

CRYPTO-GRAM
15 marzo 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:

Il futuro della privacy
Il riconoscimento facciale approda nei bar
Sicurezza, economia, e badge smarriti
Le ristampe di Crypto-Gram
Il data mining come arma antiterrorismo
Fallimento della sicurezza in un aeroporto
News
Escalation di privilegi dei dipartimenti di polizia
Un errore in un database produce un bilancio in deficit
Le compagnie di carte di credito e l'agenda di priorità
Le News di Counterpane
Una prova che gli impiegati non si curano della sicurezza
La sicurezza dei porti statunitensi e i mandatarî
Commenti dei lettori

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

Il futuro della privacy

Negli ultimi vent'anni vi è stata una svolta radicale nella battaglia per la privacy personale.

La diffusione sempre più capillare dei computer ha portato a una quasi costante sorveglianza di tutti, con profonde conseguenze per la nostra società e le nostre libertà. Sia le grandi aziende che le forze dell'ordine stanno utilizzando questo nuovo tesoro di dati di sorveglianza. Noi, in quanto società, dobbiamo comprendere le tendenze tecnologiche e discuterne le implicazioni. Se ignoriamo il problema e lo lasciamo al "mercato", scopriremo presto di avere ben poca privacy da difendere.

La maggior parte delle persone pensa alla sorveglianza in termini di procedura di polizia: seguire quell'auto, osservare quella data persona,

intercettare le sue conversazioni telefoniche. Questo genere di sorveglianza viene ancora impiegato, ma la sorveglianza attuale segue più da vicino il modello della NSA, usato di recente a danno dei cittadini americani: intercettare ogni conversazione telefonica, alla ricerca di alcune parole chiave. Si tratta sempre di sorveglianza, ma è sorveglianza all'ingrosso.

Quello della sorveglianza all'ingrosso è un universo completamente nuovo. Non si tratta di "seguire quell'auto", ma di "seguire tutte le auto". La National Security Agency può mettersi in ascolto di qualunque telefonata, ricercando pattern di comunicazione o parole chiave che possano indicare una conversazione fra terroristi. Molti aeroporti tengono traccia di tutte le targhe dei veicoli lasciati nei loro parcheggi, e possono utilizzare quel database per localizzare automobili sospette o abbandonate. In diverse città vi sono scanner di targhe automobilistiche fissi oppure montati su auto della polizia, che registrano ogni veicolo di passaggio e conservano i dati raccolti per successive analisi.

Sempre in maggior misura, giorno dopo giorno, lasciamo una scia di "impronte elettroniche". Una volta si andava in libreria, si dava un'occhiata in giro, e si comprava un libro pagandolo in contanti. Ora si visita Amazon, e tutto quel che cerchiamo e compriamo viene registrato. Una volta si pagava il pedaggio autostradale inserendo monete in una macchina; ora il Telepass registra la data e l'ora del nostro passaggio al casello. Vengono raccolti dati che ci riguardano ogni volta che facciamo una telefonata, inviamo un'email, acquistiamo qualcosa con la carta di credito o visitiamo un sito Web.

Molto è stato scritto in merito ai chip RFID e a come possano essere utilizzati per tener traccia delle persone. Le persone possono anche essere localizzate attraverso i loro telefoni cellulari, i loro dispositivi Bluetooth e i loro computer dotati di WiFi. In alcune città, delle videocamere catturano la nostra immagine centinaia di volte al giorno.

L'elemento comune in tutti questi casi sono i computer. I computer sono sempre più coinvolti nelle nostre transazioni, e i dati sono un prodotto secondario di tali transazioni. Con la progressiva diminuzione del costo della memoria dei calcolatori, un sempre maggior numero di queste "impronte elettroniche" viene conservato. E con il diminuire dei costi di elaborazione, una sempre maggior quantità di tali dati viene diversamente indicizzata e correlata, per poi venire impiegata con secondi fini.

Le informazioni che ci riguardano hanno un valore. Per la polizia, ma anche per le grandi aziende. Il Dipartimento di Giustizia vuole i dettagli delle ricerche fatte con Google, in modo da poter cercare pattern che possano servire a trovare pedopornografi. Google si serve di quegli stessi dati per visualizzare annunci pubblicitari sensibili al contesto. La città di Baltimora si serve della fotografia aerea per sorvegliare ogni casa, alla ricerca di eventuali abusi edilizi. Un'azienda di giardinaggio utilizza gli stessi dati per migliorare il marketing dei propri servizi. La compagnia telefonica mantiene registri dettagliati delle chiamate per emettere periodicamente la bolletta; la polizia li utilizza per catturare i malviventi.

Durante il boom del "dot.com", il database clienti era spesso l'unica risorsa vendibile nelle mani di una società. Aziende come Experian e Acxiom sono nel business della compravendita di questo genere di informazioni, e i loro clienti sono altre aziende ma anche enti governativi.

I computer diventano più piccoli e meno costosi ogni anno, e questa tendenza è destinata a continuare. Ecco soltanto un esempio delle "impronte elettroniche" che lasciamo:

Per memorizzare tutto quello che il dattilografo più veloce è in grado di immettere nel proprio computer in un anno sono necessari circa 100 megabyte. Ossia una singola memoria flash odierna, e possiamo immaginare i produttori di computer offrire una cosa del genere come funzionalità per una migliore affidabilità. Per registrare tutto quel che l'utente medio svolge interagendo con Internet è richiesta più memoria, da 4 a 8 gigabyte all'anno. È molto, ma "immagazzinare tutto" è il modello di Gmail, e probabilmente fra non molti anni tutti gli ISP offriranno un servizio del genere.

L'individuo medio spende 500 minuti al mese in conversazioni al cellulare, ovvero 5 gigabyte all'anno per registrare tutte queste informazioni. Il mio iPod può memorizzare 12 volte quei dati. Un piccolo "registratore vitale" da indossare e che registra di continuo è ancora lontano qualche generazione: 200 gigabyte all'anno per la parte audio, 700 gigabyte all'anno per il video. Verrà venduto come dispositivo di sicurezza, in modo che nessuno possa attaccarvi senza essere registrato. Quando questo oggetto sarà realtà, il non indossarlo verrà usato come prova che una persona intende commettere un reato, nella stessa maniera in cui oggi in tribunale gli accusatori si servono del fatto che un individuo ha lasciato il proprio cellulare a casa come prova che costui non voleva essere rintracciato?

In un certo senso stiamo vivendo in un'epoca unica nella storia. I controlli di identità sono comuni, ma tuttora siamo ancora noi a dover estrarre i documenti. Presto la cosa avverrà in automatico, tramite un chip RFID nel portafoglio oppure mediante videocamere con riconoscimento facciale. E quelle videocamere, oggi ancora visibili, si rimpiccioliranno al punto da scomparire.

Non potremo mai fermare l'avanzamento tecnologico, ma possiamo emanare una legislazione che protegga la nostra privacy: leggi di vasta portata che stabiliscano ciò che può essere fatto con le informazioni personali sul nostro conto e che garantiscano una maggiore protezione della nostra privacy dalle forze di polizia. Oggi non siete in possesso delle informazioni personali su di voi: le possiede chi le raccoglie. Vi sono leggi a protezione di parti specifiche dei dati personali (i registri dei videonoleggi, le informazioni sanitarie) ma non sono nulla a confronto delle estese leggi di protezione della privacy che è possibile trovare nei paesi europei. Questa è davvero l'unica soluzione; lasciare al mercato il compito di risolvere tale questione avrà come risultato una sorveglianza all'ingrosso ancor più invasiva.

Molti di noi non hanno problemi a fornire informazioni personali in cambio di servizi specifici. Ciò a cui ci opponiamo è la raccolta di informazioni personali fatta di nascosto, e il secondo fine dell'utilizzo di tali informazioni una volta raccolte: la compravendita di dati personali che avviene alle nostre spalle.

In un certo senso, questa ondata di dati personali è il problema di inquinamento dell'era dell'informazione. Tutti i processi di informazione lo producono. Se ignoriamo il problema, esso continuerà ad esistere. E il solo sistema per affrontare tale inquinamento in modo efficace è quello di emanare leggi che ne regolino la sua produzione, uso, e conseguente smaltimento.

Questo articolo è stato originariamente pubblicato sul Minneapolis Star-Tribune.

<http://www.startribune.com/562/story/284023.html>

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

Il riconoscimento facciale approda nei bar

BioBouncer è un sistema di riconoscimento facciale studiato per i bar:

“La sua videocamera scatta un’istantanea dei clienti che entrano nei bar e nei locali, e il software di riconoscimento facciale effettua un confronto con immagini archiviate di piantagrane già identificati in precedenza. In caso il confronto sia positivo, il sistema avverte lo staff di sicurezza del locale, mentre le immagini di persone innocue e innocenti vengono automaticamente cancellate ogni notte - ha dichiarato Dussich. Vari locali possono condividere i propri database attraverso un virtual private network, per cui gli ubriachi più aggressivi potrebbero trovarsi estromessi da tutti i bar del loro quartiere”.

Vogliamo indovinare per quanto tempo durerà quell’“automaticamente cancellate ogni notte”? Questi dati hanno un valore enorme. Le compagnie di assicurazioni vorranno sapere se la tal persona si trovava in un bar prima di un incidente d’auto. Le aziende vorranno sapere se i loro impiegati stavano bevendo prima di recarsi al lavoro (si pensi ai piloti degli aerei). Gli investigatori privati vorranno sapere chi è entrato in un bar accompagnato da chi. La polizia vorrà sapere ogni genere di dettagli. Molte persone vorranno impossessarsi di queste informazioni, e tutti saranno disposti a pagare per averle.

E i dati saranno in possesso dai bar che li raccolgono. I bar possono scegliere di distruggerli o di venderli a data aggregator come Acxiom.

Molto raramente è l’applicazione iniziale a rappresentare il problema. I guai cominciano con le applicazioni che da essa conseguono. È il “function creep”, lo spostamento della funzione. Di questo passo, entro breve tempo tutti sapranno che saranno identificati quando entrano in un edificio commerciale. Come conseguenza, tutti perderemo privacy e libertà.

<http://www.wired.com/news/technology/1,70265-0.html>

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

Sicurezza, economia, e badge smarriti

I badge delle conferenze sono un interessante simbolo di sicurezza. Possono essere molto costosi (una registrazione completa alla RSA Conference di San Jose lo scorso mese, per esempio, costava 1.895 dollari) ma il loro valore diminuisce rapidamente col tempo. Alla fine della conferenza erano senza valore.

Falsificare i badge è una problematica di sicurezza, ma un problema ancor più grande è quando le persone smarriscono il proprio badge o quando viene rubato loro. È molto più a buon mercato trovare o rubare un badge altrui che doverlo comprare. La gente potrebbe fare questo genere di cose di proposito, ovvero far finta di perdere il proprio badge per poterlo dare a qualcun altro.

Alcuni anni fa, la RSA Conference chiedeva 100 dollari per la sostituzione di un badge, che è molto più economico di una seconda iscrizione. Per cui la frode continuava (almeno così presumo: non ho

idea della portata reale di questo tipo di frode nel contesto della RSA).

Lo scorso anno la RSA Conference ha cercato di limitare ulteriormente questo genere di frode aggiungendo una foto dell'iscritto sul badge. Buona idea, ma difficile da implementare.

Perché queste funzioni, infatti, le guardie devono confrontare le fotografie con i possessori del badge. Ciò significa 1) aver bisogno di molte più guardie nei punti di ingresso, o 2) che le varie code di persone procederanno più lentamente. In realtà è molto più probabile che accada un terzo caso: nessuno controllerà le fotografie.

E si trattava di una soluzione costosa per la RSA Conference. Era necessaria l'attrezzatura per inserire le foto nei badge. Il processo di registrazione era molto più lento. E le persone in favore della privacy non volevano che la RSA Conference tenesse in archivio le loro fotografie.

Quest'anno, la RSA Conference ha risolto il problema attraverso l'economia: "In caso di smarrimento del badge o del porta-badge, sarà necessario acquistarne uno nuovo al prezzo di 1.895 dollari".

Si osservi l'astuzia di tale soluzione. Invece di risolvere questo particolare problema di frode legata ai badge da un punto di vista di sicurezza, il problema è stato semplicemente spostato dalla conferenza sul partecipante. I badge hanno ancora il loro valore di 1.895 dollari, ma se adesso il badge viene rubato e utilizzato da qualcun altro, è il partecipante alla conferenza che deve pagare. Nella prospettiva della RSA Conference, il rischio di sicurezza è un'esternalità.

Si noti invece che, da un punto di vista esterno, questo non si tratta del sistema più efficiente per affrontare il problema di sicurezza. È probabile che per la RSA Conference i costi per la sicurezza centralizzata siano minori dell'insieme dei costi delle singole misure di sicurezza. Ma è la RSA Conference a stabilire il compromesso, e quindi ha scelto la soluzione più economica per sé.

Naturalmente sarebbe stato meglio che si provvedesse a un punto di attacco più sicuro per il porta-badge, invece di un sottile nastro di plastica. Ma perché curarsi di tutto ciò? Non è più un problema della RSA Conference.

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

Le ristampe di Crypto-Gram

Crypto-Gram è attualmente al suo nono anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare tutti a questo indirizzo:

<http://www.schneier.com/crypto-gram-back.html>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

SHA-1 compromesso:

<http://www.schneier.com/crypto-gram-0503.html#1>

<http://www.crypto-gram.it/cryptogramPdf/Marzo2005.pdf> (traduzione in italiano)

I limiti dell'autenticazione a due fattori:

<http://www.schneier.com/crypto-gram-0503.html#2>

<http://www.crypto-gram.it/cryptogramPdf/Marzo2005.pdf>

Sensitive Security Information (SSI):

[<http://www.schneier.com/crypto-gram-0503.html#11>](http://www.schneier.com/crypto-gram-0503.html#11)
[<http://www.crypto-gram.it/cryptoqramPdf/Marzo2005.pdf>](http://www.crypto-gram.it/cryptoqramPdf/Marzo2005.pdf)

Tessere che certificano "Io non sono un Terrorista":

[<http://www.schneier.com/crypto-gram-0403.html#10>](http://www.schneier.com/crypto-gram-0403.html#10)
[<http://www.crypto-gram.it/marzo04.htm#a10>](http://www.crypto-gram.it/marzo04.htm#a10)

I rischi di sicurezza della centralizzazione:

[<http://www.schneier.com/crypto-gram-0403.html#11>](http://www.schneier.com/crypto-gram-0403.html#11)
[<http://www.crypto-gram.it/marzo04.htm#a11>](http://www.crypto-gram.it/marzo04.htm#a11)

Practical Cryptography - Crittografia pratica

[<http://www.schneier.com/crypto-gram-0303.html#1>](http://www.schneier.com/crypto-gram-0303.html#1)
[<http://www.crypto-gram.it/marzo03.htm#a1>](http://www.crypto-gram.it/marzo03.htm#a1)

Una falla nel protocollo SSL

[<http://www.schneier.com/crypto-gram-0303.html#3>](http://www.schneier.com/crypto-gram-0303.html#3)
[<http://www.crypto-gram.it/marzo03.htm#a3>](http://www.crypto-gram.it/marzo03.htm#a3)

Contraffazione del brevetto SSL

[<http://www.schneier.com/crypto-gram-0303.html#8>](http://www.schneier.com/crypto-gram-0303.html#8)
[<http://www.crypto-gram.it/marzo03.htm#a8>](http://www.crypto-gram.it/marzo03.htm#a8)

Vulnerabilità di SNMP:

[<http://www.schneier.com/crypto-gram-0203.html#1>](http://www.schneier.com/crypto-gram-0203.html#1)
[<http://www.crypto-gram.it/marzo02.htm#a1>](http://www.crypto-gram.it/marzo02.htm#a1)

La fattorizzazione di Bernstein: una svolta?

[<http://www.schneier.com/crypto-gram-0203.html#6>](http://www.schneier.com/crypto-gram-0203.html#6)
[<http://www.crypto-gram.it/marzo02.htm#a6>](http://www.crypto-gram.it/marzo02.htm#a6)

Richard Clarke sulle lezioni dell'11 settembre:

[<http://www.schneier.com/crypto-gram-0203.html#7>](http://www.schneier.com/crypto-gram-0203.html#7)
[<http://www.crypto-gram.it/marzo02.htm#a7>](http://www.crypto-gram.it/marzo02.htm#a7)

Realizzare una patch di sicurezza:

[<http://www.schneier.com/crypto-gram-0103.html#1>](http://www.schneier.com/crypto-gram-0103.html#1)

Le assicurazioni e il futuro della sicurezza dei network:

[<http://www.schneier.com/crypto-gram-0103.html#3>](http://www.schneier.com/crypto-gram-0103.html#3)

La "morte" degli IDS:

[<http://www.schneier.com/crypto-gram-0103.html#9>](http://www.schneier.com/crypto-gram-0103.html#9)

Sicurezza e il protocollo 802.11:

[<http://www.schneier.com/crypto-gram-0103.html#10>](http://www.schneier.com/crypto-gram-0103.html#10)

La complessità del software e la sicurezza:

[<http://www.schneier.com/crypto-gram-0003.html#SoftwareComplexityandSecurity>](http://www.schneier.com/crypto-gram-0003.html#SoftwareComplexityandSecurity)

Perché la peggiore crittografia risiede in quei sistemi che superano le prime crittanalisi:

[<http://www.schneier.com/crypto-gram-9903.html#initial>](http://www.schneier.com/crypto-gram-9903.html#initial)

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

Il data mining come arma antiterrorismo

Nel mondo post-11 settembre si presta molta attenzione a “unire i punti”. Molti credono che il data mining sia la sfera di cristallo che ci permetterà di svelare future trame terroristiche. Ma anche nelle proiezioni più sfrenatamente ottimistiche, il data mining non è sostenibile per tale scopo. Non stiamo barattando la privacy per la sicurezza; stiamo rinunciando alla privacy senza ottenere in cambio alcuna sicurezza.

Moltissime persone scoprirono per la prima volta in che cosa consiste il data mining nel novembre 2002, quando fece notizia un massiccio programma governativo di data mining chiamato Total Information Awareness. L'idea di fondo era audace quanto ripugnante: raccogliere quanti più dati possibile su chiunque, passarli al vaglio grazie a potentissimi calcolatori, e investigare quei pattern, quelle ricorrenze che potrebbero indicare trame terroristiche. Gli americani di ogni credo politico denunciarono il programma, e nel settembre 2003 il Congresso ne eliminò i fondi e ne chiuse gli uffici.

Ma Total Information Awareness non scomparve. Secondo “The National Journal” cambiò semplicemente nome e fu spostato all'interno del Dipartimento della Difesa.

Ciò non dovrebbe sorprendere. Nel maggio 2004, il General Accounting Office pubblicò un rapporto che elencava 122 diversi programmi di data mining varati dal governo federale che si servivano delle informazioni personali dei cittadini. Tale lista non comprendeva i programmi segreti, come le intercettazioni della NSA o programmi a livello statale come MATRIX.

La promessa del data mining è avvincente, e molti ne sono affascinati. Ma tutto ciò è sbagliato. Non scopriremo trame terroristiche con sistemi come questo, e siamo in procinto di sprecare risorse preziose inseguendo falsi allarmi. Per capire perché, occorre osservare l'economia del sistema.

La sicurezza è sempre un compromesso, e perché un sistema sia valido, i vantaggi devono essere maggiori degli svantaggi. Un programma di data mining nazionale troverà una certa percentuale di attacchi reali, e una certa percentuale di falsi allarmi. Se i benefici derivanti dall'individuare e dal fermare quegli attacchi superano i costi (in denaro, in libertà, ecc.) allora il sistema è buono. In caso contrario, sarebbe preferibile spendere quei costi in altro modo.

Il data mining funziona al meglio quando si è alla ricerca di un ben determinato profilo, un numero ragionevole di attacchi ogni anno, e un costo contenuto per i falsi allarmi. La frode delle carte di credito è un caso di successo del data mining: tutte le compagnie di carte di credito esaminano i propri database delle transazioni in cerca di pattern di spesa che indichino la presenza di una carta di credito rubata. Molti ladri di carte di credito presentano un simile pattern: l'acquisto di costosi beni di lusso, l'acquisto di oggetti facilmente smerciabili tramite ricettazione, ecc.; e i sistemi di data mining in molti casi possono minimizzare le perdite bloccando la carta. In più, il costo dei falsi allarmi è rappresentato solo da una telefonata al titolare della carta, richiedendogli di verificare un paio di acquisti. E i titolari delle carte non sono nemmeno seccati da queste chiamate (purché avvengano di rado), per cui il costo si riduce semplicemente ad alcuni minuti di chiamata con un operatore.

Le trame terroristiche sono differenti. Non esiste un profilo ben determinato, e gli attacchi sono molto rari. Presi insieme, questi fatti significano che i sistemi di data mining non rileveranno alcun complotto terroristico a meno che non siano molto accurati, e che anche i sistemi

più accurati saranno talmente inondati da falsi allarmi da diventare inutili.

Tutti i sistemi di data mining falliscono in due modi diversi: falsi positivi e falsi negativi. Un falso positivo è quando il sistema identifica un complotto terroristico che in realtà non è tale. Un falso negativo è quando al sistema sfugge un complotto terroristico vero e proprio. A seconda di come vengono "sintonizzati" gli algoritmi di rilevamento, l'errore può pendere da una parte o dall'altra: è possibile aumentare il numero di falsi positivi per assicurare una minore probabilità di mancare un vero complotto terroristico, oppure è possibile ridurre il numero di falsi positivi correndo il rischio di non individuare trame terroristiche.

Per ridurre entrambi quei numeri, è necessario un profilo ben definito. Ed è questo il problema quando si è alle prese con il terrorismo. Col senno di poi, era davvero semplice "unire i punti" dell'11 settembre e puntare ai vari segnali d'allarme, ma è molto più difficile prima dell'evento. Di sicuro esistono segnali d'allarme comuni a molti complotti terroristici, ma ognuno è al tempo stesso unico. Più è possibile definire nei dettagli ciò che si sta cercando, migliori saranno i risultati. Il data mining alla caccia di trame terroristiche è destinato a essere approssimativo, e sarà difficile scoprire qualcosa di utile.

Il data mining è come cercare un ago in un pagliaio. Vi sono 900 milioni di carte di credito in circolazione negli Stati Uniti. Secondo lo FTC Identity Theft Survey Report del settembre 2003, ogni anno circa l'1% (10 milioni) delle carte di credito viene rubato e usato in modo fraudolento. Il terrorismo è diverso. Vi sono trilioni di connessioni fra persone ed eventi (cose che il sistema di data mining dovrà "osservare") e pochissimi complotti. Questo livello di rarità rende inutili persino i sistemi di identificazione più accurati.

Facciamo due conti, essendo molto ottimisti. Supponiamo che il sistema presenti un tasso di falsi positivi di 1 su 100 (99% di accuratezza), e un tasso di falsi negativi di 1 su 1000 (99,9% di accuratezza).

Supponiamo di dover esaminare un trilione di possibili indicatori: si tratta all'incirca di 10 eventi (email, telefonate, acquisti, giri su Internet, ecc.) per persona negli Stati Uniti ogni giorno. Supponiamo inoltre che 10 di essi siano in effetti complotti terroristici.

Questo sistema irrealisticamente accurato genererà un miliardo di falsi allarmi per ogni complotto terroristico rilevato. Ogni giorno di ogni anno le forze dell'ordine dovranno investigare 27 milioni di potenziali complotti per poter arrivare a scoprire l'unico vero complotto terroristico ogni mese. Aumentiamo l'accuratezza dei falsi positivi a un assurdo 99,9999% e si dovranno affrontare ancora 2.750 falsi allarmi al giorno; ma questo farà aumentare inevitabilmente anche i falsi negativi, e sarà molto probabile mancare uno di quei dieci veri complotti terroristici.

Tutto ciò non è nulla di nuovo. In statistica viene chiamato "base rate fallacy" (fallacia della probabilità primaria) e si applica anche in altri contesti. Per esempio, anche test medici altamente accurati sono inutili come strumenti diagnostici se l'incidenza della malattia è rara nella popolazione generale. Anche gli attacchi terroristici sono rari, e qualsiasi "test" non porterà altro che a una scia infinita di falsi allarmi.

Questo è proprio il genere di cosa che abbiamo potuto vedere con il programma di intercettazione della NSA: il "New York Times" ha riportato

che i computer emettevano migliaia di indicazioni ogni mese, e che ognuna di esse si è rivelata essere un falso allarme.

E il costo è stato smisurato: non solo il costo degli agenti dell'FBI persi in vicoli ciechi dietro a fantomatici indizi invece di occuparsi di cose che ci rendano davvero più sicuri, ma anche il costo delle libertà civili. Le libertà fondamentali che rendono il nostro paese oggetto d'invidia in tutto il mondo sono assai preziose, e non si dovrebbero gettare via così alla leggera.

Il data mining può funzionare. Aiuta Visa a contenere i costi delle frodi, così come aiuta Amazon.com a mostrarmi libri che potrebbero interessarmi e che potrei comprare, e Google a mostrarmi annunci pubblicitari che potrebbero incuriosirmi. Ma queste sono tutte istanze in cui il costo dei falsi positivi è basso (una chiamata di un operatore Visa, un annuncio non interessante) e riguardano sistemi che hanno valore anche se il numero di falsi negativi è elevato.

Scoprire complotti terroristici non è un problema che si presta a essere risolto dal data mining. È il tipico caso dell'ago nel pagliaio, e aumentare la pila di paglia non facilita la risoluzione del problema. Sarebbe molto meglio incaricare persone all'investigazione di potenziali trame terroristiche e permettere a queste persone di dirigere i computer, invece di assegnare l'incarico ai computer e lasciar decidere a loro chi bisognerebbe indagare.

Questo articolo è originariamente apparso su Wired.com.
<<http://www.wired.com/news/columns/0,70357-0.html>>

Total Information Awareness:
<<http://www.epic.org/privacy/profiling/tia/>>
<<http://www.fas.org/sgp/congress/2003/tia.html>>

Il suo ritorno:
<<http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm>>

Il rapporto del GAO:
<http://www.epic.org/privacy/profiling/gao_dm_rpt.pdf>

MATRIX:
<<http://www.aclu.org/privacy/spying/15701res20050308.html>>

Base rate fallacy:
<<http://www.cia.gov/csi/books/19104/art15.html#ft145>>

Il "New York Times" sul programma di intercettazione della NSA:
<http://www.schneier.com/blog/archives/2006/01/post_1.html>

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

Fallimento della sicurezza in un aeroporto

All'aeroporto LaGuardia, un uomo ha passato senza problemi il metal detector, ma gli agenti di sicurezza intendevano comunque esaminare le sue scarpe (alcune fonti affermano che le scarpe avrebbero fatto scattare un allarme). Ma l'uomo non ha aspettato, ed è scomparso nella folla.

L'intero terminal della Delta Airlines è stato fatto evacuare e circa 2.500 - 3.000 persone hanno dovuto ripassare il checkpoint. Sono sicuro

che i ritardi dei voli, causati da questo incidente, hanno avuto effetto su tutto il sistema.

I sistemi di sicurezza possono fallire in due modi. Possono fallire nella difesa contro un attacco, e possono fallire quando non esiste alcun attacco da cui difendersi. Spesso questo secondo caso è più importante, perché i falsi allarmi sono molto più frequenti degli attacchi veri e propri.

A parte l'ovvio fallimento di sicurezza (come è riuscita questa persona a scomparire nella folla, fra l'altro?), è tremendamente lapalissiano come l'intero sistema di sicurezza abbia fallito miseramente. I sistemi di sicurezza ben progettati possono fallire con eleganza, senza influire sull'intero terminal dell'aeroporto. Che l'unica cosa che la TSA abbia potuto fare dopo l'errore sia stata evacuare l'intero terminal e ricontrollare tutti i passeggeri testimonia quanto mal progettato sia il sistema di sicurezza.

<http://www.newsday.com/news/printedition/newyork/nyc-nydelt114658156mar11,0,7784010.story> oppure <http://tinyurl.com/jtzuo>
<http://news.bbc.co.uk/2/hi/americas/4795534.stm>

** *** *****

News

"Lessons from the Sony CD DRM Episode" [Lezioni dall'episodio del DRM dei CD di Sony] è un interessante studio di J. Alex Halderman e Edward W. Felten.

<http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf>

Questo è un ottimo esempio di minaccia da trama cinematografica: terroristi che dirottano scuolabus e li utilizzano come ordigni esplosivi.

http://www.schneier.com/blog/archives/2006/02/school_bus_driv.html

Un tribunale ha stabilito che le aziende non sono tenute a crittografare i dati secondo il Gramm-Leach-Bliley Act. Non so nulla dei meriti legali del caso, né sono sicuro sul fatto che il Gramm-Leach-Bliley, nel suo testo dispositivo, richieda o non richieda alle compagnie finanziarie di crittografare dati personali. Ma so che noi, in quanto società, dobbiamo obbligare le aziende a crittografare le informazioni personali che ci riguardano. Le aziende non lo faranno di propria iniziativa (il mercato non incoraggia questo tipo di azione), e quindi le uniche armi a disposizione sono la legislazione o la responsabilità. Se questa legge non può garantirlo, allora ne occorre un'altra.

http://writ.news.findlaw.com/commentary/20060220_sinrod.html

<http://www.securityfocus.com/columnists/387>

Trovo impressionante questo attacco di phishing per varie ragioni. 1) È un attacco molto sofisticato e dimostra quanto scaltri stiano diventando i ladri di identità. 2) Ha specificatamente come bersaglio un istituto di credito, e sfrutta il fatto che le carte di credito emesse da un'istituzione hanno tutte le stesse cifre iniziali. 3) Sfrutta un problema di autenticazione dei certificati SSL. E 4) rappresenta l'ennesima prova che l'"educazione dell'utente" non è il sistema per risolvere questo tipo di rischi.

http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html oppure <http://tinyurl.com/773mg>

<http://isc.sans.org/diary.php?storyid=1118>

Patrick Smith, un ex-pilota, scrive delle sue esperienze (che riguardano anche le forze dell'ordine) scattando fotografie negli aeroporti.
<<http://www.salon.com/tech/col/smith/2006/02/10/askthepilot173/index1.html>> oppure <<http://tinyurl.com/gxuaw>>

Ancora sulla sicurezza nei porti (divertente):
<<http://www.defectiveyeti.com/archives/001599.html>>

Il capo della polizia di Houston intende installare videocamere di sorveglianza in complessi di edifici, strade del centro, centri commerciali e persino in case di privati per combattere il crimine durante un periodo di scarsità di agenti di polizia. Ha dichiarato: "So che molta gente è preoccupata per l'effetto Grande Fratello, ma in risposta a questo io dico: se non state facendo niente di male, perché preoccuparsi?". Uno dei problemi che abbiamo nella comunità a favore della privacy è che non possediamo una risposta incisiva a quella domanda. Ho chiesto suggerimenti nel mio blog, e vi sono state delle risposte davvero ottime.
<<http://www.dallasnews.com/sharedcontent/APStories/stories/D8FPQU300.html>> oppure <<http://tinyurl.com/z7shz>>
<http://www.schneier.com/blog/archives/2006/02/police_cameras.html>

Ecco come costruirsi un key logger hardware per tastiere PS/2.
<http://www.makezine.com/blog/archive/2006/02/diy_hardware_keylogger.html> oppure <<http://tinyurl.com/h3bp8>>
Qui è possibile comprarne uno:
<<http://www.keycatcher.com/>>
<<http://www.lakeshoretechnology.com/KeyPhantom.asp>>
<<http://www.keyghost.com/kgpro.htm>>
<<http://www.keytrapper.com/>>
<<http://www.spectorsoft.com/>>

Il progetto M4 sta cercando di decifrare tre messaggi originali di Enigma lasciati durante la Seconda Guerra Mondiale.
<http://www.bytereef.org/m4_project.html>
<<http://news.bbc.co.uk/2/hi/technology/4763854.stm>>

Qualcosa come 50 milioni di sterline sono stati rubati da un deposito di denaro nel Regno Unito. Il Times scrive: "Una volta i furti di denaro di grande portata erano una vera e propria sfida tecnica: perforare muri, cortocircuitare allarmi, soffocare guardie e posizionare il veicolo per la fuga. Oggi i punti deboli della difesa delle banche non sono gli sportelli o i caveau, ma gli esseri umani. Rubare denaro oggi è in parte anche una questione di psicologia. Il successo dei rapinatori di Tonbridge è dipeso dall'aver spaventato a morte il signor Dixon per indurlo ad aprire le porte. Avevano studiato la vittima. Sapevano che strada faceva per tornare a casa ogni giorno e sapevano come avrebbe risposto se sua moglie e suo figlio si fossero trovati in pericolo di vita. Non è stata usata la dinamite per far saltare il caveau, ma la paura, mediante la tecnica nota come 'tiger kidnapping', così chiamata per evidenziare il seguire furtivo della preda che precede il colpo. Il 'tiger kidnapping' è il punto in cui il crimine vecchio stile incontra il più moderno terrorismo".
<<http://www.timesonline.co.uk/newspaper/0,,175-2057507,00.html>>

Una buona cronologia degli eventi:
<<http://news.bbc.co.uk/1/hi/england/kent/4742972.stm>>

Sorveglianza tramite DNA nel Regno Unito:
<http://www.schneier.com/blog/archives/2006/02/dna_surveillanc.html>

Il quantum computing, l'elaborazione quantica, è diventato ancor più bizzarro: non è nemmeno necessario accendere il computer per ottenere un

risultato. Per cui ora anche spegnere il computer non impedirà necessariamente agli hacker di sottrarre password.

<http://www.newscientist.com/channel/info-tech/mg18925405.700.html>
<http://cosmicvariance.com/2006/02/28/paul-kwiat-on-quantum-computation>

oppure <http://tinyurl.com/g87yo>

Il mese scorso ho scritto in merito a uno scandalo legato a intercettazioni telefoniche in Grecia. Stanno emergendo maggiori dettagli. Pare che il "codice malevolo" fosse in realtà codice progettato all'interno del sistema. Si tratta di codice per intercettazioni inserito nel sistema per la polizia. Gli aggressori sono riusciti ad aggirare i meccanismi di autorizzazione del sistema di intercettazione e hanno attivato il modulo di "intercettazione legittima" nella rete mobile. Poi hanno reindirizzato circa 100 numeri verso 14 numeri fantasma sotto il loro controllo. Qui vi è un'importante lezione di sicurezza. Ho sostenuto per molto tempo che implementare meccanismi di sorveglianza all'interno di sistemi di comunicazione significa invitare i malviventi a sfruttare tali meccanismi per i loro scopi. Ed è esattamente quel che è avvenuto in questo caso.

http://www.schneier.com/blog/archives/2006/02/phone_tapping_i.html
<http://homes.esat.kuleuven.be/~gdanezis/intercept.html>
<http://www.quintessenz.org/cgi-bin/index?id=000100002344>
<http://betabug.ch/blogs/ch-athens/312>

Convocazione come giurato: frode allo scopo di furto d'identità.

<http://www.snopes.com/crime/fraud/juryduty.asp>

La tessera ExpressPay di FedEx Kinko's è stata oggetto di hacking. Non vi è nulla di particolarmente straordinario nell'hacking: ciò che va notato è quanto male sia stato ideato il sistema in primo luogo. L'unico elemento di sicurezza sulle tessere è un codice di tre byte che permette di leggere e scrivere sulla tessera. Sarei sorpreso se nessuno lo avesse mai craccato prima d'ora.

<http://www.mal-aware.org/2006/02/28/fedex-kinkos-smart-cards-hacked/>
<http://www.eweek.com/article2/0,1759,1932824,00.asp?kc=EWRSS03119TX1K0000594> oppure <http://tinyurl.com/zf58a>

Nulla di eccezionalmente sorprendente in questo studio sulle pratiche di creazione delle password:

<http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm>

Spoofing dell'identificativo di chiamata: scherzi dannosi, invasioni della privacy, e frodi.

<http://www.startribune.com/484/story/278518.html>
<http://www.wired.com/news/technology/0,70320-0.html>

Il database di AT&T: 1,9 trilioni di chiamate.

http://www.schneier.com/blog/archives/2006/03/atts_19trillion.html

Questa vicenda mostra quali disastri può combinare il profiling antiterrorismo: una coppia è stata indagata per aver ripagato una grossa fetta del proprio debito della carta di credito. Nell'articolo si accusa il Bank Privacy Act, ma non è esatto. Il colpevole in questo caso sono gli emendamenti apportati al Bank Secrecy Act dal Patriot Act USA, Sezioni 351 e 352. Ricordate, tutto il tempo speso inseguendo sciocchi falsi allarmi è tempo buttato. Scoprire complotti terroristici è un problema di segnale/rumore, ed episodi come questi fanno diminuire drasticamente quel rapporto: si aggiunge molto rumore senza aggiungere sufficientemente segnale. Ci rende meno sicuri, perché rende i complotti terroristici più difficili da trovare.

http://www.shns.com/shns/g_index2.cfm?action=detail&pk=RAISEALARM-02-28-06 oppure <http://tinyurl.com/pju6w>

La legge:

<http://www.epic.org/privacy/terrorism/hr3162.html>
<http://www.cyberlaw.com/aml.html>
<http://www.fincen.gov/352ccards.pdf>

Pare che vi sia un class break (forma d'attacco trasversale) di vaste proporzioni ai danni degli sportelli bancomat di Citibank in Canada, nel Regno Unito e in Russia. Non ho esaminato tutti i dettagli; intanto ecco una serie di link utili:

http://www.schneier.com/blog/archives/2006/03/more_on_the_atm.html
<http://ioerror.livejournal.com/301520.html>
http://www.boingboing.net/2006/03/05/citibank_under_fraud.html
<http://www.consumerist.com/consumer/citibank/massive-citibank-fraud-alert-update-158565.php> oppure <http://tinyurl.com/g9y2>
<http://www.liquidmatrix.org/blog/2006/03/05/citibank-under-fraud-attack/> oppure <http://tinyurl.com/eey3o>
http://www.boingboing.net/2006/03/06/citibank_live_richly.html
<http://www.securityfocus.com/brief/157>
<http://www.msnbc.msn.com/id/11714119/>
<http://software.silicon.com/security/0,39024655,39157043,00.htm>

Utilizzare l'ingegneria sociale per autoinvitarsi agli Oscar:

<http://www.cnn.com/2006/SHOWBIZ/Movies/03/04/oscars.crashers.reut/index.html> oppure <http://tinyurl.com/k65ct>

Combattere l'abuso del Patriot Act:

<http://www.suntimes.com/output/steyn/cst-edt-steyn051.html>

Studio sullo "analog hole" [buco analogico], la dimensione umana del problema di proteggere le informazioni.

http://www.infoworld.com/article/06/03/01/75874_100Pstrategic_1.html

Analogamente, questa vicenda parla dei rischi di sicurezza del parlare a voce troppo alta:

<http://networks.silicon.com/mobile/0,39024665,39156987,00.htm>

Criminali fanno irruzione negli store fingendo di saccheggiarli, in realtà è una messinscena per installare di nascosto dell'hardware per leggere i bancomat, completo di trasmettitore. Si noti l'ultimo paragrafo della storia (è in danese, mi spiace) dove la compagnia ammette che questo è, a quanto ne sanno, il quarto tentativo di installazione di apparecchiature di lettura all'interno di sportelli bancomat allo scopo di leggere numeri e PIN.

<http://www.dr.dk/Nyheder/Indland/kriminalitet/2006/02/15/152517.htm>

Secondo la TSA, nel nono caso circoscrizionale di John Gilmore, è permesso volare senza mostrare alcun documento di identità - si dovrà solamente sottoporsi a ulteriore screening. Lo Identity Project vuole che proviate. Se avete tempo, provate a volare senza mostrare documenti di identità. So che è possibile farlo se si dichiara di aver smarrito il documento, ma non so quali possano essere le conseguenze se vi rifiutate semplicemente di mostrarlo.

<http://www.papersplease.org/investigation.html>

Nei Paesi Bassi, i criminali rubano denaro dai bancomat facendoli esplodere. Prima bucano il bancomat con un trapano e vi fanno passare un qualche gas. Poi accendono il gas (da una distanza di sicurezza) e raccolgono il denaro che vola dappertutto una volta che il bancomat è esploso. Sembra una cosa da pazzi, eppure si segnala di recente un aumento di questo tipo di attacco. La contromisura delle banche è quella di installare delle ventole di aerazione in modo che il gas non possa accumularsi all'interno dei bancomat.

http://www.nu.nl/news/683538/13/Banken_wapenen_zich_tegen_plofkraak.htm

l> oppure <http://tinyurl.com/z9mng>

GPG è una versione open source del protocollo PGP di crittografia email. Recentemente è stata scoperta nel software una vulnerabilità molto grave: dato un messaggio email firmato, è possibile modificare il messaggio (nello specifico, si possono aggiungere dati arbitrari in cima o a fine messaggio) senza disturbare la procedura di verifica della firma. (Questo bug è stato riparato nella versione 1.4.2.2; gli utenti dovrebbero aggiornare immediatamente la propria versione). Pare che il bug sia esistito per anni senza che nessuno se ne accorgesse. Morale: open source non significa necessariamente "meno bug". Ho scritto in merito a questo nel 1999.

<http://lists.gnupg.org/pipermail/gnupg-announce/2006q1/000216.html>
<http://www.schneier.com/crypto-gram-9909.html#OpenSourceandSecurity>

Trovare agenti della CIA sotto copertura utilizzando Internet:
<http://www.chicagotribune.com/news/nationworld/chi-060311ciamain-story,1,123362.story> oppure <http://tinyurl.com/qhe2d>
<http://www.theregister.co.uk/2006/03/13/ispy/>
<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/03/13/ucia.xml&Sheet=/portal/2006/03/13/ixportaltop.html> oppure <http://tinyurl.com/h673n>

Un articolo spiega come sia possibile modificare e poi stampare una propria carta d'imbarco e salire su un aereo anche se il vostro nome è sulla no-fly list. Non è una novità: ne ho parlato nel 2003.

<http://www.csoonline.com/read/020106/caveat021706.html>
<http://www.schneier.com/crypto-gram-0308.html#6>

Interessante, seppur lungo articolo sul bioterrorismo:
http://www.technologyreview.com/BioTech/wtr_16485,306,p1.html

Un astuto scherzo in occasione di un incontro di basket fra college fa perno sull'ingegneria sociale:
http://www.schneier.com/blog/archives/2006/03/basketball_pran.html

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

Escalation di privilegi dei dipartimenti di polizia

Negli Stati Uniti creare un proprio dipartimento di polizia è molto più facile di quel che si creda.

Yosef Maiwandi ha formato la San Gabriel Valley Transit Authority, una piccola organizzazione privata no-profit che fornisce un servizio di autobus per disabili e anziani. La centrale operativa è un'autofficina. Successivamente, siccome pare che la legge permetta alle compagnie di trasporti di creare i propri dipartimenti di polizia, Maiwandi ha costituito il San Gabriel Valley Transit Authority Police Department. Come ringraziamento, ha offerto a Stefan Eriksson la carica di commissario aggiunto della divisione antiterrorismo del San Gabriel Valley Transit Authority Police Department, e gli ha dato dei biglietti da visita.

Dipartimenti di polizia come questi non possiedono molta autorità legale, e in realtà non ne hanno bisogno. Suppongo che il nome stesso sia sufficientemente altisonante.

Nel mondo della sicurezza informatica, escalation dei privilegi significa servirsi di una autorità legittimamente assegnata per assicurarsi un'autorità ulteriore non prevista in precedenza. Questa

vicenda ne è la controparte nel mondo reale. Anche se i dipartimenti di polizia dei trasporti vengono costituiti per vigilare solamente sui propri veicoli, il titolo (e l'autorità apparente che ne deriva) è molto utile in altri contesti. Un individuo con intenti criminosi potrebbe facilmente servirsi di tale autorità per sfuggire ai controlli o per commettere frodi.

"Deal ha affermato che la sua agenzia ha scoperto che molte agenzie ferroviarie in California hanno creato dipartimenti di polizia, anche se le compagnie non hanno linee ferroviarie da pattugliare in California. L'agenzia di certificazione di polizia sta cercando di decertificare quelle agenzie perché non vi è alcuna ragione per cui debbano esistere in California.

"Il problema di aziende di trasporti privati che creano propri dipartimenti di polizia in questi ultimi anni ha destato preoccupazione in Illinois, dove alcuni individui con precedenti penali hanno creato linee ferroviarie allo scopo di formare agenzie di polizia".

Il vero problema è che abbiamo troppa deferenza nei confronti del potere delle forze dell'ordine. Non conosciamo i limiti dell'autorità della polizia, che si tratti di un poliziotto all'aeroporto o di qualcuno con un biglietto da visita del "San Gabriel Valley Transit Authority Police Department".

<http://www.latimes.com/news/local/la-me-ferrari8mar08,0,3717162.story>

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

Un errore in un database produce un bilancio in deficit

Una casa, erroneamente valutata 400 milioni di dollari ha causato inaspettati cali di bilancio e possibili licenziamenti per crisi in municipalità e quartieri scolastici nel nord-ovest dell'Indiana. Pare che un utente non autorizzato abbia cambiato per errore i valori di alcune voci in un database.

Tre cose vengono subito in mente:

Uno, il sistema non ha fallito in maniera sicura. Quest'unico errore sembra abbia generato una serie di altri errori in cascata, dato che il nuovo totale fiscale ha cambiato immediatamente i bilanci di "18 unità fiscali governative".

Due, non sono stati fatti controlli di base sul sistema. "È stato chiesto alla città di Valparaiso e alla Valparaiso Community School Corp. di restituire 2,7 milioni di dollari". Il comune non si è domandato innanzitutto da dove venivano tutti quei soldi?

Tre, i meccanismi di controllo degli accessi nel sistema informatico erano troppo tolleranti. Quanto un utente viene autenticato per utilizzare il programma "R-E-D", egli non dovrebbe avere automaticamente il permesso di utilizzare anche il programma "R-E-R". L'autenticazione non è un sistema tutto-o-nulla, dovrebbe essere granulare nei confronti dell'operazione.

<http://cnews.canoe.ca/CNEWS/WeirdNews/2006/02/10/1436417-ap.html>

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

Le compagnie di carte di credito e l'agenda di priorità

Un tizio strappa un modulo di richiesta per una carta di credito, lo ricomponne aggiustandolo con del nastro adesivo, lo compila indicando l'indirizzo di un'altra persona e un numero di telefono diverso, e lo spedisce. Ottiene comunque una carta di credito.

Immaginate per un momento che un frodatore rovesti fra i vostri rifiuti e trovi un modulo di richiesta per una carta di credito stracciato. Ecco perché tutto questo è sbagliato.

Per capire perché questo avvenga, occorre comprendere i compromessi e l'agenda di priorità. Dal punto di vista della compagnia di carta di credito, i benefici nell'offrire una carta di credito derivano dal fatto che la persona la utilizzerà e genererà entrate. Il rischio è che si tratti di un frodatore che costerà denaro alla compagnia. L'industria delle carte di credito ha affrontato tale rischio in due modi: spingendo molti dei rischi sui commercianti, e implementando sistemi di rilevamento frodi per limitare i danni.

Tutti gli altri costi e i problemi legati al furto di identità sono interamente a carico del consumatore; rappresentano un'esternalità per la compagnia di carta di credito. Non rientrano affatto nella decisione di compromesso.

Possiamo ridere di questa cosa finché vogliamo, ma è a tutti gli effetti nei migliori interessi dell'industria delle carte di credito inviare carte in risposta a moduli di richiesta strappati e giuntati senza effettuare molti controlli sull'indirizzo o sul numero di telefono. Se vogliamo che questo cambi, occorre sistemare l'esternalità.

<http://www.cockeyed.com/citizen/creditcard/application.shtml>

** *** *****

Le News di Counterpane

Counterpane e MessageLabs hanno rilasciato un rapporto congiunto sulle tendenze degli attacchi:

<http://www.counterpane.com/pr-20060313.html>

Il rapporto:

<http://www.counterpane.com/dl/attack-trends-2005-messagelabs.pdf>

TippingPoint diventa partner di Counterpane:

<http://www.crn.com/sections/security/security.jhtml?articleId=181500683>

> oppure <http://tinyurl.com/e5rax>

Schneier intervorrà alla Software Development Conference a Santa Clara il 15 marzo:

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

Schneier intervorrà allo IDC IT Security Roadshow a Istanbul, Praga e Varsavia (21-28 marzo):

http://www.idc-cema.com/?showproduct=28039&content_lang=ENG

http://www.idc-cema.com/?showproduct=28034&content_lang=ENG

http://www.idc-cema.com/?showproduct=28036&content_lang=ENG

Schneier intervorrà al Rochester Institute of Technology il 7 aprile:

http://www.gccis.rit.edu/index.php3?dir=sidebar/&var=summary_of_DLS

L'informazione, l'educazione, sono modi per affrontare il problema, ma hanno i loro limiti. Sono sicuro che queste banche hanno attuato campagne di informazione sulla sicurezza, solo che non hanno avuto sufficiente presa. La punizione è un'altra forma di educazione, e presumo che possa essere più efficace. Se le banche licenziassero chiunque sia cascato nel trucco del CD-ROM, si può stare sicuri che una cosa del genere non accadrebbe una seconda volta (almeno fino a quando non cadrà nel dimenticatoio). Ma una risoluzione simile non verrà presa, perché avrebbe pesanti ripercussioni sul morale nel luogo di lavoro.

Invece di incolpare gli utenti per questo tipo di comportamento, sarebbe preferibile concentrarsi sulla tecnologia. Perché l'utente medio di una banca ha bisogno della capacità di poter installare software da un CD-ROM? Perché il computer non blocca questa azione, o non ne dà un resoconto al reparto IT? I computer devono essere sicuri a prescindere da chi vi si siede davanti e da come li usa.

Se vado nel seminterrato e cerco di riparare il sistema di riscaldamento di casa mia, probabilmente andrò contro ogni genere di norma di sicurezza, provocando danni a me stesso e al sistema. Non ho esperienza per queste cose, e onestamente cercare di educarmi in questi ambiti è inutile. Ma il sistema di riscaldamento di casa mia funziona benissimo senza che io debba imparare ogni cosa sul suo funzionamento. So come regolare il termostato, e so di dover chiamare un tecnico nel caso qualcosa si guasti.

I computer dovrebbero funzionare sempre di più in questo modo.

<http://software.silicon.com/security/0,39024655,39156503,00.htm>

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

La sicurezza dei porti statunitensi e i mandatarî

Ha senso affidare la gestione, sicurezza compresa, di sei porti statunitensi a un'azienda con sede a Dubai? Questo interrogativo ha innescato un dibattito animato fra l'amministrazione e il Congresso, dato che i membri di entrambi i partiti hanno condannato l'accordo.

Molta della retorica è puro atteggiamento politico, ma la controversia presenta al suo interno un'interessante problematica di sicurezza. Essa riguarda i mandatarî, la fiducia e la trasparenza.

Ho trattato il concetto di mandatario (proxy) nel mio libro "Beyond Fear". Si tratta di una persona o di un'organizzazione che agisce per nostro conto in qualche modo. Così funzionano le società complesse: è impossibile occuparsi di tutto e prendere ogni decisione, così cediamo una parte di autorità ai mandatarî.

Che si tratti del cuoco al ristorante dove state mangiando, dei fornitori che permettono alla vostra attività di prosperare, o del vostro governo, i mandatarî sono ovunque. Medici, agenti di borsa, catene alberghiere e regolatori governativi come la FDA e la FAA, sono tutti mandatarî.

A volte i mandatarî agiscono in nostro nome semplicemente perché non è possibile occuparci di tutto. Ma più spesso ci serviamo di questi mandatarî perché non abbiamo l'esperienza per svolgere un certo lavoro.

Gran parte della sicurezza funziona attraverso mandatarî. Non abbiamo sufficiente esperienza per prendere decisioni in merito alla sicurezza

aerea, alla copertura delle forze dell'ordine, e alla prontezza dell'esercito, quindi ci affidiamo ad altri. Tutti ci auguriamo che i nostri mandatari prendano le decisioni che prenderemmo noi, ma la nostra unica scelta è quella di fidarci, anzi di affidarci letteralmente ai nostri mandatari.

Ecco il paradosso: pur essendo costretti ad affidarci a loro, possiamo fidarci o non fidarci di loro. Quando ci fidiamo dei nostri mandatari, questa fiducia è frutto di vari elementi: a volte è dettata dall'esperienza con loro, altre volte da raccomandazioni di una fonte fidata. Altre volte ancora deriva da verifiche di terzi, affiliazioni in società professionali o semplicemente istinto. Ma quando si tratta del governo, la fiducia si basa sulla trasparenza. Più il nostro governo si affida alla segretezza, più siamo costretti a "fidarci e basta", e quindi in realtà ci fidiamo di meno.

La sicurezza dei porti statunitensi coinvolge moltissimi mandatari. Noi, i cittadini, abbiamo affidato l'autorità di mandatari ai pubblici ufficiali che abbiamo eletto. Essi hanno emanato delle leggi, il Maritime Transportation Security Act (una legge USA) e gli International Ship and Port Facility Security (ISPS) codes, che regolano la sicurezza in questi porti, e hanno affidato alla Guardia Costiera (un altro mandatario) il compito di farle rispettare.

Quegli stessi pubblici ufficiali eletti (o forse altri ufficiali, attraverso qualche altro mandatario burocratico) hanno assunto un ulteriore mandatario, una compagnia del Regno Unito chiamata Peninsular and Oriental Steam Navigation Company (P&O), per gestire i porti di New York, New Jersey, Philadelphia, Baltimore, Miami e New Orleans.

E ora i dirigenti della P&O, agendo in qualità di mandatari degli azionisti della compagnia, hanno accettato di essere assorbiti da ancora un altro mandatario: Thunder FZE, essa stessa sussidiaria di un'altra compagnia chiamata Dubai Ports World, un'azienda che ha sede negli Emirati Arabi Uniti.

Un altro mandatario, il Committee on Foreign Investment (Comitato per gli Investimenti Esteri) degli Stati Uniti, parte del Dipartimento del Tesoro, ha approvato la vendita. E infine, sia P&O sia Thunder FZE assumono migliaia di mandatari - impiegati, fornitori e partner - per svolgere il lavoro vero e proprio nei vari porti in cui operano.

È una rete di mandatari molto complicata, ma è il sistema a essere complicato. Non è facile, da parte nostra, fidarci di esso perché molto viene coperto dal segreto. Non sappiamo che genere di sicurezza abbiano tali porti. Sentiamo frammenti come "solo il 5% dei carichi in entrata viene ispezionato", ma non sappiamo niente di più. Leggiamo che gli aspetti della sicurezza della vendita di P&O sono stati "rigorosamente presi in esame", e poi che la disamina è stata "affrettata e superficiale".

Non sappiamo che genere di sicurezza vi sia negli Emirati Arabi Uniti, alla Dubai Ports World o presso la sussidiaria che sta svolgendo il lavoro vero e proprio. Non abbiamo altra scelta se non quella di affidarci a questi mandatari, e allo stesso tempo non abbiamo basi sulle quali poterci fidare di loro.

Retorica a parte, questo è il punto di vista di tutti. Vi è chi non si fida dell'amministrazione Bush e ritiene che i suoi intenti siano politici. Vi è chi non si fida degli Emirati Arabi Uniti per i loro legami con il terrorismo (due dei terroristi dell'11 settembre e parte dei finanziamenti per l'attacco provenivano da quella nazione) e chi non si fida sulla base di pregiudizi razziali. Vi è chi non si fida 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.