

CRYPTO-GRAM
15 marzo 2008

Scritta da Bruce Schneier
Fondatore e CTO di BT Counterpane

Edizione italiana curata da Communication Valley SpA
<<http://www.communicationvalley.it/>>

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

Per consultare i numeri arretrati, o per iscriversi, andare all'indirizzo:
<<http://www.schneier.com/crypto-gram.html>>.

Oppure si può leggere il presente numero direttamente sul Web, all'indirizzo:
<<http://www.schneier.com/crypto-gram-0703.html>>.

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier "Schneier on Security": <<http://www.schneier.com/blog>>.

Crypto-Gram è anche consultabile in formato RSS.

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

In questo numero:

- Privacy e potere
- Israele implementa il sistema IFF per i voli commerciali
- News
- Le informazioni controllate da terze parti
- Amtrak inizierà a effettuare lo screening dei passeggeri
- Le news su Schneier/BT Counterpane
- Il Canile: Drecom
- Prodotti di sicurezza: le Suite o i migliori della categoria?
- Commenti dei lettori

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

Privacy e potere

Quando parlo e scrivo di privacy, mi viene regolarmente presentata l'obiezione della divulgazione reciproca di informazioni. Spiegata in libri quali "The Transparent Society" [La Società Trasparente] di David Brin, tale obiezione si può riassumere così: in un mondo di sorveglianza continua e onnipresente, voi saprete tutto di me, ma allo stesso tempo io saprò tutto di voi. Il governo ci osserverà, ma al contempo noi osserveremo il governo. È una situazione diversa rispetto al passato, ma non è automaticamente peggiore. E dato che conosco i tuoi segreti, tu non puoi usare i miei come arma contro di me.

Questa potrebbe non essere l'idea di utopia che tutti abbiamo in mente (e di certo non affronta il valore intrinseco della privacy), ma tale teoria può essere molto attraente, e può venire facilmente scambiata per una soluzione al problema della continuata erosione della privacy da parte della tecnologia. Solo che non funziona, perché ignora la fondamentale diversità di potere.

Non è possibile stimare il valore di privacy e divulgazione senza tenere in conto dei relativi livelli di potere di chi divulga informazioni e di chi riceve le informazioni divulgate.

Se io rivelo informazioni a te, il tuo potere nei miei confronti aumenta. Un sistema per risolvere questo squilibrio di potere è che, allo stesso modo, tu riveli delle informazioni a me. Entrambi avremo meno privacy, ma l'equilibrio di potere verrà mantenuto. Ma questo meccanismo fallisce miseramente se i nostri livelli di potere sono differenti sin dall'inizio.

Un esempio chiarificatore. Venite fermati da un agente di polizia, che vuole che gli mostriate un documento di identità. Rivelare la vostra identità darà all'agente un'enorme quantità di potere su di voi. Egli potrà effettuare ricerche nei database della polizia utilizzando le informazioni sul vostro documento; egli potrà aprire un file su di voi; o potrebbe persino aggiungere il vostro nome a questa o quella watch list antiterrorismo segreta. Chiedere all'agente che in cambio vi mostri il suo documento di identità non vi darà lo stesso tipo di potere su di lui/lei. Lo squilibrio fra i due poteri è troppo grande e non verrà colmato dalla divulgazione reciproca di informazioni.

Potete pensare al potere che già avete come all'esponente in un'equazione che determina il valore (per voi) di maggiori informazioni. Più potere avete, più potere ricaverete dai nuovi dati.

Altro esempio: quando il vostro medico vi dice "si spogli", non ha senso rispondere "prima lei, dottore". La vostra non è un'interazione fra pari.

Questo è il principio che dovrebbe guidare chi ha il compito di prendere decisioni quando si considera l'installazione di telecamere di sorveglianza o il lancio di programmi di data mining. Non è sufficiente aprirsi al pubblico scrutinio. Tutti gli aspetti del governo funzionano meglio quando il potere relativo fra governatori e governati rimane il minore possibile, ovvero quando il livello di libertà è alto e il livello di controllo basso. La trasparenza imposta al governo riduce il differenziale di potere relativo fra le due parti, ed è generalmente una buona cosa. La trasparenza imposta alla gente aumenta il potere relativo, ed è generalmente una cosa negativa.

Il 17enne Erik Crespo fu arrestato nel 2005 in quanto implicato in una sparatoria in un ascensore a New York. Non vi è dubbio che sia stato lui a sparare: è stato registrato dalle telecamere di sorveglianza. Ma Crespo dichiarò che mentre veniva interrogato dal detective Christopher Perino, questi cercò di convincerlo a non richiedere un avvocato, e gli disse che avrebbe dovuto firmare una confessione prima di poter vedere un giudice.

Perino negò sotto giuramento; negò addirittura di aver interrogato Crespo. Ma Crespo aveva ricevuto un lettore MP3 come regalo di Natale, e di nascosto aveva registrato l'interrogatorio. La difesa portò come prova una trascrizione della conversazione e un

CD. Poco dopo l'accusa offrì a Crespo un accordo migliore di quello precedentemente offerto (sette anni di reclusione invece di quindici). Crespo accettò l'accordo e Perino fu accusato di spergiuro in separata sede.

Senza quella registrazione era la parola del detective contro quella di Crespo. E chi avrebbe creduto alla parola di un sospetto omicida contro la parola di un detective della polizia di New York? Quello squilibrio di potere è stato ridotto soltanto perché Crespo è stato abbastanza furbo da premere il pulsante di registrazione sul suo lettore MP3. Perché non vengono effettuate delle registrazioni di tutti gli interrogatori? Perché gli imputati non hanno diritto a che vengano eseguite, così come hanno il diritto di avere un avvocato d'ufficio? Per proteggersi, la polizia registra periodicamente i controlli al traffico dalle proprie volanti; quelle videoregistrazioni non dovrebbero fermarsi una volta che la persona fermata non è più una minaccia.

Ha senso utilizzare le telecamere per riprendere la polizia, come ha senso metterle negli uffici in cui i legislatori si incontrano con gli esponenti delle lobby, e in qualsiasi luogo in cui i funzionari governativi hanno potere sulla gente. Hanno senso anche le leggi per un governo trasparente, che mettono a disposizione dell'opinione pubblica gli archivi governativi e le riunioni dei vari organi di governo. Tutte queste cose promuovono la libertà.

Programmi di sorveglianza totale che colpiscono tutti, senza fondati elementi di prova e senza mandati, come i programmi di intercettazione illegale della National Security Agency, o le varie proposte di monitorare tutto quel che passa su Internet, promuovono il controllo. E nessuno è al sicuro in un sistema politico di controllo.

Il valore intrinseco della privacy:

<<http://www.schneier.com/essay-114.html>>

La vicenda di Erik Crespo:

<<http://www.nytimes.com/2007/12/08/nyregion/08about.html>>

<<http://abcnews.go.com/TheLaw/wireStory?id=3968795>>

Le telecamere filmano un poliziotto:

<[http://www.officer.com/web/online/Top-News-Stories/Cameras-Turn-Lens-on-Police-Activities-/1\\$40169](http://www.officer.com/web/online/Top-News-Stories/Cameras-Turn-Lens-on-Police-Activities-/1$40169)> oppure <<http://tinyurl.com/2ltqcy>>

Sicurezza e controllo:

<<http://www.schneier.com/essay-203.html>>

Questo articolo è originariamente apparso su Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306> oppure <<http://tinyurl.com/2xrcnn>>

Commento/risposta di David Brin.

<http://www.wired.com/politics/security/news/2008/03/brin_rebuttalj>

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

Israele implementa il sistema IFF per i voli commerciali

Israele sta implementando un sistema IFF ('Identification, Friend or Foe', ossia Identificarsi: Amico o Nemico) per i voli commerciali, allo scopo di distinguere aerei legittimi da aerei controllati da terroristi.

L'articolo dà a intendere che si tratti di un semplice sistema di challenge-response (stimolo-risposta). La torre di controllo invia un qualche codice alfanumerico al velivolo. Il pilota inserisce il codice alfanumerico (challenge) in un dispositivo portatile che legge e trasmette la risposta (response). Si ottiene così un'autenticazione mediante 1) il possesso fisico del dispositivo e 2) l'inserimento di un PIN corretto nel dispositivo per attivarlo.

L'articolo parla anche di un segnale di soccorso, che il pilota invia per avvertire che un terrorista gli sta puntando una pistola. Probabilmente lo si attiva inserendo un codice PIN speciale nel dispositivo e nell'inviare quanto visualizzato sullo schermo.

L'esercito ha utilizzato questo tipo di sistema (prima su carta, poi mediante computer) per decenni. Il problema fondamentale nell'utilizzo di tale sistema su un volo commerciale è come comportarsi in caso di errore umano. Il sistema deve essere sufficientemente semplice da usarsi e l'hardware difficile da smarrire, così da evitare troppi falsi allarmi.

<<http://www.haaretz.com/hasen/spages/926626.html>>

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

News

Un'arma a onde sonore:

<<http://blog.wired.com/defense/2008/02/i-was-a-puke-ra.html>>

Nota per la TSA: l'inventore non ha avuto alcun problema a portare questo dispositivo sugli aerei.

Questa è una storia di reati minori e di furto di identità, ma anche una storia incredibile e affascinante sull'ingegneria sociale. Funziona anche in luoghi che tengono la sicurezza in grande considerazione.

<<http://www.washingtoncitypaper.com/display.php?id=34552>>

Di tanto in tanto rispunta il concetto idiota di worm benigno. Stavolta proviene da un gruppo di ricercatori Microsoft nel Regno Unito:

<http://www.schneier.com/blog/archives/2008/02/benevolent_worm_1.html>

La risposta di Microsoft:

<http://www.infoworld.com/article/08/02/19/Microsoft-scrambles-to-quash-friendly-worm-story_1.html> oppure <<http://tinyurl.com/34mtmb>>

Questa vicenda è vecchia di un anno e mezzo, ma le lezioni che se ne possono ricavare, sull'investimento di denaro sulle minacce di sicurezza sbagliate, sono ancora valide:

<<http://www.wthr.com/Global/story.asp?S=4934988>>

Vi sono un paio di cose interessanti in merito al dirottamento avvenuto lo scorso mese in Nuova Zelanda. Prima di tutto si è trattato di un dirottamento tradizionale. Ricordate che dopo l'11 settembre si era detto che l'epoca dei dirottamenti aerei era finita, e che non sarebbe più stato possibile dirottare un aereo e chiedere un riscatto o il raggiungimento di qualche lontano luogo esotico? Pare che non sia vero: possono ancora esserci dei dirottamenti tradizionali senza terroristi.

<http://www.nzherald.co.nz/section/1/story.cfm?c_id=1&objectid=10491291>

<<http://www.stuff.co.nz/4392665a11.html>>

<<http://www.stuff.co.nz/4395723a10.html>>

<<http://www.stuff.co.nz/4395846a11.html>>

L'altro elemento interessante è che la copertura dei media si è comportata di conseguenza. Andate a leggere i link qui sopra. Sono articoli calmi e ragionati. Non si fa menzione della parola 'Terrorismo'. Nessun avvertimento che stiamo tutti per morire. Se non altro raccomandano a tutti di non lasciarsi trasportare da reazioni eccessive. Davvero una boccata d'aria fresca.

<<http://stuff.co.nz/4414911a10.html>>

Continuano i progressi: un intero articolo su un ordigno esplosivo a Times Square e nessuna menzione della parola 'Terrorismo'.

<http://news.yahoo.com/s/ap/20080306/ap_on_re_us/times_square_shutdown>

I registri sanitari sono tremendamente insicuri, e costantemente minacciati dai criminali, ma credo che metterla sul piano della sicurezza naturale sia iperbolico.

<http://www.schneier.com/blog/archives/2008/02/foreign_hackers.html>

Le Poste Statunitensi stanno costruendo un database che permetterà alle persone di tracciare la corrispondenza commerciale attraverso il sistema.

<<http://www.washingtonpost.com/wp-dyn/content/article/2008/02/17/AR2008021701801.html?hpid=sec-tech>> oppure

<<http://tinyurl.com/2arcjy>>

Quel che l'articolo non riporta è che adesso il governo avrà un database che mostra da quali aziende tutti riceviamo comunicazioni per posta.

Attacco 'cold-boot' contro la crittografia di un disco: un attacco hardware davvero brillante che recupera le chiavi dalla DRAM:

<<http://www.freedom-to-tinker.com/?p=1257>>

<<http://citp.princeton.edu.nyud.net/pub/coldboot.pdf>>

<<http://citp.princeton.edu/memory/>>

<http://www.news.com/8301-13578_3-9876060-38.html>

<<http://blog.wired.com/27bstroke6/2008/02/researchers-dis.html>>

Qui viene illustrato un problema di sicurezza generale: è molto difficile proteggere i dati quando l'aggressore ha il controllo fisico della macchina in cui i dati vengono conservati.

<<http://www.schneier.com/essay-142.html>>

Le istruzioni su come fare, con tanto di figure:

<http://content.techrepublic.com.com/2346-1009_11-189078.html>

Nuova analisi crittografica di A5/1 (l'algoritmo utilizzato nei cellulari GSM). Le novità di questo attacco sono: 1) è completamente passivo, 2) il costo totale dell'hardware necessario è di circa mille dollari, e 3) il tempo necessario a rompere la chiave è di circa 30 minuti.

È impressionante. E dimostra una massima crittografica importante: gli attacchi, col tempo, migliorano; non peggiorano. Ecco perché tendiamo ad abbandonare un algoritmo al primo segno di vulnerabilità: sappiamo che, col tempo, le vulnerabilità verranno sfruttate in maniera più efficiente per eseguire attacchi migliori e più veloci.

<http://www.schneier.com/blog/archives/2008/02/cryptanalysis_o_1.html>

Ho già parlato di codici segreti incorporati nelle stampanti laser. Pare che tali codici possano violare le leggi europee sulla privacy.

<http://www.theregister.co.uk/2008/02/15/secret_printer_tracking_dots/>

<<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/02/18/wpriv118.xml>

> oppure <<http://tinyurl.com/3xqw6o>>

<http://www.schneier.com/blog/archives/2005/10/secret_forensic.html>

Una ricerca interessante sulla distribuzione del malware:

<http://www.schneier.com/blog/archives/2008/02/research_on_mal.html>

Questo non sorprende: la paura di predatori in Internet è in gran parte infondata.

<<http://www.mcclatchydc.com/homepage/story/28029.html>>

<<http://pogue.blogs.nytimes.com/2008/02/28/assessing-the-dangers-of-the-internet-for-children/>> oppure <<http://tinyurl.com/2kqtk6>>

<http://www.schneier.com/blog/archives/2008/02/fear_of_internet.html>

Altri isterismi in merito a un esplosivo liquido:

<<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/02/26/nbomb126.xml>

!> oppure <<http://tinyurl.com/39basa>>

<http://www.channel4.com/video/checking-in-to-airport-chaos/series-1/episode-3/explosive-combination_p_1.html> oppure <<http://tinyurl.com/ynrwh3>>

Un ottimo intervento che riporta il buonsenso:

<http://www.theregister.co.uk/2008/02/26/gilligan_bomb_terror_liquid_again/>

oppure <<http://tinyurl.com/2wffmh>>

<http://www.theregister.co.uk/2006/08/17/flying_toilet_terror_labs/>

Una macchina a raggi X di sicurezza aeroportuale giocattolo per bambini:

<http://lifesinventions.com/index.cfm?fuseaction=product.display&Product_ID=2385&CFID=17420493&CFTOKEN=53095688> oppure <<http://tinyurl.com/2d48ln>>

Mi ricorda il checkpoint di sicurezza Playmobil:

<<http://www.amazon.com/Playmobil-3172-Security-Check-Point/dp/B0002CYTL2>>

oppure <<http://tinyurl.com/2vz3ua>>

In "Underlying Reasons for Success and Failure of Terrorist Attacks: Selected Case Studies" [I motivi principali del successo e del fallimento degli attacchi terroristici: casistica selezionata] (Homeland Security Institute, Giugno 2007), gli autori prendono in esame otto recenti complotti terroristici contro aerei commerciali e treni passeggeri, e giungono a interessanti conclusioni. Mi piace soprattutto il seguente passaggio, che fa eco a ciò che vado sostenendo da tempo: "Un fenomeno è particolarmente notevole: è raro che dei terroristi vengano catturati durante la fase di esecuzione di un'operazione, a parte nei casi in cui la loro attrezzatura o le loro armi abbiano dei problemi. Molto spesso, invece, i complotti vengono scoperti durante le fasi precedenti l'esecuzione". Intelligence, investigazioni e risposta alle emergenze: ecco in cosa dovremmo investire il denaro per l'antiterrorismo. Difendere i bersagli è raramente la risposta corretta.

<http://www.homelandsecurity.org/hshireports/Reasons_for_Terrorist_Success_Failure.pdf> oppure <<http://tinyurl.com/2u8ft3>>

<http://www.schneier.com/blog/archives/2008/02/why_some_terror.html>

Ancora guerra all'Imprevisto: l'aeroporto di Los Angeles è stato evacuato per due ore a causa di un commento sospetto.

<<http://www.msnbc.msn.com/id/23216544/>>

<<http://www.knbc.com/news/15331048/detail.html>>

Un articolo affascinante su come i bambini imparano a mentire. (Forse esula un poco dall'argomento sicurezza, ma non ne sono tanto convinto, viste le mie varie letture sulla psicologia della sicurezza).

<<http://www.nymag.com/news/features/43893>>

Due usi efficaci per i chip RFID: inventariare automaticamente gli utensili che un camion sta trasportando e ritrovare i bagagli che sono finiti in un altro aeroporto. Visto? Nessuna tecnologia è interamente buona o cattiva.

<http://www.boston.com/cars/news/articles/2008/02/11/rfid_equipped_pickups_wont

[let_tools_go_missing/](http://www.boston.com/cars/news/articles/2008/02/11/rfid_equipped_pickups_wont)> oppure <<http://tinyurl.com/37acl2>>

<<http://news.bbc.co.uk/1/hi/uk/7242620.stm>>

Nuova versione (5.1) di TrueCrypt, il software open source di crittografia per dischi.

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

Da anni sappiamo tutti che è possibile utilizzare Google per effettuare scansioni di vulnerabilità. Beh, ora il processo è stato automatizzato: Goolag Scanner, prodotto da the Cult of the Dead Cow. Ho visto parecchi risultati di scansioni fatte con una versione pre-release del software, e ciò che questi tizi hanno trovato è incredibile.

<[http://www.eweek.com/index2.php?option=content&task=view&id=46520&pop=1&hide](http://www.eweek.com/index2.php?option=content&task=view&id=46520&pop=1&hide_ads=1&page=0&hide_js=1)

[de_ads=1&page=0&hide_js=1](http://www.eweek.com/index2.php?option=content&task=view&id=46520&pop=1&hide_ads=1&page=0&hide_js=1)> oppure <<http://tinyurl.com/2rtmkj>>

<[http://www.networkworld.com/news/2008/022208-hackers-turn-google-into-](http://www.networkworld.com/news/2008/022208-hackers-turn-google-into)

[vulnerability.html](http://www.networkworld.com/news/2008/022208-hackers-turn-google-into)> oppure <<http://tinyurl.com/346ysd>>

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

Quando ho scritto l'articolo "Ritratto del Terrorista Moderno da Idiota", ho pensato molto all'idea che il governo si inventi terroristi cospiratori per poi intrappolarli, così da far sembrare il mondo più pericoloso e spaventoso. Sin da allora è rimasta nel mio elenco di argomenti da trattare in futuro. Il "Rolling Stone" ha questo eccellente articolo sul tema, che parla delle Joint Terrorism Task Forces negli Stati Uniti.

<http://www.rollingstone.com/politics/story/18137343/the_fear_factory>

Il mio articolo:

<<http://www.schneier.com/essay-174.html>>

SurveillanceSaver, un salvaschermo che mostra immagini in diretta prese da telecamere di sorveglianza in tutto il mondo:

<<http://code.google.com/p/surveillancesaver/>>

Un ottimo articolo sul rischio di sapere troppe cose sui rischi. Leggetelo tutto:

<<http://www2.csoonline.com/exclusives/column.html?CID=33571>>

Gangsta rap della TSA. Divertente.

<<http://www.youtube.com/watch?v=z7AWw7t5zj0>>

Una storia davvero strana sulla 'borsa per portatile ideale' della TSA. Sembra che la TSA creda che siamo tutti disposti a ridisegnare le nostre vite basandoci sui loro checkpoint di sicurezza.

Personalmente, preferisco avere una borsa per portatile che sia utile a me in ogni occasione e non che sia utile alla TSA quando volo. E passo da un checkpoint di sicurezza circa due volte alla settimana.

<<http://gsnmagazine.com/cms/features/news-analysis/542.html>>

Il video del mio intervento sulle tecnologie a duplice uso alla conferenza CPSR's Technology in Wartime.

<http://www.archive.org/details/Bruce_Schneier.Dual_Use_Technologies>

Non saprei quanto sia grave il fatto che siano spariti 122 badge di ispettore di sicurezza della FAA, ma la cosa mi diverte ugualmente:

<<http://www.nbc5i.com/travelgetaways/15508460/detail.html>>

Dunque, ve ne state seduti in casa con gli amici, giocando a World of Warcraft. Uno di voi si domanda: "Come possiamo FARCI PAGARE per fare questo?" Un altro dice: "Io lo so: facciamo finta di combattere il terrorismo, e poi otteniamo una sovvenzione dal governo".

"Dopo aver completamente eliminato il terrorismo nel mondo reale, la comunità dell'intelligence statunitense sta lavorando allo sviluppo di un software che rileverà gli estremisti più violenti infiltrati in World of Warcraft e altri giochi online di massa, secondo un rapporto di data mining del Direttore della National Intelligence". Cose del genere non si possono inventare di sana pianta.

<<http://blog.wired.com/27bstroke6/2008/02/nations-spies-w.html>>

<<http://news.bbc.co.uk/1/hi/technology/7274377.stm>>

<<http://www.crispygamer.com/comics/backward/2008-03-03.aspx>>

I tribunali tedeschi si sono pronunciati in merito alla legalità delle operazioni di spionaggio nel cyberspazio da parte della polizia. Ottimo materiale.

<http://www.schneier.com/blog/archives/2008/03/german_courts_r.html>

Un articolo molto interessante in merito all'hacking di dispositivi medici impiantati nel paziente. Un numero sempre maggiore di essi contiene piccoli computer e comunica mediante radiofrequenze.

<http://www.schneier.com/blog/archives/2008/03/hacking_medical_1.html>

Ross Anderson, Rainer Böhme, Richard Clayton e Tyler Moore hanno pubblicato un importante rapporto su sicurezza ed economia: "Security, Economics, and the Internal Market" [Sicurezza, Economia e il mercato interno], pubblicato dall'ENISA (European Network and Information Security Agency).

<http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf>

oppure <<http://tinyurl.com/35ao58>>

Hackerare fisicamente macchine Windows via Firewire:

<http://www.darkreading.com/document.asp?doc_id=147713&f_src=drweekly>

La crittografia totale del disco pare essere l'unica difesa in questo caso.

Un articolo sui furti nelle librerie:

<<http://www.thestranger.com/seattle/Content?oid=520472>>

La smart card della Metropolitana di Londra è stata craccata. La crittografia pare proprio penosa.

<http://www.schneier.com/blog/archives/2008/03/london_tube_sma.html>

Articolo interessante di Popular Mechanics sulle telecamere di sorveglianza: vengo citato in più punti.

<http://www.popularmechanics.com/technology/military_law/4236865.html>

E questo articolo parla di osservare chi osserva:

<http://www.popularmechanics.com/technology/military_law/4237005.html>

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

Le informazioni controllate da terze parti

Wine Therapy è una bacheca online per appassionati di vini. È attiva dal 2000 e il suo database di post e commenti archiviati è una miniera di informazioni: note di assaggio, guide ai ristoranti, aneddoti, e così via. Sul finire dello scorso anno qualcuno si è introdotto nel software del forum, ha ottenuto privilegi di amministratore e ha cancellato il database. Non esisteva alcun backup.

Naturalmente il proprietario del forum avrebbe dovuto fare copie di backup, ma è stato gravemente malato per tutto l'anno passato e non ha potuto. E l'Internet Archive è stato utile solo in parte.

Sempre più di frequente, le informazioni a cui ci affidiamo (che siano state create da noi o da altri) si trovano fuori dal nostro controllo. Sono là fuori, in Internet, sul sito Web di qualcun altro, sotto le cure di altri. Ci serviamo di quei siti Web, a volte quotidianamente, e nemmeno pensiamo alla loro affidabilità.

Pezzetti e frammenti del Web spariscono in continuazione. Il fenomeno si chiama 'link rot' (decadimento dei link) e ci siamo tutti abituati. Nel 1999 un amico che stava pianificando un viaggio in Toscana aveva salvato 65 link di informazioni; oggi solo la metà di quei link funziona. All'interno di Crypto-Gram e sul mio blog gli articoli, le notizie e i siti Web a cui faccio riferimento con un link spariscono regolarmente.

Può essere a causa delle regole di un sito (alcuni quotidiani conservano gli articoli solo per due settimane sui loro siti), oppure per i motivi più vari: le posizioni ufficiali di un politico spariscono dal suo sito Web dopo aver cambiato idea in merito a una questione; parte della letteratura aziendale può svanire dal sito Web di una compagnia dopo una situazione imbarazzante, e così via. Il caso estremo di link rot è la 'morte di un sito', in cui interi siti Web cessano di esistere: siti delle Olimpiadi o dei Mondiali di calcio una volta che gli eventi sportivi sono terminati, siti di candidati politici dopo le elezioni, siti aziendali quando cessano i finanziamenti, ecc.

Nella maggior parte dei casi ignoriamo il problema. A volte salvo una copia di un'ottima ricetta di cucina, o di un articolo importante per le mie ricerche, ma spesso confido nel fatto che potrò facilmente ritrovare qualsiasi cosa mi interessi tornando su un sito. Dovessi pianificare un viaggio in Toscana, a ogni modo, farei una ricerca di informazioni importanti oggi e non mi affiderei a un elenco vecchio di nove anni. Nella stragrande maggioranza dei casi, il link rot e la morte di un sito non sono un vero problema.

Questo panorama sta cambiando con il Web 2.0, con siti che si fondano più sulla comunità che sulle informazioni. Noi contribuiamo alla costruzione di questi siti, grazie ai nostri post o ai nostri commenti. Li visitiamo regolarmente ed entriamo in contatto con altri frequenti visitatori. Entrano a far parte della nostro socializzare online e la perdita di questi siti ci tocca in modi differenti, come hanno potuto sperimentare gli utenti di Greatest Journal quando il loro sito è 'morto'.

Pochi, forse nessuno degli utenti che hanno fatto di Wine Therapy la propria 'casa' hanno mantenuto delle copie di backup dei propri post e commenti. Sono certo che non ci hanno nemmeno pensato. Io non ci penso quando pubblico qualcosa sui vari blog, bacheche e forum che frequento. Certo che uno come me dovrebbe pensarci, ma considero questi forum come vere e proprie estensioni del mio computer... finché non spariscono.

Affidandoci a terze parti per il mantenimento dei nostri scritti e delle nostre relazioni online, perdiamo il controllo sulla loro affidabilità. Chiaramente perdiamo anche il controllo sulla loro sicurezza, come hanno potuto vedere gli utenti di MySpace il mese scorso quando è stato caricato su un sito BitTorrent un file di 17 GB contenente mezzo milione di foto che avrebbero dovuto essere private.

Agli albori del Web, ricordo di essermi sentito positivamente frastornato dall'enorme quantità di informazioni disponibili online e dalla facilità con cui era possibile ottenerle. "L'Internet è il mio disco rigido", dicevo agli inesperti. Oggi è ancora più vero: non credo che sarei in grado di scrivere senza questa miniera di informazioni così facilmente accessibili. Ma si tratta di un disco rigido alquanto inaffidabile.

L'Internet è il mio disco rigido, ma soltanto se i miei bisogni sono immediati e le mie richieste possono essere soddisfatte in maniera imprecisa. È stato facile per me cercare informazioni sull'hacking delle foto di MySpace. E sarà semplice cercare e rispondere ai commenti di questo articolo, sia su Wired.com che sul mio sito Web. Wired.com è un'impresa commerciale, quindi esiste un valore pubblicitario nel mantenere accessibile l'intero contenuto. Il mio sito non ha natura commerciale, ma esiste un valore personale nel mantenere accessibile l'intero contenuto. Secondo un'analisi del genere, tutti i siti dovrebbero rimanere su Internet per sempre, anche se di fatto non è vero. L'unica certezza è che non vi è modo di prevedere che cosa scomparirà e quando.

Purtroppo non possiamo farci molto. Le misure di sicurezza, per la maggior parte, non sono nelle nostre mani. Possiamo registrare localmente copie di pagine Web importanti, e copie di qualsiasi cosa pubblichiamo che riteniamo importante. L'Internet Archive è tremendamente prezioso perché conserva pezzi e frammenti di Internet. E di recente abbiamo iniziato a veder comparire strumenti per archiviare informazioni e pagine di siti di social networking. Ma quel che è davvero importante è l'intera comunità, e non sappiamo quali pezzi ci interessano di più finché non sono scomparsi.

Tornando a Wine Therapy, mi SEMBRA che abbia cominciato nel 2000. O forse poteva essere il 2001. Non posso controllare, perché qualcuno ha cancellato gli archivi.

Internet Archive:

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

Greatest Journal:

<<http://dropbeatsnotbombs.vox.com/library/post/farewell-gj-youll-kind-of-be-missed.html>> oppure <<http://tinyurl.com/2t2yg5>>
<<http://barry095.vox.com/library/post/greatest-journal-death.html>>

Altri hack:

<http://www.schneier.com/blog/archives/2005/02/tmobile_hack_1.html>
<http://www.wired.com/politics/security/news/2008/01/myspace_torrent>

Questo articolo è originariamente apparso on Wired.com.

<http://www.wired.com/politics/security/commentary/securitymatters/2008/02/securitymatters_0221> oppure <<http://tinyurl.com/2a4go3>>

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

Amtrak inizierà a effettuare lo screening dei passeggeri

Amtrak inizierà a effettuare controlli casuali dei passeggeri, nel tentativo di colmare il divario di messinscena di sicurezza che esiste fra treni e aerei.

È piuttosto casuale:

“Le squadre arriveranno senza preavviso alle stazioni e allestiranno checkpoint per il controllo bagagli di fronte ai cancelli di imbarco. I funzionari sceglieranno delle persone a casaccio dalla coda in attesa e passeranno un tampone speciale sui loro bagagli, che verrà poi inserito in una macchina per il rilevamento di esplosivi. Se la macchina segnala qualcosa, i funzionari apriranno il bagaglio per effettuare un’ispezione.

“Chiunque venga selezionato per lo screening e rifiuta di sottoporsi alla procedura non sarà ammesso a bordo e verrà rimborsato delle spese per il biglietto.

“Oltre allo screening, funzionari antiterrorismo con cani anti-bomba pattuglieranno i binari e passeranno fra i treni; di tanto in tanto viaggeranno sui treni”.

Ma questo è il commento più emblematico:

“Non esiste una minaccia specifica nuova o diversa’, ha dichiarato Alex Kummant, direttore esecutivo di Amtrak. ‘Questa è semplicemente la cosa giusta da fare”.

Perché è la cosa giusta da fare? Perché lo fa stare meglio. E questa è esattamente la definizione di messinscena di sicurezza.

<<http://www.forbes.com/afxnewslimited/feeds/afx/2008/02/18/afx4667193.html>>
oppure <<http://tinyurl.com/3688xe>>

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

Le news su Schneier/BT Counterpane

Video di un'intervista con Schneier:

<<http://www.builderau.com.au/news/soa/Schneir-Bad-news-is-good-news-not-so-for-security-/0,339028227,339285999,00.htm>> oppure <<http://tinyurl.com/2jztv4>>

Una mia intervista su Computerworld Hong Kong:

<http://www.cw.com.hk/article.php?id_article=1088>

Un articolo su di me (e un frammento scritto da me):

<http://www.infoworld.com/article/08/02/22/08OP-security-schneier_1.html> oppure <<http://tinyurl.com/2qu9qq>>

Un mio editoriale di opinione sui documenti di identità nazionali pubblicato sul Minneapolis Star Tribune:

<<http://www.startribune.com/opinion/commentary/15891037.html>>

E un breve domanda-e-risposta sempre sulla medesima testata:

<<http://www.startribune.com/opinion/editorials/15891022.html>>

Schneier parlerà sul tema "The Theater of Security" [Il teatro della sicurezza] al Weisman Art Museum il 27 marzo a Minneapolis:

<<http://www.weisman.umn.edu/events/eventscal.php>>

Schneier interverrà alla conferenza Freedom to Connect il primo aprile a Washington, DC.

<<http://freedom-to-connect.net/>>

Schneier interverrà all'InterSystems DEVCON2008 il 2 aprile a Orlando.

<<http://www.intersystems.com/devcon2008/>>

Schneier interverrà alla RSA Conference l'8 aprile a San Francisco.

<<http://www.rsaconference.com/2008/US/Home.aspx>>

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

Il Canile: Drecom

Pubblicizzano una crittografia AES a 128 bit, ma utilizzano XOR.

Questo spiega perché è difficile valutare i prodotti di sicurezza: il diavolo è nei dettagli.

<<http://www.heise-online.co.uk/security/Enclosed-but-not-encrypted--features/110136/0>> oppure <<http://tinyurl.com/2xqv5r>>

<<http://www.easy-nova.de/index.php?siteID=18&productID=28>>

L'URL del post sul mio blog:

<http://www.schneier.com/blog/archives/2008/02/the_doghouse_dr.html>

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

Prodotti di sicurezza: le Suite o i migliori della categoria?

Sappiamo che cosa non va quando acquistiamo una suite di prodotti: un'applicazione sola è ottima, le altre sono mediocri. E sappiamo cosa non va quando acquistiamo i prodotti migliori della categoria: produttori diversi, interfacce diverse, e applicazioni diverse che non interagiscono molto bene fra di esse. L'industria della sicurezza ha altalenato fra le due scelte per un certo tempo, e ora una nuova generazione di professionisti della sicurezza IT riscopre gli svantaggi di ciascuna delle due.

Il vero problema è che nessuna delle due scelte funziona davvero, e continuiamo a convincerci che quella di cui non disponiamo al momento è migliore di quella che abbiamo. E la vera soluzione è acquistare risultati, non prodotti.

In tutta onestà, nessuno vuole comprare la sicurezza informatica. La gente vuole acquistare un qualsiasi prodotto (connettività, una presenza sul Web, un servizio email, applicazioni in rete, ecc.) e vuole che tale prodotto sia sicuro. Che sia obbligata a spendere soldi per la sicurezza informatica è un manufatto della giovinezza dell'industria informatica. E prima o poi il bisogno di acquistare la sicurezza scomparirà.

Scomparirà perché i produttori IT stanno iniziando a rendersi conto che devono offrire sicurezza come parte del prodotto che vendono. Scomparirà perché le organizzazioni stanno iniziando a comprare servizi invece che prodotti, e a pretendere che la sicurezza sia parte di tali servizi. Scomparirà perché l'industria della sicurezza svanirà come categoria di consumo, e verrà invece indirizzata all'industria IT.

L'elemento conduttore essenziale in questo contesto è l'outsourcing. L'outsourcing è l'unificatore definitivo, perché al consumatore non importano più i dettagli. Se io compro i miei servizi di rete da una grande azienda di infrastruttura IT, non mi interessa se protegge la rete installando l'ultima novità in fatto di sistemi antintrusione, configurando i router e i server così da ovviare al bisogno di sicurezza basata sulla rete, o se utilizza della polvere magica donata dai re degli elfi. Io voglio semplicemente un contratto che specifichi un livello e una qualità del servizio, e lascio che il rivenditore si occupi di come ottenerli.

L'IT è infrastruttura. L'infrastruttura viene sempre esternalizzata. E i dettagli su come funziona l'infrastruttura vengono lasciati alle aziende che la forniscono.

Questo è il futuro dell'IT, e quando inizierà a manifestarsi vedremo un tipo di fusione di società che non abbiamo mai visto prima. Invece di assistere all'assorbimento di piccole aziende di sicurezza da parte di grandi compagnie di sicurezza, sia le grandi che le piccole aziende di sicurezza verranno assorbite da compagnie che non si occupano di sicurezza. Sta già accadendo. Nel 2006 IBM ha comprato ISS. Quello stesso anno BT ha assorbito la mia azienda, Counterpane, e lo scorso anno ha acquisito INS. Queste non sono grandi aziende di sicurezza che acquisiscono piccole imprese di sicurezza, ma compagnie che non si occupano di sicurezza che assorbono piccole e grandi aziende di sicurezza.

Se fossi Symantec e McAfee, mi preparerei ad affrontare un compratore.

Queste sono ottime fusioni. Invece di dover scegliere fra una suite di prodotti di scarso livello e una serie di applicazioni, di cui ognuna è la migliore nella propria categoria, ma che non interagiscono bene fra di esse, possiamo ignorare del tutto il problema. Possiamo cercare un fornitore di infrastruttura che troverà il sistema per far funzionare il tutto; non ci interessa come.

Questo articolo è originariamente apparso su "Information Security" come seconda parte di un 'botta e risposta' con Marcus Ranum.

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1303850_idx2,00.html>

L'intervento di Marcus:

<http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1303850,0.html> oppure <<http://tinyurl.com/36zhml>>

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

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul 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 sempre <<http://www.schneier.com/crypto-gram.html>>

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>

I commenti a CRYPTO-GRAM devono essere inviati a schneier@counterpane.com. Si sottintende il permesso di riprodurre tali commenti, salvo indicazione contraria. I commenti possono venire adattati per ragioni di spazio e di chiarezza.

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 BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

BT Counterpane è leader mondiale nella protezione delle informazioni su network - l'inventore del Managed Security Monitoring gestito in outsourcing e la principale autorità nella riduzione efficace delle nuove minacce in ambito IT. BT Counterpane protegge reti per conto di governi e di aziende inserite nella Fortune 1000 a livello mondiale.

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

Crypto-Gram è una newsletter personale. Le opinioni qui espresse non sono necessariamente quelle di BT o di BT Counterpane.

Copyright (c) 2008 - Bruce Schneier.