore a bere un tè a casa mia il giorno dopo che io ho brutalmente ucciso il suo cane. Così lui affermerà che gli ho "danneggiato la sua proprietà" e si servirà di tutte quelle armi fastidiose di costrizione comunitaria per arrestarmi in base a tale accusa. Come si può vedere, se egli vuole far rispettare i diritti di proprietà secondo la legge, allora è come se affermasse che le leggi funzionano. Ma non le leggi A FAVORE dei beni comuni.

In terzo luogo, egli sta mettendo da una parte il meglio di ciò che è la proprietà privata e un governo minimalista, e dall'altra il peggio del governo del bene pubblico. "I proprietari privati sono tutte persone oneste e buone, che terranno pulite le loro strade" ma "gli sporchi politicanti abituati agli intrighi per ottenere fondi pubblici non aspettano altro che essere corrotti per ignorare le leggi sull'ambiente." L'immagine opposta è data da chi si oppone alla privatizzazione, ecc. "Quelle maledette multinazionali stanno inquinando la terra" e "dobbiamo fare in modo che il nostro papà grande e forte, che è il Governo, legiferi in merito al comportamento morale di queste aziende". Sono entrambi degli estremi che mettono a confronto il lato peggiore di ogni partito con il migliore, a seconda delle preferenze di chi prende la parola. La verità sta molto più nel mezzo.

Il fatto è che sento puzza di pregiudizio e preconcetto. Le leggi funzionano per il nostro amico. Ciò che non funziona per il caro lettore sono quelle leggi che non supportano un ordine del giorno che veda la proprietà privata prevalere sulla pubblica. È una bella posizione da prendere, e anch'io in un certo senso simpatizzo per quelle leggi che fanno rispettare i diritti di proprietà. La presentazione della faccenda da parte di quel lettore, però, ha cercato di far passare una certa retorica unita a un pizzico di partigianeria come fosse un argomento sensato, mentre invece si rivela essere piuttosto contraddittorio e dimostrabilmente falso, seppur facendo uso di aneddoti.

** *** ***** **

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza informatica e sulla crittografia.

La versione italiana è curata da Communication Valley SpA

<http://www.communicationvalley.it/>; per iscriversi o cancellarsi andare all'indirizzo

<http://www.cryptogram.it/>.

I numeri arretrati sono disponibili all'indirizzo <http://www.cryptogram.it/>.

Per informazioni crypto-gram@communicationvalley.it.

Inoltre liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare la rivista interessante. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è il fondatore e CTO di Counterpane Internet Security, Inc., autore di "Secrets and Lies" e di "Applied Cryptography" e inventore degli algoritmi Blowfish, Twofish e Yarrow. È membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

<<http://www.counterpane.com/>>