

CRYPTO-GRAM
15 gennaio 2006

Scritta da Bruce Schneier
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: schneier@counterpane.com

Web: <<http://www.schneier.com>> oppure <<http://www.counterpane.com>>

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

Crypto-Gram in versione originale è anche consultabile in formato RSS:

<<http://www.schneier.com/crypto-gram-rss.xml>>

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:

<<http://www.schneier.com/blog>>.

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

In questo numero:

[Anonimato e responsabilità](#)

[Le aziende di telefonia cellulare e la sicurezza](#)

[Le ristampe di Crypto-Gram](#)

[Un botnet olandese](#)

[Internet Explorer è pessimo](#)

[Note di sicurezza da ogni dove: manette elettroniche e comunicazioni telefoniche](#)

[News](#)

[Statistiche sulle minacce dall'interno \(insider threat\)](#)

[Sono tornati i controlli sull'esportazione di sicurezza informatica?](#)

[Tracciamento dei veicoli nel Regno Unito](#)

[Le News di Counterpane](#)

[Le intercettazioni illegali di Bush e della NSA](#)

[La minaccia per la sicurezza che deriva da un potere presidenziale non controllato](#)

[Il Progetto Shamrock](#)

[Commenti dei lettori](#)

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

Anonimato e responsabilità

In un recente articolo, Kevin Kelly mette in guardia sui pericoli dell'anonimato. Va bene a piccole dosi, egli ammette, ma quando è troppo diventa un problema: "In ogni sistema da me analizzato, dove l'anonimato diviene comune, il sistema finisce

col fallire. La recente macchia sull'onore di Wikipedia è generata dall'estrema facilità con cui dichiarazioni anonime possono essere inserite in uno strumento ad altissima visibilità pubblica. Le comunità infettate dall'anonimato finiscono con il collassare oppure con il mutare l'anonimato in pseudo-anonimato, come su eBay, dove si ha un'identità tracciabile dietro a un nickname inventato".

Ciò che dice Kelly è interessante, ma il discorso che ne scaturisce è malposto. I sistemi anonimi sono intrinsecamente più semplici da abusare e più difficili da proteggere, come illustra il suo esempio di eBay. In un sistema di commercio anonimo, in cui il compratore non conosce il venditore e viceversa, è molto facile per l'uno ingannare l'altro. Questo inganno, anche se coinvolge una ristretta minoranza, farebbe diminuire rapidamente la fiducia nel mercato, ed eBay sarebbe costretta a chiudere bottega. Solo che eBay ha trovato una soluzione brillante al problema: un sistema di feedback che ha aggiunto una "reputazione" agli anonimi nickname degli utenti, e ha reso così i venditori e i compratori responsabili delle proprie azioni.

Ed è proprio a questo punto l'errore di Kelly. Il problema non è l'anonimato, è la responsabilità. Se un tizio non può essere reso responsabile, conoscerne il nome non serve a nulla. Se si ha qualcuno che è totalmente anonimo ma anche pienamente responsabile, allora, cavolo, basta chiamarlo Fred.

La storia è piena di banditi e pirati dalla proverbiale reputazione, eppure nessuno conosce i loro veri nomi.

Il funzionamento del sistema di feedback di eBay non è dovuto all'identità rintracciabile dietro un nickname anonimo, ma al fatto che ogni nickname anonimo è corredato da una cronologia di transazioni precedenti, e se qualcuno inganna qualcun altro, tutti lo sapranno.

Analogamente, i problemi legati alla veridicità di Wikipedia non sono il risultato di autori anonimi che aggiungono falsità alle voci di Wikipedia, ma una proprietà intrinseca di un sistema di informazione dotato di responsabilità distribuita. La gente pensa a Wikipedia come a un'enciclopedia: non lo è. Tutti ci fidiamo dell'esattezza delle voci dell'Enciclopedia Britannica perché conosciamo la reputazione di quella compagnia, e per estensione quella dei suoi autori e curatori. D'altro canto, tutti dovremmo sapere che Wikipedia conterrà giocoforza una piccola quantità di informazioni inesatte o false perché non vi è alcuna persona in particolare a essere responsabile della precisione delle voci. Questo sarebbe comunque vero anche se si potesse passare con il mouse sopra ogni frase e vedere il nome di chi l'ha scritta.

Storicamente la responsabilità è sempre stata legata all'identità, ma non v'è ragione perché ciò debba necessariamente aver luogo. Non serve che il mio nome compaia sulla mia carta di credito. Potrei avere una fototessera anonima che provi che ho un'età sufficiente a consumare alcolici legalmente. Non v'è ragione che il mio indirizzo email sia correlato al mio vero nome.

Ciò è quel che Kelly definisce pseudo-anonimato. In questi sistemi, si affida la propria identità a una terza parte fidata che promette di rispettare la nostra identità entro un certo limite. Per esempio, la mia compagnia di carta di credito mi fornisce un'altra carta di credito sotto un altro nome. È sempre collegata al mio conto, ma mi

permette di rimanere anonimo quando mi rapporto ai commercianti con cui tratto i miei affari.

La sicurezza dello pseudo-anonimato dipende strettamente da quanto fidata è quella "terza parte fidata". A seconda delle leggi locali e da quanto vengono rispettate, lo pseudo-anonimato può essere rotto da grandi aziende, dalla polizia o dal governo. Può essere rotto dalla polizia che raccoglie moltissime informazioni sul vostro conto, o da ChoicePoint che raccoglie miliardi di piccolissime informazioni su chiunque per poi effettuare correlazioni. Lo pseudo-anonimato è solamente un anonimato limitato. È un anonimato che protegge da chi non ha potere, non da chi ce l'ha. Si ricordi che anon.penet.fi non ha potuto tener testa al governo.

In un mondo perfetto non ci sarebbe bisogno dell'anonimato. Non sarebbe necessario per il commercio, dal momento che nessuno vi metterebbe al bando o vi ricatterebbe basandosi sui vostri acquisti. Non sarebbe necessario in Internet, perché nessuno vi ricatterebbe o vi arresterebbe basandosi su chi sono i vostri corrispondenti o su quel che leggete. Né l'anonimato sarebbe necessario per i malati di AIDS, per i membri di frange politiche o per le persone che chiamano centri di assistenza psicologica via telefono. Certo, i criminali sfruttano l'anonimato, proprio come sfruttano qualsiasi altra cosa che la società offre. Ma i benefici dell'anonimato, discussi in modo esaustivo in un eccellente scritto di Gary T. Marx, sono decisamente superiori ai rischi.

Nel mondo di Kelly, un mondo perfetto, una forma limitata di anonimato è sufficiente perché le uniche persone che potrebbero danneggiarvi sono individui che non hanno il potere di conoscere la vostra identità, e non chi ha il potere di farlo.

Non viviamo in un mondo perfetto, ma in una realtà dove le informazioni sulle nostre attività (anche quelle perfettamente legali) possono essere usate contro di noi con facilità. Notizie recenti hanno parlato del caso di uno studente che è stato cacciato dal suo college per aver scritto cose poco piacevoli nel suo blog, di aziende che intentano cause SLAPP contro persone che le criticano, e di persone di cui viene tracciato il profilo sulla base del loro discorso politico.

Viviamo in un mondo in cui la polizia e il governo sono costituiti da individui tutt'altro che perfetti, i quali possono servirsi di informazioni personali altrui, unitamente al proprio enorme potere, in maniera impropria e scorretta. L'anonimato ci protegge tutti dai potenti proprio perché non permette a questi individui di ottenere innanzitutto i nostri dati personali.

Questo articolo è originariamente apparso in Wired:
<<http://www.wired.com/news/columns/0,70000-0.html>>

L'intervento di Kelly:
<http://www.edge.org/q2006/q06_4.html>

Gary T. Marx sull'anonimato:
<<http://web.mit.edu/gtmarx/www/anon.html>>

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

Le aziende di telefonia cellulare e la sicurezza

Si tratta di un'affascinante storia di frode telefonica (cellulare), sicurezza, economia ed esternalità. La morale è scontata, e dimostra come le considerazioni di ordine economico condizionino le decisioni di sicurezza. Dal "The Globe and Mail":

"Susan Drummond era un cliente di Rogers Wireless, una grande azienda di telefonia cellulare canadese. Il suo telefonino è stato clonato mentre si trovava in vacanza, e ha ricevuto una bolletta di 12.237,60 dollari (la sua bolletta normale era di 75 dollari). Rogers continua a sostenere che non vi sia nulla da fare e che Drummond debba pagare".

Come tutte le aziende di telefonia cellulare, Rogers è dotata di sistemi automatici antifrode che rilevano questo tipo di utilizzo anomalo del cellulare. Non disattivano i telefonini, però, perché non vogliono disturbare i clienti.

"Ms. Hopper [un manager del dipartimento sicurezza di Rogers] ha dichiarato che dei gruppi terroristici avevano scelto i funzionari delle maggiori aziende di telefonia cellulare come bersagli perfetti poiché l'azienda era restia a disattivare i loro telefonini per varie ragioni, fra cui le possibili seccature per i dirigenti molto occupati e, ovviamente, il danno a livello di pubbliche relazioni che ne conseguirebbe se la notizia si diffondesse".

Finché Rogers può fare in modo che altri paghino i costi di una frode, tutto questo ha assolutamente senso. Disattivare un telefono basandosi su un sistema automatico antifrode è un costo per l'azienda, in termini di persone infastidite da falsi allarmi e pessima pubblicità. Ma il costo maggiore derivato dal non disattivare un telefono rimane un'esternalità: è il cliente a pagarlo.

Infatti paiono esserci alcune prove secondo cui Rogers decide se disattivare o meno un telefono sospetto basandosi sulla possibilità di pagare del cliente:

"Ms. Innes [un vicepresidente di Rogers Communications] ha dichiarato che Rogers ha una linea di condotta che prevede di contattare i clienti in caso vi sia un sospetto di frode. In alcuni casi, ha ammesso, i telefoni vengono disattivati automaticamente, ma si è rifiutata di spiegare i criteri utilizzati. (Ms. Drummond e Mr. Gefen ritengono che l'azienda basi tale decisione sulla capacità di credito del cliente. 'Se avete il curriculum finanziario giusto, lasciano correre il tassametro', ha detto Ms. Drummond). Ms. Drummond ha fatto notare che il suo salario ammonta a più di 100.000 dollari, e che possiede un ottimo curriculum finanziario. 'Sapevano che qualcosa non quadrava, ma hanno pensato che avrebbero potuto far pagare me. È assurdo'".

Ha senso dal punto di vista di Rogers. I clienti danarosi sono 1) più propensi a pagare e 2) più pericolosi se irritati da un falso allarme. Ancora una volta, le considerazioni di ordine economico vincono sulla sicurezza.

<<http://www.cryptogram.it/cryptogramPdf/Gennaio2005.pdf>> (versione tradotta)

La Guerra Cibernetica

<<http://www.schneier.com/crypto-gram-0501.html#10>>

<<http://www.cryptogram.it/cryptogramPdf/Gennaio2005.pdf>> (versione tradotta)

Dirottare aerei e Servizi Segreti nazionali:

<<http://www.schneier.com/crypto-gram-0401.html#11>>

<<http://www.cryptogram.it/gennaio04.htm#a11>> (versione tradotta)

Prendere le impronte digitali agli stranieri:

<<http://www.schneier.com/crypto-gram-0401.html#3>>

<<http://www.cryptogram.it/gennaio04.htm#a3>> (versione tradotta)

I livelli di minaccia terroristica codificati a colori:

<<http://www.schneier.com/crypto-gram-0401.html#1>>

<<http://www.cryptogram.it/gennaio04.htm#a1>> (versione tradotta)

L'esercito e la Guerra Cibernetica

<<http://www.schneier.com/crypto-gram-0301.html#1>>

<<http://www.cryptogram.it/gennaio03.htm#a1>> (versione tradotta)

Una Underwriters Laboratories in versione cibernetica?

<<http://www.schneier.com/crypto-gram-0101.html#1>>

Code signing:

<<http://www.schneier.com/crypto-gram-0101.html#10>>

Block ciphers e stream ciphers:

<<http://www.schneier.com/crypto-gram-0001.html#BlockandStreamCiphers>>

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

Un botnet olandese

Lo scorso ottobre, la polizia olandese ha arrestato tre individui che avevano creato un grande botnet e lo avevano utilizzato per estorcere denaro ad aziende statunitensi. Quando il trio è stato arrestato, le autorità hanno dichiarato che il botnet era composto da circa 100.000 calcolatori. Il numero effettivo era di 1,5 milioni di computer.

E ho sentito rapporti di fonti affidabili secondo cui il vero numero effettivo era "significativamente più alto".

E potrebbe essere tuttora in crescita. I bot continuano a esplorare la rete nel tentativo di infettare altre macchine. Lo fanno autonomamente, anche dopo che il nodo di comando e controllo è stato disattivato. Dato che sulla maggior parte di quel

milione e mezzo di macchine (o qualunque sia il loro numero) è ancora attivo il software del botnet, è ragionevole ritenere che il botnet stia ancora sviluppandosi.

<<http://informationweek.com/story/showArticle.jhtml?articleID=172303265>>
oppure <<http://tinyurl.com/95s5e>>

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

Internet Explorer è pessimo

Questo studio è di agosto, ma non l'avevo notato. I ricercatori hanno analizzato tre browser (Microsoft Internet Explorer, Firefox, Opera) nel 2004 e hanno contato per quanti giorni i browser erano "riconosciuti non sicuri". La loro definizione di "riconosciuto non sicuro": una vulnerabilità di sicurezza sfruttabile remotamente è stata annunciata pubblicamente e non era ancora disponibile una patch.

Internet Explorer era non sicuro al 98%. Vi sono stati solo 7 giorni nel 2004 senza una falla di sicurezza pubblicamente resa nota e non patchata.

Firefox era non sicuro al 15%. Vi sono stati 56 giorni con una falla di sicurezza pubblicamente resa nota e non patchata. 30 di quei giorni riguardavano una falla di sicurezza sulla piattaforma Mac che interessava solo gli utenti Mac. Firefox su Windows era non sicuro al 7%.

Opera era non sicuro al 17%: 65 giorni. Tale numero è casualmente un poco migliore di quanto dovrebbe essere, in quanto due dei periodi senza patch si sono sovrapposti.

Tutto questo sottovaluta i rischi, perché non tiene conto delle vulnerabilità note agli aggressori e non divulgate pubblicamente (ed è sciocco ritenere che non esista tale eventualità). Pertanto, il valore "98% non sicuro" per Internet Explorer è generoso, e la situazione potrebbe persino essere peggiore.

<<http://bcheck.scanit.be/bcheck/page.php?name=STATS2004>>

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

Note di sicurezza da ogni dove: manette elettroniche e comunicazioni telefoniche

Questo articolo è in ebraico, ma la vicenda di sicurezza è divertente in qualsiasi lingua.

Riguarda un detenuto a cui è stato fatto indossare un bracciale elettronico per controllare che non violasse gli arresti domiciliari. Il funzionamento del bracciale è semplice: se il sospettato abbandona il perimetro di detenzione, il bracciale elettronico manda un segnale alla polizia locale attraverso la linea telefonica.

Come fare per sconfiggere un sistema come questo? Basta smettere di pagare la bolletta del telefono e aspettare che la compagnia telefonica interrompa il servizio.

<<http://www.haaretz.co.il/hasite/pages/ShArt.jhtml?contrassID=1&subContrassID=5&sbSubContrassID=0&itemNo=660328>> oppure <<http://tinyurl.com/bjhth>>

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

News

Due storie che pubblicizzano esageratamente e vergognosamente il crimine informatico:

<<http://www.cnn.com/SPECIALS/2005/online.security/>>

<http://www.usatoday.com/tech/news/internetprivacy/2005-12-14-meth-online-theft_x.htm> oppure <<http://tinyurl.com/a2be8>>

Fate attenzione ai Quattro Cavalieri dell'Apocalisse Informatica: terroristi, spacciatori di droga, sequestratori e pedofili. Pare che si possa spaventare il pubblico in modo che permetta al governo di fare qualsiasi cosa con quei quattro.

Microsoft ha ricevuto una certificazione CC (Common Criteria) EAL 4+ per Windows, dimostrando quanto debole in realtà sia tale certificazione:

<<http://www.eweek.com/article2/0,1895,1901965,00.asp>>

Dopo che gli agenti dell'FBI hanno espresso frustrazione per il fatto che l'Office of Intelligence Policy and Review non stesse approvando i loro ordini sotto la Sezione 215 del Patriot Act, sono stati apportati cambiamenti procedurali in modo da permettere all'FBI di aggirare quell'ufficio.

<http://www.epic.org/foia_notes/note10.html>

Si ricordi che qui la questione non è se l'FBI debba o meno occuparsi di antiterrorismo. Il problema è l'erosione di supervisione giudiziaria, ossia l'unico controllo che abbiamo sul potere delle forze dell'ordine. E questa presa di potere è pericolosa a prescindere da quale partito governi la Casa Bianca al momento.

Nel frattempo, l'esercito degli Stati Uniti sta spiando gli americani. Nello specifico, il Dipartimento della Difesa sta raccogliendo dati, violando la legge americana, su chi protesta contro la guerra in modo legale e pacifico.

<<http://www.msnbc.msn.com/id/10454316/>>

Quasi duecento chili di alto esplosivo rubati da un "bunker" fuori Albuquerque di proprietà di Cherry Engineering. Si noti che non vi erano né guardie né telecamere di sorveglianza:

<<http://www.abcnews.go.com/GMA/story?id=1424214>>

È stato ritrovato:

<http://www.atf.gov/press/fy06press/field/122405pho_atf_new_mexico.htm>

oppure <<http://tinyurl.com/d6qc4>>

Un'interessante intervista con Damien Miller, sviluppatore di OpenSSH:

<<http://www.securityfocus.com/columnists/375>>

Criminali adattabili: con l'avvento di dispositivi di sicurezza per auto sempre più efficaci, è più facile che i ladri penetrino nelle case per rubare le chiavi.

<http://www.themercury.news.com.au/common/story_page/0,5936,17605616^3462,00.html> oppure <<http://tinyurl.com/8ytkp>>

Un articolo idiota sul TPM:

<<http://www.msnbc.msn.com/ID/10441443>>

Il mio commento:

<http://www.schneier.com/blog/archives/2005/12/idiotic_article.html>

Un pedofilo ha ricevuto il worm Sober.Y. Tale worm presenta un messaggio dai toni molto ufficiali per invitare i destinatari ad aprire l'allegato. Egli si è talmente spaventato che ha finito col costituirsi alla polizia.

<http://news.yahoo.com/s/nm/20051220/wr_nm/crime_germany_worm_dc>

La storia dello studente della Università del Massachusetts a Dartmouth che ha dichiarato di aver ricevuto una visita da parte di agenti della Sicurezza Nazionale dopo aver richiesto il Libro Rosso di Mao Tse-Tung dalla biblioteca, si tratta di una bufala:

<<http://www.southcoasttoday.com/daily/12-05/12-24-05/a01lo719.htm>>

Non so quale sia la morale qui. 1) Il tizio è un idiota. 2) Non credete a tutto quel che leggete. 3) Viviamo in un clima politico talmente invasivo che è facile credere a storie come questa. 4) Il tizio è davvero un idiota.

Nuove linee guida della TSA da The Onion:

<<http://www.theonion.com/content/node/43716>>

Richard M. Smith ha alcune idee interessanti per verificare se la NSA sta intercettando le vostre email.

<<http://www.computerbytesman.com/privacy/emailsnooping.htm>>

L'unico problema è che potreste ricevere una visita da parte di qualche agenzia investigativa. O essere perquisiti ogni volta che cercate di imbarcarvi su un aereo. Ma penso che in effetti un tal rischio sia piuttosto ridotto. Se qualcuno è intenzionato a seguire le idee di Smith per davvero, faccia sapere. Sono molto incuriosito.

Un ottimo scritto sui "cacciatori di bug" (bug bounty) e sul perché non siano un sostituto dell'auditing di sicurezza:

<<http://www.pebbleandavalanche.com/weblog/2005/12/19/blog-20051219T0454>>

oppure <<http://tinyurl.com/896bh>>

Ciò non significa che i cacciatori di bug non siano una buona idea: sono infatti un'ottima aggiunta a un rigoroso sviluppo e collaudo del software.

Vespe che rilevano ordigni esplosivi possono essere la soluzione più efficace e meno costosa rispetto ad altre alternative:

<http://www.usatoday.com/tech/news/2005-12-26-wasps-terrorism_x.htm>

Anche le api:

<<http://www.defensetech.org/archives/001754.html>>

Ecco come realizzare un portafoglio blocca-RFID con del nastro isolante:

<<http://www.rpi-polymath.com/ducttape/RFIDWallet.php>>

Il Dipartimento di Giustizia degli Stati Uniti non è migliore di altri nella protezione della privacy del singolo:

<<http://www.informationweek.com/news/showArticle.jhtml?articleID=175400150>>

oppure <<http://tinyurl.com/exs27>>

Un buon intervento sugli effetti di sicurezza imprevisi di documenti d'identità inefficaci:

<http://www.theregister.co.uk/2005/12/28/lords_voluntary_id_register_plan>

oppure <<http://tinyurl.com/7nvz4>>

La "Top Ten 2005" delle storie sulla privacy secondo EPIC, e la "Top Ten" delle problematiche da considerare nel 2006. Una lettura decisamente consigliata.

<http://www.epic.org/alert/EPIC_Alert_yir2005.html>

Il Dipartimento del Tesoro stima che il crimine cibernetico abbia realizzato 105 miliardi di dollari nel 2004, ben di più rispetto al traffico di droga. La domanda è sempre: come hanno fatto a calcolare quella cifra? Se scarico un CD musicale da Internet, ciò equivale a 15 dollari di crimine cibernetico? Se il calcolo viene fatto così, non credete a quel totale.

<http://money.cnn.com/2005/12/29/technology/computer_security/index.htm>

oppure <<http://tinyurl.com/aaskv>>

Un dispositivo palmare che disabilita i chip RFID passivi:

<[https://events.ccc.de/congress/2005/wiki/RFID-Zapper\(EN\)](https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN))>

Un affascinante esperimento di data mining utilizzando le wish list di Amazon:

<<http://www.applefritter.com/node/view/10074>>

Ora, immaginate i falsi allarmi e gli abusi che è possibile innescare se si possiedono molti più dati e molti più computer per analizzarli e combinarli. Naturalmente vi sono applicazioni dove questo genere di data mining ha ragion d'essere. Ma fra di esse non vi è certo quella di scovare terroristi. Si tratta di un problema di aghi in un pagliaio, e accumulare altra paglia non è di grande aiuto.

Nel Wisconsin le macchine per il voto elettronico devono produrre schede cartacee e funzionare mediante un software open source.

<<http://wistechnology.com/article.php?id=2585>>

I miei interventi precedenti sul voto elettronico:

<<http://www.schneier.com/essay-068.html>>

<<http://www.schneier.com/crypto-gram-0312.html#9>>

<<http://www.schneier.com/crypto-gram-0012.html#1>>

Un passeggero di un aereo ha scritto le parole "dinamitardo suicida" nel suo taccuino ed è stato arrestato.

<http://news.yahoo.com/s/nm/20060105/od_uk_nm/oukoe_uk_life_passenger>

<http://www.mercurynews.com/mld/mercurynews/news/local/states/california/the_valley/13551154.htm> oppure <<http://tinyurl.com/b2yu7>>

Qui il mio commento:

<http://www.schneier.com/blog/archives/2006/01/stupid_band_nam.html>

Chiunque può ottenere i registri delle telefonate di chiunque:

<<http://www.suntimes.com/output/news/cst-nws-privacy05.html>>

<http://www.concurringopinions.com/archives/2006/01/cell_phone_reco_1.html>

<http://www.boingboing.net/2006/01/08/online_service_claim.html>

<http://west.epic.org/archives/2006/01/pretexting_isnt.html>

Pare che si ottenga questo mediante una tecnica chiamata "pretexting", ovvero telefonare alla compagnia telefonica e mentire sulla propria identità. A me suona tanto di frode.

Molestare le persone in forma anonima via Internet è contro la legge americana:

<http://news.com.com/Create+an+e-annoyance%2C+go+to+jail/2010-1028_3-6022491.html> oppure <<http://tinyurl.com/a2kqp>>

Si veda il commento di un procuratore, che sostiene come ciò fosse vero in precedenza:

<http://www.boingboing.net/2006/01/09/flame_someone_anonym.html>

Che senso ha per la nostra società, quando vengono passate leggi evidentemente stupide come questa, e si deve sperare che le forze dell'ordine siano sufficientemente cortesi da non farle rispettare?

Controlli di sicurezza per chi viaggia nello spazio, compreso lo screening fisico e il confronto delle persone con una watch list:

<<http://www.cnn.com/2006/TECH/space/01/04/space.travel.reut>>

<<http://news.bbc.co.uk/1/hi/sci/tech/4589072.stm>>

"I residenti di un quartiere alla moda di Londra saranno in primi in Gran Bretagna a ricevere 'Asbo TV', un canale proiettato direttamente nelle loro case da telecamere a circuito chiuso situate nelle strade circostanti".

<<http://www.timesonline.co.uk/article/0,,2087-1974974,00.html>>

Una storia interessante che tratta di credenziali falsificate e sicurezza:

<http://www.schneier.com/blog/archives/2006/01/forged_credenti.html>

REAL ID si sta rivelando essere molto più costoso del previsto.

<http://news.yahoo.com/s/ap/20060112/ap_on_re_us/real_id>

Si ricordi che la sicurezza è un compromesso. REAL ID è una pessima idea in primo luogo perché la sicurezza acquisita non vale l'enorme spesa del progetto.

La ACLU ha un nuovo sito su REAL ID:

<<http://www.realnighmare.org/>>

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

Statistiche sulle minacce dall'interno (insider threat)

Interessanti statistiche provenienti dall'Europa (dubito che negli Stati Uniti la situazione sia molto diversa).

- * Un impiegato su cinque (21%) permette alla famiglia e agli amici di accedere a Internet attraverso computer (portatili e non) dell'azienda.
- * Più della metà (51%) connettono i propri dispositivi e/o gingilli al computer aziendale.
- * Un quarto di questi lo fa ogni giorno.
- * Circa il 60% ammette di archiviare contenuti personali nel proprio PC aziendale.
- * Un impiegato su dieci ha confessato di aver scaricato del materiale al lavoro, contravvenendo alle regole aziendali.
- * Due terzi (62%) hanno ammesso di avere conoscenze molto scarse di sicurezza informatica.
- * Più della metà (51%) non ha idea di come aggiornare la protezione antivirus sul proprio PC.
- * Il cinque per cento sostiene di essere entrato in aree del loro sistema informatico a cui non avrebbe dovuto accedere.

Un'avvertenza: lo studio proviene da McAfee, che ha un interesse acquisito nel gonfiare questo genere di minaccia.

Mi piacciono i loro "quattro tipi di impiegato che mettono a rischio il loro ambiente di lavoro": il "Security Softie" [i "cuori teneri" che mettono a rischio la sicurezza lasciando che amici e familiari utilizzino i computer aziendali], il "Gadget Geek", lo "Squatter" [l'occupante abusivo] e il "Saboteur" [sabotatore].

<http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/>
oppure <<http://tinyurl.com/8rjz5>>

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

Sono tornati i controlli sull'esportazione di sicurezza informatica?

Pensavo che la questione legata alle norme di esportazione USA fosse risolta e definitivamente chiusa, almeno per quanto riguarda il software. Allora perché Symantec invia la seguente comunicazione ai clienti stranieri?

"Purtroppo, a causa di severe norme di esportazione emanate dal Governo degli Stati Uniti, Symantec è in grado di provvedere a nuovi ordini per LC5 o di offrire supporto tecnico soltanto a utenti finali situati negli Stati Uniti e ad entità commerciali in Canada, a patto che tutti i controlli di sicurezza abbiano esito positivo.

"Merci, tecnologia o software sono soggetti al controllo del Dept. of

Commerce, Bureau of Industry and Security USA se esportati o trasferiti in forma elettronica al di fuori degli Stati Uniti d'America. Merci, tecnologia o software sono soggetti a controllo sotto lo ECCN 5A002.c.1, cryptanalytic.

"È possibile ottenere ulteriori informazioni sul nostro sito Web all'indirizzo:
<http://www.symantec.com/region/reg_eu/techsupp/enterprise/index.html>"

Il software in questione è lo strumento di password breaking e auditing chiamato LC5, meglio noto come L0phtCrack. A me sembra che stiano semplicemente ferdandone lo sviluppo, usando il governo come scusa.

<http://www.theregister.co.uk/2005/11/25/symantec_l0phtcrack_export_controversy/> oppure <<http://tinyurl.com/89vto>>
<<http://it.slashdot.org/article.pl?sid=05/12/22/1548209>>

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

Tracciamento dei veicoli nel Regno Unito

La sorveglianza automobilistica globale non è lontana. Secondo l'"Independent":

"La Gran Bretagna sta per diventare il primo paese del mondo in cui gli spostamenti di tutti i veicoli sulle strade saranno registrati. Un nuovo sistema di sorveglianza nazionale conserverà le registrazioni per almeno due anni.

"Mediante una rete di telecamere che possono automaticamente leggere le targhe dei mezzi in transito, il progetto è quello di realizzare un enorme database degli spostamenti dei veicoli, in modo che la polizia e i servizi di sicurezza possano analizzare qualsiasi viaggio che una persona ha compiuto negli ultimi anni.

"La rete incorporerà migliaia di telecamere a circuito chiuso già esistenti che verranno dotate di un sistema per leggere in automatico le targhe automobilistiche, notte e giorno, in modo da offrire una copertura 24 ore su 24, 7 giorni su 7 di tutte le autostrade e le strade principali, compresi paesi, città, porti e stazioni di servizio.

"Dal prossimo marzo, un database centrale installato a fianco del Police National Computer a Hendon (nord di Londra), archiverà i dettagli di 35 milioni di "letture" quotidiane di targhe automobilistiche. I dettagli comprenderanno ora, data e posizione precisa, e i luoghi ove saranno disposte le telecamere saranno monitorati da un sistema satellitare globale di posizionamento (GPS)".

In un altro articolo, l'"Independent" ritiene che questo sia solo l'inizio:

"La nuova rete di sorveglianza nazionale per tracciare gli spostamenti automobilistici, il cui sviluppo ha impiegato più di 25 anni, è soltanto l'inizio di una serie di piani per controllare i movimenti di tutti i cittadini inglesi. Lo Home Office Scientific Development Branch nello Hertfordshire è già al lavoro su sistemi per far riconoscere automaticamente a un computer i volti umani, progetto che in molti vedranno come

l'introduzione di una sorveglianza stradale di tipo orwelliano, dove ogni nostra mossa viene registrata e archiviata da macchine.

"Malgrado i problemi del riconoscimento facciale computerizzato siano più difficili da affrontare rispetto alla lettura di targhe automobilistiche, gli esperti ritengono sia solo questione di tempo prima che le macchine possano individuare in maniera affidabile un volto all'interno di una folla in movimento.

"Se la polizia e i servizi di sicurezza potranno dimostrare che un'operazione di sorveglianza nazionale basata sulla registrazione di spostamenti automobilistici può effettivamente proteggere le persone contro la minaccia di criminali e terroristi, vi sarà una forte volontà politica di applicare lo stesso sistema alle telecamere presenti in città per controllare gli spostamenti delle persone".

Ho già parlato dei rischi di sicurezza di quella che io chiamo "sorveglianza all'ingrosso". Una volta che tutte queste informazioni vengono raccolte, saranno abusate, utilizzate in modi impropri, perse e rubate. Saranno piene di errori. I problemi e le insicurezze che derivano dal vivere in una società di sorveglianza superano di gran lunga qualsiasi vantaggio nella lotta contro il crimine o il terrorismo.

<<http://news.independent.co.uk/uk/transport/article334686.ece>>

<http://news.independent.co.uk/world/science_technology/article334684.ece>

I miei precedenti interventi sulla sorveglianza all'ingrosso:

<<http://www.schneier.com/essay-061.html>>

<<http://www.schneier.com/essay-057.html>>

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

Le News di Counterpane

Counterpane ha annunciato una partnership con Verano per estendere il monitoraggio a sistemi di controllo in tempo reale:

<<http://www.counterpane.com/pr-20060109.html>>

Schneier interverrà alla RSA Conference in San Jose (14-26 febbraio). Parlerà in merito all'"Economia della Sicurezza" il 14 febbraio alle ore 16:30, e sul tema "Perché la Sicurezza ha così poco a che fare con la Sicurezza" il 15 febbraio alle ore 14:00. Parteciperà a una tavola rotonda di primo piano sui documenti d'identità il 16 febbraio alle ore 8:00.

<<http://2006.rsaconference.com/us/>>

Gartner ha nominato Counterpane "leading visionary company" (maggior azienda visionaria e lungimirante) nel suo rapporto del dicembre 2005, Managed Security Services Provider Magic Quadrant.

<<http://www.counterpane.com/pr-20060113.html>>

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

Le intercettazioni illegali di Bush e della NSA

(Nota: ho scritto questo articolo nei giorni immediatamente successivi allo scandalo).

Quando il presidente Bush ha ordinato alla National Security Agency (NSA) di effettuare intercettazioni segrete ai danni dei cittadini americani, ha trasferito al Dipartimento della Difesa un'autorità che rientrava precedentemente fra le competenze del Dipartimento di Giustizia e ha aggirato proprio quelle leggi che dovrebbero proteggere gli americani dalle intercettazioni governative su vasta scala. La ragione può essere stata quella di mettere alla prova le capacità di data mining e di sorveglianza estesa della NSA.

Questo genere di spionaggio illegale ai danni dei cittadini americani non è una novità: negli anni Cinquanta e Sessanta, attraverso un programma chiamato "Progetto Shamrock", la NSA intercettò ogni singolo telegramma da e verso gli Stati Uniti. Tali intercettazioni furono condotte senza un mandato e per conto della CIA e di altre agenzie. Molto di tutto questo divenne di dominio pubblico durante le udienze del Church Committee nel 1975 e risultò nell'ora ben noto Foreign Intelligence Surveillance Act (FISA) del 1978.

Lo scopo di questa legge era di proteggere gli americani regolamentando le intercettazioni governative. Come molte leggi che limitano i poteri del governo, si affida a controlli ed equilibri: una sezione del governo ne controlla un'altra. La legge stabilì un tribunale segreto, il Foreign Intelligence Surveillance Court (FISC), conferendo ad esso il potere di approvare mandati per intercettazioni legate alla sicurezza nazionale. Il Dipartimento di Giustizia può richiedere mandati FISA per monitorare comunicazioni straniere così come comunicazioni fra cittadini americani, a patto che soddisfino alcuni criteri minimi.

Il FISC ha emanato circa 500 mandati FISA all'anno dal 1979 al 1995, e il numero è andato lentamente aumentando fino a oggi: nel 2004 sono stati emessi 1.758 mandati. Il procedimento è pensato per funzionare velocemente e comporta persino alcune disposizioni per cui il Dipartimento di Giustizia può intercettare prima, e chiedere il permesso in seguito. In tutto quell'arco di tempo soltanto quattro richieste di mandato sono state respinte, tutte nel 2003 (non se ne conoscono i dettagli, ovviamente, dato che le procedure del tribunale sono segrete).

È l'FBI che si occupa dei mandati FISA, ma nei giorni immediatamente successivi agli attacchi terroristici a Washington vi era la percezione diffusa che l'FBI non sarebbe stato in grado di gestire queste minacce nuove: non potevano scoprire i complotti in tempi sufficientemente rapidi. E quindi l'amministrazione Bush si è rivolta alla NSA, che aveva gli strumenti, le capacità e l'esperienza, affidandole la missione.

La capacità di ascolto delle comunicazioni da parte della NSA è esemplificata da una tecnologia chiamata Echelon. Echelon è il più grande "aspirapolvere" mondiale di

informazioni, e risucchia un'incredibile quantità di comunicazioni, siano esse voce, fax, dati, via satellite, via microonde, in fibra ottica, cellulari e tutto il resto, da ogni parte del mondo. Si stimano 3 miliardi di comunicazioni al giorno. Queste comunicazioni vengono poi elaborate mediante sofisticate tecnologie di data mining, che ricercano semplici frasi quali "assassinare il presidente", così come pattern di comunicazione più complessi.

Apparentemente Echelon copre soltanto le comunicazioni al di fuori degli Stati Uniti. Anche se non vi sono prove che l'amministrazione Bush abbia impiegato Echelon per monitorare comunicazioni da e verso gli Stati Uniti, questa capacità di sorveglianza è probabilmente proprio quel che serviva al presidente e potrebbe spiegare perché l'amministrazione ha cercato di aggirare il procedimento FISA per l'ottenimento di un mandato.

Forse la NSA non aveva semplicemente alcuna esperienza nel sottoporre mandati FISA, per cui Bush ha unilateralmente tralasciato quel requisito. E forse Bush ha pensato che il FISA non era altro che un ostacolo (nel 2002 vi fu una credenza diffusa, ma erronea, secondo cui il FISC ostacolò le indagini su Zacarias Moussaoui, il presunto "ventesimo dirottatore"), e per questo motivo ha aggirato il tribunale.

Molto probabilmente Bush voleva un modello di sorveglianza completamente nuovo. Possiamo pensare alle capacità dell'FBI nei termini di "sorveglianza al dettaglio": intercettano le comunicazioni di un singolo individuo o apparecchio telefonico. La NSA, invece, conduce "sorveglianza all'ingrosso". Essa, o più esattamente i suoi computer, è in ascolto su qualsiasi cosa. Un esempio potrebbe essere quello di sottoporre ai computer ogni comunicazione vocale, via fax, o email in cerca del nome "Ayman al-Zawahiri". Questo tipo di sorveglianza è più simile ai metodi del Progetto Shamrock, e non è legale secondo il FISA. Come scrisse il Senatore Jay Rockefeller in un memo segreto dopo aver ricevuto il briefing sul programma, essa solleva "profonde problematiche di supervisione".

Inoltre non è chiaro se un tipo di sorveglianza in stile Echelon servirebbe a prevenire attacchi terroristici. Nei mesi precedenti l'11 settembre 2001, Echelon notò parecchio "chiacchiericcio": frammenti di conversazioni che suggerivano un qualche tipo di attacco imminente. Ma dato che la maggior parte della pianificazione dell'attacco dell'11 settembre è avvenuta faccia a faccia, gli analisti non furono in grado di apprenderne i dettagli.

La questione fondamentale qui è la sicurezza, ma non la sicurezza a cui pensa la maggior parte delle persone. Come disse egregiamente James Madison, "Se gli uomini fossero angeli, non sarebbe necessario alcun governo. Se gli angeli dovessero governare gli uomini, non sarebbero necessari controlli sul governo, né internamente né esternamente". Il terrorismo è un grave rischio per il nostro paese, ma una minaccia ancor più grande è la centralizzazione del potere politico americano nelle mani di un'unica sezione del governo.

Più di 200 anni fa, gli artefici della Costituzione Americana realizzarono un ingegnoso meccanismo di sicurezza per evitare un governo tirannico: suddivisero il potere governativo in tre diverse entità. Un sistema di controlli ed equilibri attentamente

studiato nel ramo esecutivo, il ramo legislativo e il ramo giudiziario hanno garantito un'equa ripartizione dei poteri, senza che un ramo diventasse troppo potente.

Dopo aver assistito all'ascesa e al declino delle tirannie in tutta Europa, questo sembrò un modo assai prudente e lungimirante per formare un governo. I tribunali controllano le azioni della polizia. Il Congresso approva leggi che persino il presidente deve rispettare. Dall'11 settembre gli Stati Uniti hanno assistito a un'enorme presa di potere da parte del ramo esecutivo. È ora di ripristinare il sistema di sicurezza che ci ha protetto dal governo per più di 200 anni.

Una versione di questo articolo è originariamente apparsa su Salon:
<<http://www.salon.com/opinion/feature/2005/12/20/surveillance/>>

Il testo del FISA:
<http://www.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36_20_I.html> oppure <<http://tinyurl.com/d7ra4>>

Riepilogo dei mandati FISA annuali:
<http://www.epic.org/privacy/wiretap/stats/fisa_stats.html>

Il memo segreto di Rockefeller:
<<http://talkingpointsmemo.com/docs/rock-cheney1.html>>

Qui un approfondimento:
<http://www.schneier.com/blog/archives/2005/12/nsa_and_bushs_i.html>

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

La minaccia per la sicurezza che deriva da un potere presidenziale non controllato

Lo scorso giovedì [15 dicembre 2005], il "New York Times" ha esposto la violazione più significativa della legge sulla sorveglianza federale dell'era post-Watergate. Il presidente Bush ha segretamente autorizzato la National Security Agency a procedere allo spionaggio interno, spiando migliaia di americani e aggirando le procedure legali che regolamentano questa attività.

Il problema non è tanto lo spionaggio, che è già una questione assai grave di per sé. Si tratta delle protezioni garantite dal Quarto Emendamento contro le ricerche illegali. Si tratta di evitare un piccolissimo controllo da parte del ramo giudiziario, controllo istituito dal ramo legislativo 27 anni fa, ovvero l'ultima volta in cui il ramo esecutivo ha abusato dei suoi poteri così ampiamente.

Nel difendere questo spionaggio segreto ai danni degli americani, Bush ha dichiarato di aver fatto appello ai suoi poteri costituzionali (Articolo 2) e alla deliberazione congiunta (Joint Resolution) passata dal Congresso dopo l'11 settembre che ha portato alla guerra in Iraq. Tale fondamento è stato spiegato nei dettagli in un memo scritto da John Yoo, un procuratore della Casa Bianca, meno di due settimane dopo gli attacchi dell'11 settembre. È una lettura densissima e un pezzo terrificante di

contorsionismo legale, ma afferma in sostanza che il presidente ha poteri illimitati per combattere il terrorismo. Può spiare chiunque, arrestare chiunque, sequestrare e trasferire chiunque in un altro paese... basandosi semplicemente sul sospetto che tale persona possa essere un terrorista. E secondo il memo, questo potere durerà finché non vi sarà più terrorismo nel mondo.

Yoo inizia con l'affermare che la Costituzione dà al presidente pieni poteri in periodo di guerra. Fa inoltre notare come il Congresso sia stato accondiscendente quando il presidente ha intrapreso azioni militari di sua iniziativa, citando l'attacco ordinato da Clinton nel 1998 contro Sudan e Afghanistan.

Poi Yoo dice: "Gli incidenti terroristici dell'11 settembre 2001 sono stati sicuramente una minaccia più grave per la sicurezza nazionale degli Stati Uniti rispetto agli attacchi del 1998. [...] Il potere presidenziale per rispondere militarmente agli attacchi più recenti deve essere quindi proporzionalmente maggiore".

Questo modo di ragionare è davvero nuovo. È come dire che la polizia dovrebbe avere maggiori poteri quando indaga su un omicidio rispetto a un furto.

Tornando al punto, la deliberazione del Congresso del 14 settembre 2001 rifiutò specificatamente il tentativo iniziale da parte della Casa Bianca di ottenere l'autorità di frustrare ogni atto terroristico futuro, e concesse a stento il permesso a Bush di perseguire i responsabili degli attacchi al Pentagono e al World Trade Center.

Il memo di Yoo ha ignorato tutto ciò. Scritto 11 giorni dopo che il Congresso rifiutò di concedere al presidente poteri su vasta scala, ammise che "la Deliberazione Congiunta è in un certo senso più rigorosa rispetto all'autorità costituzionale del presidente", ma sostenne che "il grande potere costituzionale del presidente di servirsi della forza militare [...] permetterebbe al presidente di [intraprendere] qualunque azione ritenga appropriata [...] per neutralizzare o rispondere a minacce terroristiche provenienti da nuove direzioni".

Anche se il Congresso lo vieta specificatamente.

Il risultato è che i poteri del presidente in periodo di guerra, con i suoi eserciti, le battaglie, le vittorie e le dichiarazioni congressuali, ora si estendono alla retorica "Guerra al Terrore": una guerra senza fronti, confini, senza un esercito antagonista e, cosa più inquietante, senza alcuna "vittoria" conoscibile. Indagini, arresti e processi non sono strumenti di guerra. Ma secondo il memo di Yoo, il presidente può definire guerra qualsiasi cosa voglia, e rimanere "in stato di guerra" finché vuole.

Questo è potere dittatoriale indefinito. E non sto usando questo termine con leggerezza: la stessa definizione di dittatura è quella di un sistema che pone un governatore al di sopra della legge. Nelle settimane successive all'11 settembre, mentre l'America e il mondo erano addolorati per la tragedia, Bush ha costruito il fondamento legale per una dittatura. Poi ha iniziato subito a usarlo per sfuggire alla legge.

Questo è il motivo per cui, fondamentalmente, la questione è andata oltre gli schieramenti politici nel Congresso. Se il presidente può ignorare le leggi che

regolano la sorveglianza e le intercettazioni, perché il Congresso si sta preoccupando di discutere la riautorizzazione di alcune disposizioni del Patriot Act? Qualsiasi dibattito sulle leggi è fondato sulla convinzione che il ramo esecutivo rispetterà la legge.

Non si tratta di una questione di partito fra Democratici e Repubblicani: si tratta di un presidente che calpesta unilateralmente il Quarto Emendamento, il Congresso e la Corte Suprema. Il potere presidenziale non controllato non ha niente a che vedere con quanto si possa amare o odiare George W. Bush. Occorre immaginare tale potere nelle mani della persona che più di ogni altra non si vorrebbe avere come presidente, che sia Dick Cheney o Hillary Rodham Clinton, Michael Moore o Ann Coulter.

Le leggi sono ciò che ci dà sicurezza contro le azioni della maggioranza e dei potenti. Se rinunciamo alle nostre protezioni costituzionali contro la tirannia nel tentativo di proteggerci dal terrorismo, finiremo con l'essere tutti molto meno al sicuro.

Questo articolo è stato pubblicato il 21 dicembre come editoriale di opinione nel "Minneapolis Star Tribune".

<<http://www.startribune.com/562/story/138326.html>>

Ecco il paragrafo di apertura del memo di Yoo. Ribadisco, nel leggerlo pensate a questo potere nelle mani dell'uomo politico che più odiate:

"Avete richiesto la nostra opinione in merito all'ambito dell'autorità presidenziale di intraprendere azioni militari in risposta agli attacchi terroristici ai danni degli Stati Uniti dell'11 settembre 2001. Concludiamo che il presidente possiede pieni poteri costituzionali di utilizzare la forza militare. Il Congresso ha riconosciuto tali intrinseci poteri esecutivi nella War Powers Resolution, Pub. L. No. 93-148, 87 Stat. 555 (1973), codificata in 50 U.S.C. §§ 1541-1548 (la "WPR"), e nella Joint Resolution approvata dal Congresso il 14 settembre 2001, Pub. L. No. 107-40, 115 Stat. 224 (2001). Inoltre, il presidente possiede il potere costituzionale non soltanto di rivalersi ai danni di qualsiasi persona, organizzazione o Stato sospettati di essere coinvolti in azioni terroristiche contro gli Stati Uniti, ma anche contro paesi stranieri sospettati di ospitare e supportare tali organizzazioni. Infine, il presidente potrà disporre forza militare preventivamente contro organizzazioni terroristiche o contro i paesi che le ospitano o le supportano, a prescindere che tali entità siano o meno collegate agli specifici incidenti terroristici dell'11 settembre".

Un modo analogo di ragionare è presente nel memo di Braybee, scritto nel 2002 sulla tortura.

Il memo di Yoo:

<<http://www.usdoj.gov/olc/warpowers925.htm>>

Il memo di Braybee:

<<http://www.washingtonpost.com/wp-srv/nation/documents/dojinterrogationmemo20020801.pdf>>

Questa storia si è animata di vita propria. Ma vi sono un milione di link elencati qui:

<http://www.schneier.com/blog/archives/2005/12/the_security_th_1.html>

Mi diverte in particolar modo il pezzo sui supervisori di turno della NSA che prendono decisioni legalmente riservate al tribunale FISA.

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

Il Progetto Shamrock

Decenni prima dell'11 settembre e del successivo ordine di Bush che ha autorizzato la NSA a intercettare qualsiasi telefonata, messaggio email, e chissà cos'altro, da e verso gli Stati Uniti, spiando anche i cittadini americani, il governo fece la stessa cosa con i telegrammi. Venne chiamato Progetto Shamrock, e chiunque pensi che questo sia un nuovo terreno legale e tecnologico dovrebbe andarsi a leggere in che cosa è consistito quel programma.

Dalla Wikipedia: "Il Progetto SHAMROCK [...] fu un esercizio di spionaggio che prevedeva l'accumulo di tutti i dati telegrafici in entrata e in uscita dagli Stati Uniti. All'Armed Forces Security Agency (AFSA) e al suo successore, la NSA, venne consentito l'accesso diretto alle copie quotidiane su microfilm di tutti i telegrammi in entrata, in uscita e in transito attraverso la Western Union e i suoi associati RCA e ITT. L'operazione Shamrock durò per tutti gli anni Sessanta, quando operazioni computerizzate (HARVEST) resero possibile la ricerca per parole chiave, senza dover leggere le comunicazioni per intero.

"Il Progetto Shamrock ebbe un tale successo che nel 1966 la NSA e la CIA costituirono un'azienda di copertura in lower Manhattan (dove si trovavano gli uffici delle compagnie telegrafiche) con il nome in codice LPMEDLEY. All'apice del Progetto Shamrock, venivano stampati e analizzati da agenti della NSA ben 150.000 messaggi al mese. Tuttavia, nel maggio 1975, alcuni critici governativi iniziarono a investigare e ad esporre il programma. Di conseguenza il direttore della NSA Lew Allen lo terminò. La testimonianza di entrambi i rappresentanti delle compagnie telegrafiche e del direttore Allen alle udienze spinse il presidente del Senate Intelligence Committee, Senatore Frank Church, a concludere che il Progetto SHAMROCK è stato 'probabilmente il più grande programma di intercettazione governativo ai danni degli americani mai intrapreso'".

Per chi è interessato ai dettagli, il luogo migliore ove trovarli sono i libri di James Bamford sulla NSA: "The Puzzle Palace", del 1982, e "Body of Secrets" del 2001. L'estratto seguente è dal secondo libro, pagina 440:

"Fra le riforme scaturite dall'indagine del Church Committee vi fu la creazione del Foreign Intelligence Surveillance Act (FISA), il quale, per la prima volta, indicava ciò che alla NSA era permesso o proibito fare. Il nuovo statuto mise fuori legge l'acquisizione su vasta scala e senza un mandato di telegrammi come erano stati raccolti sotto il Progetto Shamrock. Inoltre mise fuori legge la compilazione arbitraria di watch list contenenti nomi di cittadini americani. Attraverso il FISA venne costituito un tribunale federale segreto, il Foreign Intelligence Surveillance Court. Se la NSA intende prendere di mira un cittadino americano o uno straniero con residenza permanente (chi possiede una "green

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate la vicenda sulla quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

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

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

I numeri arretrati sono disponibili all'indirizzo <<http://www.schneier.com/crypto-gram.html>>.

Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate: <<http://www.schneier.com/crypto-gram.html>>

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

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

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.

Copyright (c) 2006 by Bruce Schneier.