

CRYPTO-GRAM  
15 ottobre 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:

Le sette abitudini di terroristi altamente inefficaci

Le due categorie di materiali proibiti in aeroporto

News

Più le cose cambiano, più rimangono le stesse

Le intercettazioni senza mandato della NSA prendono di mira americani innocenti

Le news su Schneier/BT Counterpane

Taleb sui limiti della gestione dei rischi

"Nuovo attacco" contro immagini criptate

Adesso gli attivisti non-violenti sono terroristi

La gestione dei rischi ha senso?

Commenti dei lettori

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Le sette abitudini di terroristi altamente inefficaci

La maggior parte delle strategie antiterrorismo non falliscono a causa di problemi tattici, ma per un malinteso di fondo in merito a ciò che spinge in primo luogo i terroristi ad agire. Se vogliamo sconfiggere il terrorismo, dobbiamo comprendere anzitutto che cosa spinge le persone a diventare terroristi.

Secondo il giudizio prevalente, il terrorismo è un fenomeno intrinsecamente politico e si diventa terroristi per ragioni politiche. Questo è il modello "strategico" del terrorismo, e si tratta sostanzialmente di un modello economico. Esso stabilisce che le persone ricorrono al terrorismo quando credono (a ragione o a torto) che ne valga la pena; ovvero, quando ritengono che i vantaggi politici del terrorismo meno i costi politici siano superiori a quanto otterrebbero con una qualsiasi altra forma di protesta più pacifica. Si presume, per esempio, che chi si unisce a Hamas abbia come obiettivo la realizzazione di uno stato palestinese; e chi si unisce al PKK lo faccia per arrivare a ottenere una realtà nazionale curda; e chi si unisce ad al-Qaida voglia, fra le altre cose, cacciare gli Stati Uniti dal Golfo Persico.

Se si crede a questo modello, il sistema per combattere il terrorismo è quello di modificare tale equazione, e ciò è quanto consigliano molti esperti. I governi tendono a ridurre al minimo i guadagni politici del terrorismo mediante una policy che rifiuta ogni concessione. La comunità internazionale tende a consigliare la riduzione delle ingiustizie politiche dei terroristi mediante pacificazione, nella speranza di indurli a rinunciare alla violenza. Entrambi i casi suggeriscono policy che offrano alternative non-violente credibili, come le elezioni libere.

Storicamente, nessuna di queste soluzioni ha funzionato in maniera costante o affidabile. Max Abrahms, un ricercatore predottorato al Center for International Security and Cooperation della Stanford University, ha studiato decine di gruppi terroristici di ogni parte del mondo. Secondo lui quel modello è errato. In uno studio pubblicato quest'anno in *International Security* (che, purtroppo, non ha il titolo "Le sette abitudini di terroristi altamente inefficaci") egli parla, appunto, di sette abitudini di terroristi altamente inefficaci. Queste sette tendenze si riscontrano in organizzazioni terroristiche di tutto il mondo, e contraddicono direttamente la teoria secondo cui i terroristi sono dei massimizzatori politici:

I terroristi -- scrive Abrahms -- (1) attaccano i civili, una linea di condotta che vanta precedenti ben poco efficaci nel convincere quei civili a dare ai terroristi quello che vogliono; (2) trattano il terrorismo come prima risorsa, non come ultima spiaggia; (3) non scendono a compromessi con il paese preso di mira, anche quando quei compromessi sarebbero nei loro migliori interessi da un punto di vista politico; (4) hanno piattaforme politiche proteiformi, che cambiano regolarmente e a volte radicalmente; (5) spesso sferrano attacchi anonimi, che impedisce ai paesi bersagliati di garantire loro delle concessioni politiche; (6) attaccano regolarmente altri gruppi terroristici che hanno la stessa piattaforma politica; e (7) rifiutano la dispersione, anche quando continuano a non raggiungere i loro obiettivi politici o anche dopo aver raggiunto gli obiettivi politici dichiarati.

Abrahms fornisce un modello alternativo per spiegare tutto questo: le persone si rivolgono al terrorismo alla ricerca di solidarietà sociale. Egli teorizza che le persone si uniscono a organizzazioni terroristiche in tutto il mondo per poter essere parte di una comunità, proprio come i ragazzini delle grandi città si uniscono alle gang da strada negli Stati Uniti.

I fatti corroborano questa teoria. I singoli terroristi spesso non hanno mai avuto niente a che fare con l'attività e le priorità di un gruppo terroristico, e frequentemente si uniscono a più gruppi terroristici con piattaforme politiche incompatibili. Molti individui che si uniscono a gruppi terroristici spesso non sono soggetti oppressi in alcun modo, né sanno delineare gli obiettivi politici delle loro organizzazioni. Spesso chi entra a far

parte di un gruppo terroristico ha amici o parenti che già ne sono membri, e la stragrande maggioranza dei terroristi sono isolati socialmente: giovani uomini non sposati o vedove che non avevano un lavoro prima di entrare nel gruppo. Queste caratteristiche si possono riscontrare in gruppi terroristici radicalmente diversi fra loro, come l'IRA e al-Qaida.

Per esempio, molti dei dirottatori dell'11 settembre avevano pianificato di combattere in Cecenia, ma erano sprovvisti della documentazione necessaria, e quindi hanno attaccato l'America. I mujaedin non sapevano chi attaccare dopo che i Russi si ritirarono dall'Afghanistan, per cui se ne sono stati senza far niente finché non hanno trovato un nuovo nemico: l'America. I terroristi pakistani passano regolarmente ad altri gruppi con una piattaforma politica completamente diversa. Molti nuovi membri di al-Qaida dichiarano, con poca convinzione, di aver deciso di diventare parte della jihad dopo aver letto un blog estremista e anti-americano, oppure dopo essersi convertiti all'islamismo, magari solo da qualche settimana. Queste persone sanno ben poco di politica e di islamismo, e francamente non danno l'impressione di voler saperne di più. I blog a cui si riferiscono non sono molto profondi in questi campi, anche se esistono blog assai più ricchi di informazioni.

Tutto ciò spiega le sette abitudini. Non è che siano inefficaci di per sé, solo che hanno un obiettivo differente. Possono non essere efficaci da un punto di vista politico, ma lo sono socialmente, e contribuiscono a preservare l'esistenza e la coesione del gruppo.

Questo genere di analisi non è solo teoria: ha delle conseguenze pratiche per l'antiterrorismo. Non solo ora possiamo comprendere con maggiore chiarezza chi potrebbe diventare un terrorista, ma possiamo mettere a punto delle strategie mirate a indebolire i vincoli sociali all'interno delle organizzazioni terroristiche. Creando disaccordi fra i membri dei gruppi -- convertendo le condanne penali in cambio di informazioni pratiche di intelligence, inserendo un maggior numero di agenti doppi nei gruppi terroristici -- sarà un ottimo sistema per indebolire considerevolmente i vincoli sociali all'interno di quei gruppi.

Occorre anche prestare più attenzione agli emarginati sociali più che ai politicamente oppressi, come tutte quelle comunità non assimilate che vivono in paesi occidentali. Bisogna sostenere e favorire comunità e organizzazioni vivaci e positive come alternative da offrire a potenziali terroristi affinché abbiano quella coesione sociale di cui hanno bisogno. E infine è necessario ridurre al minimo i danni collaterali nelle nostre operazioni antiterrorismo, nonché porre un freno al fanatismo e ai crimini motivati dall'odio, che non fanno altro che creare un maggiore dislocamento e isolamento sociale, e fomentare le inevitabili ritorsioni.

<[http://maxabrahms.com/pdfs/DC\\_250-1846.pdf](http://maxabrahms.com/pdfs/DC_250-1846.pdf)>

Questo articolo è precedentemente apparso su Wired.com.

<[http://www.wired.com/print/politics/security/commentary/securitymatters/2008/10/securitymatters\\_1002](http://www.wired.com/print/politics/security/commentary/securitymatters/2008/10/securitymatters_1002)>

oppure <<http://tinyurl.com/3vf3x5>>

Una confutazione interessante:

<<http://www.cambridgeblog.org/2008/10/can-terror-be-understood/>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## Le due categorie di materiali proibiti in aeroporto

Il mese scorso, il personale di sicurezza ha trovato un vasetto di sugo per pasta nel mio bagaglio. Si trattava di un vasetto da 170 grammi, e superava il limite consentito. L'addetto lo ha confiscato, perché sarebbe stato troppo pericoloso permettermi di portarlo a bordo con me. E per dimostrare quanto considerasse davvero pericoloso quel vasetto, lo ha tranquillamente gettato in un bidone lì accanto, insieme ad altre bottigliette e simili contenitori, e mi ha fatto proseguire.

Vi sono due categorie di materiali proibiti ai checkpoint di sicurezza negli aeroporti: la categoria che vi metterà nei guai se cercate di portarla a bordo di un aereo, e la categoria che vi verrà allegramente sottratta se cercate di portarla a bordo. Questa differenza è importante: obbligare il personale di sicurezza a confiscare qualsiasi cosa appartenga a quella seconda categoria è una perdita di tempo. Non serve ad altro che a danneggiare persone innocenti, e non ferma di certo i terroristi.

Lasciate che vi spieghi. Se venite scoperti in possesso di una pistola o di una bomba dal personale di sicurezza di un aeroporto, gli addetti non si limiteranno a confiscarvele. Chiameranno la polizia e dovrete fermarvi per qualche ora per rispondere a parecchie domande imbarazzanti. Potreste essere arrestati e sicuramente perderete il vostro volo. Nel migliore dei casi, passerete una giornata davvero brutta.

Per questo non mi preoccupano quegli articoli che parlano del fatto che gli screener non scoprono tutte o molte delle armi e delle bombe che passano i checkpoint di sicurezza. Gli screener non devono essere perfetti: basta che siano sufficientemente in gamba. Nessun terrorista metterà al centro dei propri piani il fatto di riuscire a far passare una pistola attraverso la sicurezza aeroportuale se c'è una buona probabilità di essere scoperto, perché in tal caso le conseguenze sarebbero troppo gravi.

Ora si confronti tutto questo con un piano terroristico che richiede una bottiglietta di liquido da 33 cl. Non si hanno prove che i dinamitardi di Londra, con gli esplosivi liquidi, avessero un piano realizzabile, ma assumiamo per un momento che lo avessero. Se dei terroristi imitatori provassero a far passare il loro esplosivo liquido attraverso la sicurezza aeroportuale, e venissero scoperti dal personale addetto -- come è capitato a me con il mio vasetto di sugo per pasta -- i terroristi potrebbero semplicemente provarci di nuovo. Potrebbero continuare a provarci fino a riuscirci. Dato che non vi sono conseguenze nel fare questi tentativi, gli screener devono essere efficaci al 100%. È sufficiente sbagliare una volta su cento e il piano terroristico potrebbe riuscire.

Stesso discorso per gli aghi da uncinetto, per i coltellini tascabili, le forbici, i cavatappi, gli accendini e qualsiasi altro oggetto sia proibito questa settimana. Se il fatto di essere scoperti con un oggetto proibito non porta conseguenze, allora il confiscarlo non serve ad altro che a danneggiare persone innocenti. Nel migliore dei casi può essere una banale seccatura per i terroristi.

Per ovviare al problema, la sicurezza aeroportuale deve fare una scelta. Se qualcosa è pericoloso, lo si tratti come pericoloso, e si tratti la persona che ha quel materiale con sé come soggetto potenzialmente pericoloso. Se non è pericoloso, allora è inutile continuare a requisirlo per tenerlo lontano dagli aerei. Cercare di ottenere entrambe le

cose non fa altro che distrarre gli screener e impedire loro di contribuire alla nostra sicurezza.

<<http://www.cnn.com/2008/US/01/28/tsa.bombtest/index.html>>  
<<http://www.homelandstupidity.us/2007/10/25/tsa-screeners-fail-most-bomb-tests/>>  
oppure <<http://tinyurl.com/4npg9o>>  
<<http://www.homelandstupidity.us/2006/10/31/tsa-screeners-still-fail-to-find-guns-bombs/>>  
oppure <<http://tinyurl.com/3ephqq>>  
<[http://www.boston.com/news/local/articles/2003/10/16/logan\\_screeners\\_fail\\_weapons\\_tests/](http://www.boston.com/news/local/articles/2003/10/16/logan_screeners_fail_weapons_tests/)>  
oppure <<http://tinyurl.com/r5gu>>

Questo articolo è originariamente apparso su Wired.com.

<[http://www.wired.com/politics/security/commentary/securitymatters/2008/09/securitymatters\\_0918](http://www.wired.com/politics/security/commentary/securitymatters/2008/09/securitymatters_0918)>  
oppure <<http://tinyurl.com/4m6vvj>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## News

Secondo documenti del governo degli Stati Uniti, la paura del terrorismo potrebbe provocare un'epidemia psicosomatica:

<<http://blog.wired.com/27bstroke6/2008/09/terrorism-fear.html>>

GPS spoofing:

<<http://philosecurity.org/2008/09/07/gps-spoofing>>

<<http://www.ne.anl.gov/capabilities/vat/spoof.html>>

La NSA e altri intercettano le telefonate cellulari servendosi di tecnologie facilmente reperibili sul mercato:

<[http://news.cnet.com/8301-13739\\_3-10030134-46.html](http://news.cnet.com/8301-13739_3-10030134-46.html)>

La NSA si unisce al governo cinese per limitare l'anonimato su Internet:

<[http://www.schneier.com/blog/archives/2008/09/the\\_nsa\\_teams\\_u.html](http://www.schneier.com/blog/archives/2008/09/the_nsa_teams_u.html)>

La minaccia da trama cinematografica pensata dal Pentagono: terroristi che utilizzano World of Warcraft:

<[http://www.schneier.com/blog/archives/2008/09/the\\_pentagons\\_w.html](http://www.schneier.com/blog/archives/2008/09/the_pentagons_w.html)>

I dipendenti della TSA evitano lo screening agli aeroporti.

<<http://www.9news.com/news/article.aspx?storyid=99941&catid=339>>

Non è un gran problema. Durante il turno di lavoro, gli screener devono entrare e uscire passando per la sicurezza tutte le volte. Certo, possono introdurre o portar fuori di nascosto degli oggetti dall'aeroporto. Ma occorre ricordare che per il sistema gli screener di un aeroporto sono degli elementi interni fidati: potrebbero superare la sicurezza aeroportuale in milioni di modi. D'altro canto però sarebbe forse una buona idea controllare gli screener quando passano attraverso la sicurezza in aeroporto ogni volta che non stanno lavorando in quel dato checkpoint in quel momento. Il motivo è lo

stesso per cui si dovrebbero controllare tutte le persone; compresi i piloti, che potrebbero far schiantare i loro aerei: non state controllando gli screener (o i piloti), ma individui che indossano divise da screener (o da pilota) e che hanno con sé tesserini da screener (o da pilota). È possibile addestrare gli screener in modo che sappiano riconoscere divise e tesserini autentici, oppure controllare chiunque. La seconda opzione è la più semplice. Ma, ripeto, non è un gran problema.

Posso pensare a dei casi specifici in cui possa essere utile poter aprire la propria porta di casa via Internet, ma nella maggior parte dei casi non è una buona idea.

<<http://www.theinquirer.net/gb/inquirer/news/2008/09/04/unlock-house-via-internet>>  
oppure <<http://tinyurl.com/4rsyve>>  
<<http://treocentral.com/content/Stories/1999-1.htm>>

In India stanno utilizzando delle letture encefaliche per provare la colpevolezza in tribunale.

<<http://www.nytimes.com/2008/09/15/world/asia/15brainscan.html>>

La pseudo-scienza qui è ancora peggio di quella delle macchine della verità.

<<http://www.thehindu.com/2008/09/08/stories/2008090854420400.htm>>

Mi è stato chiesto di rilasciare un commento in merito all'hacking effettuato ai danni dell'account email di Sarah Palin. Ho già parlato nel 2005 dei problemi di sicurezza legati alle "domande segrete":

<[http://www.schneier.com/blog/archives/2005/02/the\\_curse\\_of\\_th.html](http://www.schneier.com/blog/archives/2005/02/the_curse_of_th.html)>

Altri commenti:

<<http://www.freedom-to-tinker.com/blog/felten/how-yahoo-could-have-protected-palins-email>>

oppure <<http://tinyurl.com/4689km>>

Il sistema di telecamere da 20 milioni di dollari della Freedom Tower di New York è molto sofisticato:

<<http://cityroom.blogs.nytimes.com/2008/09/24/unblinking-eyes-for-20-million-at-freedom-tower/>>

oppure <<http://tinyurl.com/53e52c>>

Stiamo sviluppando uno strumento pre-reato che rileva pensieri ostili.

<<http://www.newscientist.com/blogs/shortsharpscience/2008/09/precrime-detector-is-showing-p.html>>

oppure <<http://tinyurl.com/53ftps>>

<[http://www.foxnews.com/printer\\_friendly\\_story/0,3566,426485,00.html](http://www.foxnews.com/printer_friendly_story/0,3566,426485,00.html)>

Spykee è il vostro robot-spia personale. Scatta foto e realizza filmati che potete guardare su Internet in tempo reale o salvare per un secondo momento. Potete anche parlare via Skype con chiunque stiate spiando. Costa soltanto 300 dollari.

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

<<http://www.robotsrule.com/html/spykee.php>>

<<http://www.amazon.com/gp/offer-listing/B000N6470A?tag=counterpane>>

Massime sulla sicurezza di Roger Johnston. Divertenti e assolutamente vere.

<<http://www.ne.anl.gov/capabilities/vat/seals/maxims.html>>

Inviare un vostro messaggio personalizzato agli screener della TSA addetti alle macchine a raggi X, utilizzando targhe metalliche da mettere nel bagaglio a mano.

<[http://blog.makezine.com/archive/2008/09/metal\\_plates\\_send\\_message.html](http://blog.makezine.com/archive/2008/09/metal_plates_send_message.html)>  
oppure <<http://tinyurl.com/4ro8es>>  
<[http://www.nytimes.com/idg/IDG\\_852573C400693880002574D70000A2FB.html](http://www.nytimes.com/idg/IDG_852573C400693880002574D70000A2FB.html)>

Un altro falso allarme bomba. Stavolta si tratta di hot dog.

<[http://www.philly.com/philly/blogs/phillies\\_zone/Just\\_Hot\\_Dogs\\_Folks.html](http://www.philly.com/philly/blogs/phillies_zone/Just_Hot_Dogs_Folks.html)>  
oppure <<http://tinyurl.com/5xpzsp>>  
<<http://www.nytimes.com/aponline/us/AP-ODD-Hot-Dog-Scare.html>>

The Hackers Choice ha rilasciato uno strumento che permette di clonare e modificare i passaporti elettronici. Il problema sono i certificati autofirmati. Una Autorità Certificatrice non è una gran soluzione, e il link offre un'ottima spiegazione del perché. "E dunque qual è la soluzione? Sappiamo che gli esseri umani fanno un buon lavoro al controllo di frontiera. In fondo ci hanno protetti egregiamente in questi ultimi 120 anni. Sappiamo anche che gli esseri umani sono bravi a riconoscere determinati pattern e nel riconoscimento di immagini. Inoltre gli umani svolgono un ottimo lavoro nel 'valutare' la persona e non soltanto il passaporto. Se si elimina la parte umana, la sicurezza dei passaporti viene meno".

<<http://blog.thc.org/index.php?/archives/4-The-Risk-of-ePassports-and-RFID.html>>  
oppure <<http://tinyurl.com/4l49v4>>  
<[http://www.theregister.co.uk/2008/09/30/epassport\\_hack\\_description/](http://www.theregister.co.uk/2008/09/30/epassport_hack_description/)>

Le bombe a mano ora sono diventate armi di distruzione di massa:

<[http://www.schneier.com/blog/archives/2008/10/hand\\_grenades\\_a.html](http://www.schneier.com/blog/archives/2008/10/hand_grenades_a.html)>

Una fotocamera dell'MI6, informazioni segrete incluse, è stata venduta su eBay. Il compratore l'ha consegnata alla polizia.

<<http://www.techcrunch.com/2008/09/30/top-secret-mi6-camera-sold-to-the-highest-bidder-on-ebay/>>  
oppure <<http://tinyurl.com/4n5ov2>>  
<<http://gizmodo.com/5056749/mi6-camera-with-secret-images-bought-on-ebay-for-30>>  
oppure <<http://tinyurl.com/4pj5jh>>

Denunciati i produttori di 'scareware' -- era ora.

<[http://voices.washingtonpost.com/securityfix/2008/09/microsoft\\_washington\\_state\\_t ar.html](http://voices.washingtonpost.com/securityfix/2008/09/microsoft_washington_state_t ar.html)>  
oppure <<http://tinyurl.com/3pxho4>>

Brillante: rapinatore di banche recluta i suoi complici mediante Craigslist.

<[http://www.king5.com/topstories/stories/NW\\_100108WAB\\_monroe\\_robber\\_floating\\_escape\\_TP.ce3930c1.html](http://www.king5.com/topstories/stories/NW_100108WAB_monroe_robber_floating_escape_TP.ce3930c1.html)>  
oppure <<http://tinyurl.com/3h8wfe>>

Nuovi attacchi cross-site request forgery.

<<http://www.freedom-to-tinker.com/blog/wzeller/popular-websites-vulnerable-cross-site-request-forgery-attacks>>  
oppure <<http://tinyurl.com/4ubb2f>>  
<<http://www.freedom-to-tinker.com/sites/default/files/csrf.pdf>>

"Clickjacking" è un nome incredibilmente sexy, ma la vulnerabilità non è altro che una variante del cross-site scripting. Non sappiamo quanto sia grave, perché i dettagli non

sono ancora stati rivelati. Ma basta il nome a scatenare il panico. Ecco un buon Q&A sulla vulnerabilità:

<[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115818&source=NLT\\_SEC&nid=38](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115818&source=NLT_SEC&nid=38)>

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

<<http://www.cgisecurity.org/2008/10/interview-jerem.html>>

<<http://hackademix.net/2008/09/27/clickjacking-and-noscript/>>

Pare che sia possibile aggiungere il numero di chiunque alla (o toglierlo dalla) do-not-call list canadese (la do-not-call list è la lista di numeri in cui chiunque può chiedere di essere inserito per segnalare di non voler ricevere chiamate telefoniche a scopi di marketing). È anche possibile aggiungere (ma non togliere) numeri alla do-not-call list statunitense, ma solo tre alla volta, e occorre fornire un indirizzo email valido per confermare l'aggiunta. Ecco la mia idea: se siete un'azienda, aggiungete i recapiti telefonici di tutti i vostri clienti: in questo modo nessuno dei vostri concorrenti potrà chiamarli per sottoporre proposte commerciali.

<https://www.lnnte-dncl.gc.ca/>

<https://www.donotcall.gov/register/reg.aspx>

I cinesi controllano i messaggi Skype:

<<http://arstechnica.com/news.ars/post/20081002-skype-security-flub-leads-to-discovery-of-chinese-monitoring.html>>

oppure <<http://tinyurl.com/4pgn2j>>

Secondo un voluminoso resoconto del National Research Council, il data mining per i terroristi non funziona.

<[http://news.cnet.com/8301-13578\\_3-10059987-38.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-13578_3-10059987-38.html?part=rss&subj=news&tag=2547-1_3-0-20)>

oppure <<http://tinyurl.com/4klgqe>>

<<http://arstechnica.com/news.ars/post/20081009-analysis-data-mining-doesnt-work-for-spotting-terrorists.html>>

oppure <<http://tinyurl.com/4azsds>>

<[http://www.nap.edu/catalog.php?record\\_id=12452](http://www.nap.edu/catalog.php?record_id=12452)>

Uno studio interessante di Adam Shostack sulla modellazione delle minacce di Microsoft.

<<http://blogs.msdn.com/sdl/attachment/8991806.ashx>>

Secondo Elcomsoft il protocollo WPA sarebbe morto, solo perché sono in grado di velocizzare di 100 volte il cracking a forza bruta utilizzando un acceleratore hardware. E dove sarebbe la novità? Certo, le password deboli sono deboli, grazie, lo sappiamo già. E le password WPA forti sono ancora forti. Questo mi sembra l'ennesimo tentativo di attirare l'interesse della stampa e farsi pubblicità con dei risultati crittanalitici immaturi.

<<http://www.elcomsoft.com/edpr.html?r1=pr&r2=wpa>>

<<http://mobile.slashdot.org/mobile/08/10/12/1724230.shtml>>

<[http://www.theregister.co.uk/2008/10/10/graphics\\_card\\_wireless\\_hacking/](http://www.theregister.co.uk/2008/10/10/graphics_card_wireless_hacking/)>

<<http://www.schneier.com/essay-148.html>>

Un astuto attacco antiterroristico contro l'IRA: metter su una lavanderia a gettone e controllare chi ha residui di esplosivo sui vestiti.

<[http://www.schneier.com/blog/archives/2008/10/clever\\_countert.html](http://www.schneier.com/blog/archives/2008/10/clever_countert.html)>

Ecco una nuova truffa chip-and-pin nel Regno Unito. I lettori di schede sono stati hackerati in fase di produzione, "o durante il processo di manifattura in una fabbrica cinese, o subito dopo". Viene chiamato "supply chain hack", ossia hack della catena di fornitura. Molto sofisticato, e dimostra ancora una volta come questi sistemi di sicurezza completamente automatizzati presentino parecchi rischi.

<<http://online.wsj.com/article/SB12236699999723871.html>>

<<http://www.telegraph.co.uk/news/newsttopics/politics/lawandorder/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html>>

<<http://www.telegraph.co.uk/news/worldnews/asia/pakistan/3173161/Credit-card-scam-How-it-works.html>>

Tra l'altro, quanto vale sabotare un'elezione?

<<http://www.schneier.com/essay-046.html>>

BART, l'autorità della rete di trasporti metropolitani di San Francisco, ha recentemente discusso sul permettere o meno ai passeggeri di portarsi bibite sui treni. Vi sono delle ottime ragioni per proibirlo o permetterlo (comodità, problemi dati dal rovesciamento dei liquidi, eccetera), ma una che non ha assolutamente senso è che dei terroristi possano portare a bordo dei liquidi infiammabili. Eppure è proprio quella menzionata dagli amministratori del BART. Non è questa gran novità -- abbiamo visto stupidaggini come questa sin dall'11 settembre 2001 -- ma questa volta la gente ha reagito: "Il direttore aggiunto Tom Radulovich: 'Se qualcuno vuole infrangere la legge e portare sui treni dei liquidi infiammabili, faccia pure. Non è che quelli di al Qaeda stanno aspettando nelle loro caverne che istituiamo la regola del bicchiere salvagoccia'. Dirigendo i propri commenti agli amministratori del BART, ha detto: 'Sapete, non è altro che allarmismo esasperato e dovrete vergognarvi'". L'allarmismo terroristico sembra che stia avendo meno effetto.

<<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/10/10/BAB813EELU.DTL>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Più le cose cambiano, più rimangono le stesse

Indovinate l'epoca: "Le organizzazioni criminali sono aumentate per dimensioni e ambiti di azione; sono più audaci e si avvalgono delle più terribili armi offerte dalla scienza moderna, e il mondo oggi è minacciato da nuove forze che, se incautamente liberate, potrebbero un giorno portare alla distruzione globale. Le bombe Orsini erano dei giocattoli se confrontate con gli ultimi sviluppi di macchine infernali. Fra il 1858 e il 1898 l'ignobile scienza della distruzione aveva fatto enormi e allarmanti progressi..."

No, non è un errore di battitura. "Fra il 1858 e il 1898...". Questo passaggio è tratto da Magg. Arthur Griffith, "Mysteries of Police and Crime", London, 1898, II, p. 469. Viene citato in Walter Laqueur, "A History of Terrorism", New Brunswick/London, Transaction Publishers, 2002.

<<http://query.nytimes.com/mem/archive-free/pdf?res=9907E7D8153DE633A25757C0A9659C94689ED7CF>>

oppure <<http://tinyurl.com/3wn2ct>>

<[http://www.amazon.com/History-Terrorism-Walter-Laqueur/dp/0765807998/ref=pd\\_bbs\\_sr\\_1?ie=UTF8&s=books&qid=1223482236&sr=8-1](http://www.amazon.com/History-Terrorism-Walter-Laqueur/dp/0765807998/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1223482236&sr=8-1)>

oppure <<http://tinyurl.com/46s7ny>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Le intercettazioni senza mandato della NSA prendono di mira americani innocenti

Vi ricordate quando il governo degli Stati Uniti disse che stava spiando soltanto i terroristi? Chiunque con un po' di buon senso sapeva che si trattava di una menzogna (un potere senza supervisione viene sempre abusato), ma neppure io mi sarei immaginato che fosse così grave:

"Faulk ha dichiarato che lui ed altri alla sua sezione della sede della NSA a Fort Gordon si passavano regolarmente telefonate lascive o provocanti che erano state intercettate, segnalando ai colleghi d'ufficio certi codici temporali di 'estratti' disponibili sui computer di ogni operatore.

"Ehi, senti questa', Faulk sostiene che gli dicessero, 'c'è dell'ottimo sesso telefonico o una bella conversazione intima, prendi questa chiamata, è proprio divertente, va' a sentire'. Magari era qualche colonnello impegnato in una conversazione privata a letto e commentavamo cose tipo 'Wow, roba da matti', Faulk ha detto ad ABC News".

I mandati sono un dispositivo di sicurezza. Ci proteggono dagli abusi di potere del governo.

<<http://www.nytimes.com/2008/10/10/washington/10nsa.html>>

<<http://abcnews.go.com/Blotter/story?id=5987804&page=1>>

<[http://www.upi.com/Top\\_News/2008/10/10/Spy\\_agency\\_accused\\_of\\_improper\\_listening/UPI-99751223644874/](http://www.upi.com/Top_News/2008/10/10/Spy_agency_accused_of_improper_listening/UPI-99751223644874/)>

<<http://www.reuters.com/article/domesticNews/idUSTRE4990CD20081010>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Le news su Schneier/BT

Schneier parlerà alla 30esima International Conference of Data Protection and Privacy Commissioners il 15 ottobre a Strasburgo, Francia.

<<http://www.privacyconference2008.org/>>

Schneier parlerà allo European Security and Information System Congress il 17 ottobre a Monaco.

<<http://cms.event-catalyst.com/assises/home.aspx>>

Schneier parlerà alla RSA Europe il 28 ottobre a Londra.

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

Schneier parlerà alla 22esima Large Installation System Administration Conference il 13 novembre a San Diego, California.

<<http://usenix.org/events/lisa08/>>

Schneier è stato intervistato da Telecom Asia:  
<[http://www.telecomasia.net/article.php?id\\_article=10230](http://www.telecomasia.net/article.php?id_article=10230)>

Schneier è stato intervistato dall'Irish Times:  
<<http://www.irishtimes.com/newspaper/finance/2008/1003/1222959300589.html>>  
oppure <<http://tinyurl.com/4ccjmw>>

Schneier è stato intervistato dal Dr. Dobb's Journal:  
<<http://www.ddj.com/security/210605067>>

Il mio articolo sulle centrali chimiche e sulla sicurezza per il Guardian. Niente che non abbia già detto in precedenza.  
<<http://www.schneier.com/essay-243.html>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Taleb sui limiti della gestione dei rischi

Un bel paragrafo sui limiti della gestione dei rischi tratto da un'intervista, a tratti interessante, a Nicholas Taleb:

"Perché poi ci si ritrova con un problema da Linea Maginot. [Dopo la Prima Guerra Mondiale i Francesi eressero delle fortificazioni di cemento per evitare un'ulteriore invasione da parte della Germania -- una risposta alla guerra precedente che si rivelò inefficace per la successiva]. Fanno di tutto per risolvere quel particolare problema: i tedeschi non potranno invadere passando di qui. Ciò a cui bisogna stare più attenti, naturalmente, è la pianificazione degli scenari, perché di solito se si parla di scenari, si finirà col sopravvalutare le probabilità di tali scenari. Se li esaminiamo a scapito di tutti quelli che non esaminiamo, è un metodo che a volte ha peggiorato la situazione; per cui la pianificazione degli scenari può essere deleteria. Mi limiterò alla mia passata esperienza personale. Coloro che si sono cimentati nella pianificazione degli scenari non hanno ottenuto risultati migliori rispetto a chi non l'ha fatta. Molte persone hanno attuato delle misure "ragionevoli", e ciò le ha rese più vulnerabili perché danno l'illusione di aver fatto il proprio lavoro. Questo è il problema con la gestione dei rischi. Io ritorno sempre a una questione classica. Mai dare a uno sciocco l'illusione del risk management. Mai chiedere a qualcuno di indovinare il numero di dentisti a Manhattan dopo avergli chiesto le ultime quattro cifre del suo numero di Previdenza Sociale. I numeri verranno sempre messi in correlazione. Io stesso ho svolto qualche lavoro nel risk management, per dimostrare quanto siamo stupidi nell'affrontare i rischi".

<<http://www.portfolio.com/views/columns/the-world-according-to/2008/08/14/Interview-With-Nassim-Nicholas-Taleb>>  
oppure <<http://tinyurl.com/5eazpu>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

"Nuovo attacco" contro immagini criptate

Nel palese tentativo di ottenere un po' di pubblicità, un ricercatore dell'azienda PMC Ciphers ha scoperto che criptando i dati in modalità ECB genera dei pattern di crittogrammi.

Sì, lo sapevamo già.

E un punto in meno per un'azienda di sicurezza che richiede l'uso di JavaScript e che non prevede una soluzione in caso di errore quando non è abilitato nel browser. E, uhm, da dove salta fuori quella fotografia nello studio? I ricercatori non avrebbero potuto ricorrere a qualcosa di meno adolescenziale?

Per la cronaca, ho sbattuto PMC Cipher nel Canile nel 2003: "PMC Ciphers. La descrizione della teoria è talmente intrisa di pseudo-crittografia che rende la lettura molto divertente. Le varie ipotesi vengono presentate come conclusioni. La ricerca attuale viene ignorata o esposta in maniera inesatta. Il primo link è uno studio tecnico con quattro riferimenti, tre dei quali scritti prima del 1975. Chi ha bisogno di trent'anni di ricerca crittografica quando si può avere la teoria del cifrario polimorfico?"

All'epoca non mi accorsi che PMC Ciphers aveva risposto alla mia provocazione. Molto divertente.

<<http://www.techworld.com/security/news/index.cfm?newsid=105263>>  
<[http://www.turbocrypt.com/vpics/9a8f098c615a425eab6d17c804dd67ae/whitepapers/backup\\_attack.pdf](http://www.turbocrypt.com/vpics/9a8f098c615a425eab6d17c804dd67ae/whitepapers/backup_attack.pdf)>

oppure <<http://tinyurl.com/3fe64r>>

'Il Canile' e la risposta:

<<http://www.schneier.com/crypto-gram-0303.html#4>>

<<http://www.ciphers.de/eng/content/Background-Info/Bruce-Schneiers-comments.html>>

oppure <<http://tinyurl.com/52ymfo>>

Quando ho pubblicato questo pezzo sul mio blog, sono comparsi tre nuovi commentatori a difendere lo studio, tutti con accesso dialup dello stesso Internet Provider tedesco. Ma guarda un po'.

<[http://www.schneier.com/blog/archives/2008/10/new\\_attack\\_agai.html](http://www.schneier.com/blog/archives/2008/10/new_attack_agai.html)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Adesso gli attivisti non-violenti sono terroristi

Questo è abominevole: "La Maryland State Police ha classificato 53 attivisti non-violenti come terroristi e ha inserito i loro nomi e i loro dati personali nei database statali e federali che tracciano i sospetti terroristi, ha ammesso ieri il capo della polizia statale".

Perché lo hanno fatto? "Sia Hutchins che Sheridan hanno detto che i nomi degli attivisti sono stati inseriti come terroristi nel database della polizia statale in parte perché il software offriva opzioni limitate di classificazione".

So che una volta avevamo questa mentalità "o sei con noi o con i terroristi", ma non pensate che, forse, il software dovrebbe consentire un po' più di elasticità?

<[http://www.washingtonpost.com/wp-dyn/content/article/2008/10/07/AR2008100703245\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/10/07/AR2008100703245_pf.html)>  
oppure <<http://tinyurl.com/3znjv7>>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

La gestione dei rischi ha senso?

Siamo continuamente impegnati nella gestione dei rischi, ma ha senso soltanto se la facciamo nel modo migliore.

La gestione dei rischi, il "risk management", è semplicemente un termine altisonante per descrivere il compromesso costi-benefici associato a ogni decisione di sicurezza. È quel che facciamo quando reagiamo alla paura, o quando cerchiamo di sentirci più al sicuro. È il riflesso "combatti o fuggi" che si è evoluto nei pesci primitivi e rimane in tutti i vertebrati. È istintivo, intuitivo e fondamentale per la vita, nonché una delle funzioni primarie del cervello.

Alcuni hanno ipotizzato che gli esseri umani sono dotati di un "termostato del rischio" che cerca di mantenere un certo livello di rischio ottimale. Ciò spiega perché andiamo più forte in moto quando indossiamo un casco, o perché è più probabile prendere il vizio del fumo in tempi di guerra. È il nostro "risk management" naturale in azione.

Il problema è che il nostro cervello è molto più ottimizzato per i compromessi di sicurezza legati alla vita in piccoli gruppi familiari nelle zone montagnose dell'Africa Orientale del 100.000 a.C. che non a quelli legati alla vita nella città di New York nel 2008. Commettiamo spesso errori sistematici di gestione dei rischi: calcoliamo male le probabilità di eventi rari, reagendo più alle storie che ai dati, rispondendo più alla percezione della sicurezza che non alla realtà, e prendendo decisioni basate su un contesto irrilevante. E quel nostro termostato del rischio? Non è affatto così finemente regolato come ci piacerebbe che fosse.

Come un coniglio che risponde all'arrivo di un'automobile con il proprio comportamento classico per evitare un predatore -- lanciandosi a sinistra, poi a destra, poi ancora a sinistra, e saltare all'ultimo momento -- invece di scansarsi e basta, il nostro intuito da Età della Pietra non ci è di grande aiuto in una società moderna e tecnologica. Pertanto, quando noi dell'industria della sicurezza utilizziamo il termine "risk management", non vogliamo che lo affrontiate seguendo il vostro istinto. Vogliamo che la gestione dei rischi sia effettuata coscienziosamente e in maniera intelligente, analizzando il compromesso e prendendo la decisione migliore.

Ciò significa bilanciare i costi e i benefici di qualunque decisione di sicurezza: acquistare e installare una nuova tecnologia, implementare una nuova procedura o rinunciare a una normale precauzione. Significa allocare un budget di sicurezza per mitigare rischi diversi con somme diverse. Significa stipulare un'assicurazione per trasferire alcuni rischi ad altre entità. È quel che fanno le imprese, in ogni momento e per qualsiasi

cosa. La sicurezza IT presenta le sue proprie decisioni di risk management, basate sulle minacce e sulle tecnologie.

Non esiste mai un rischio solo, ovviamente, e cattive decisioni di risk management spesso portano con sé un compromesso basilare. La policy antiterrorismo negli Stati Uniti si basa molto più sulla politica che sul rischio per la sicurezza vero e proprio, ma i politici che prendono queste decisioni sono più preoccupati per i rischi di non essere rieletti.

Molte decisioni di sicurezza in ambito aziendale vengono prese per mitigare il rischio di cause legali, più che per affrontare il rischio di una eventuale falla di sicurezza. E i singoli individui prendono decisioni di risk management che non considerano solo i rischi per l'azienda, ma anche i rischi per i budget dei loro dipartimenti e i rischi per la propria carriera.

Non è possibile eliminare completamente il fattore emotivo dalle decisioni di gestione dei rischi, ma il sistema migliore per mantenere il risk management focalizzato sui dati è quello di formalizzare la metodologia. Questo è ciò che cercano di fare quelle aziende che fanno del risk management il proprio mestiere: compagnie assicurative, ditte di trading finanziario e chi si occupa di arbitraggio. Cercano di rimpiazzare l'istinto con dei modelli, e le intuizioni con la matematica.

Il problema nella realtà della sicurezza è che spesso ci mancano i dati per effettuare un buon risk management. I rischi tecnologici sono complessi e intricati. Non sappiamo quanto bene la nostra sicurezza di rete sia in grado di tener fuori gli aggressori, e non sappiamo quanto verrà a costare all'azienda se non teniamo fuori gli aggressori. E i rischi cambiano in continuazione, rendendo i calcoli ancora più difficili. Ma questo non vuol dire che non dovremmo provarci lo stesso.

Non è possibile evitare il risk management: è fondamentale per il business quanto lo è per la vita. La questione è se si intende provare a utilizzare i dati o se ci si limita a reagire basandosi sulle emozioni, sulle intuizioni e sugli aneddoti.

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

<[http://searchsecurity.techtarget.com/loginMembersOnly/1,289498,sid14\\_gci1332745,00.html?](http://searchsecurity.techtarget.com/loginMembersOnly/1,289498,sid14_gci1332745,00.html?)>

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

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](mailto: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.