

CRYPTO-GRAM
15 giugno 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:

- La guerra alla fotografia
- Attraversare le frontiere con computer portatili e PDA
- News
- Email dopo il Ratto Salvifico
- Le firme via fax
- La guerra alle T-shirt
- Le news su Schneier/BT Counterpane
- Ancora sulle telecamere nei sedili degli aerei
- Come vendere la sicurezza
- Commenti dei lettori

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

La guerra alla fotografia

Che sta succedendo con i fotografi di recente? Sono davvero tutti dei terroristi, o semplicemente tutti pensano che lo siano?

Dall'11 settembre 2001 in avanti si è potuto notare una guerra sempre più aspra contro la fotografia. Molti fotografi sono stati tormentati, interrogati, detenuti, arrestati o peggio, e dichiarati inopportuni, sgraditi. Ci è stato detto più volte di stare attenti ai fotografi, soprattutto quelli dall'aria sospetta. Ovviamente ogni terrorista si mette a fotografare prima il suo bersaglio, per cui è necessario vigilare.

Solo che si tratta di un'enorme sciocchezza. I terroristi dell'11 settembre non fotografarono nulla. Né i dinamitardi dei trasporti pubblici di Londra, o i dinamitardi della metropolitana di Madrid, o i dinamitardi muniti di esplosivo liquido arrestati a Londra nel 2006. Timothy McVeigh non ha fotografato l'Oklahoma City Federal Building. Unabomber non ha mai fotografato nulla, né tantomeno Richard Reid (il dinamitardo con l'esplosivo nelle scarpe). Non sono state trovate fotografie fra le carte dei bombaroli suicidi palestinesi. L'IRA non era conosciuto per le sue fotografie. Prendiamo anche quelle trame terroristiche costruite che piacciono tanto al governo americano: i terroristi di Fort Dix, i dinamitardi dell'aeroporto JFK, i Miami 7, i Lackawanna 6... Di fotografie neanche l'ombra.

Visto che i veri terroristi, e persino gli aspiranti terroristi, pare che non si mettano a fotografare alcunché, perché questa diffusa credenza secondo cui i terroristi fotografano i loro prossimi bersagli è così radicata? Per quale motivo le nostre paure sono tali che non ci resta altra scelta se non quella di nutrire sospetti verso qualunque fotografo?

Perché è una minaccia da trama cinematografica.

Una minaccia da trama cinematografica è una minaccia specifica, molto vivida nelle nostre menti come la trama di un film. Ricordiamo simili minacce sin dai mesi successivi agli attacchi dell'11 settembre: antrace propagata dai polverizzatori usati in agricoltura, una fornitura di latte contaminata, gruppi di subacquei terroristi armati di calendari. La nostra immaginazione si scatena elaborando minacce specifiche e ricche di dettagli, che derivano dalle notizie, ma anche da film e show televisivi. Queste trame da film echeggiano nelle nostre menti e in quelle delle persone con cui parliamo. E molti si spaventano.

I terroristi che si appostano e scattano foto è un dettaglio fondamentale in ogni buon film di questo genere. Naturalmente ha senso che i terroristi scattino foto dei loro prossimi bersagli. Dovranno pur effettuare una ricognizione, no? Servono 45 minuti di azione televisiva prima dell'effettivo attacco terroristico, 90 minuti se si tratta di un film, e una scena in cui vengono scattate delle foto è perfetta. Sono i terroristi delle nostre trame da film a essere dei fotografi, non quelli del mondo reale.

L'eterno problema della sicurezza che viene creata intorno alle minacce da trama cinematografica è che funziona soltanto se indoviniamo correttamente la trama. Se spendiamo un fantastiliardo di dollari per difendere Wimbledon e i terroristi fanno saltare in aria un altro evento sportivo, quelli sono soldi sprecati. Se mettiamo delle guardie a pattugliare l'intera rete della metropolitana e i terroristi fanno saltare in aria un centro commerciale affollato, anche in questo caso avremo investito denaro inutilmente. Se diciamo a tutti di prestare attenzione ai fotografi, e i terroristi non scattano fotografie, avremo buttato denaro ed energie, e avremo insegnato alla gente ad aver paura di una cosa che non dovrebbero temere.

E anche se i terroristi fotografassero i loro bersagli, i conti non tornano ugualmente. Ogni anno, miliardi di foto vengono scattate da persone oneste, 50 miliardi da fotografi amatoriali solo negli Stati Uniti. E i monumenti nazionali che immaginiamo vengano fotografati dai terroristi sono gli stessi monumenti che i turisti amano fotografare. Se vedete qualcuno scattare una di quelle foto, le probabilità che questa persona sia un terrorista sono pressoché nulle.

Naturalmente, è più facile spiegare il problema che risolverlo. Dato che siamo una razza di narratori, troviamo estremamente affascinanti le minacce da trama cinematografica. Un solo scenario descritto in maniera vivida tende a essere molto più convincente sul fatto che i fotografi possano essere terroristi, di tutti i dati che io riesca a raccogliere per dimostrare il contrario.

Terrore a parte, non esistono molte restrizioni legali su ciò che è possibile fotografare da un luogo pubblico quando è già visibile pubblicamente. Se venite maltrattati, si tratta quasi certamente di un agente delle forze dell'ordine, pubblico o privato, che sta abusando della propria autorità. Non vi è nulla in nessuna legge post-11 settembre che riduca o ridimensioni il vostro diritto a fotografare.

È una lotta che val la pena portare avanti. Cercate "photographer rights", "diritti dei fotografi" in Google e scaricate uno dei tanti documenti da stampare e da mettere nel portafogli che possano aiutarvi in caso veniate fermati o molestati. Ne ho trovato uno per il Regno Unito, per gli USA e per l'Australia. Non rinunciate al vostro diritto di fotografare in pubblico. Non contribuite a diffondere la storia del fotografo terrorista. Ricordate alle autorità che proibire la fotografia era una di quelle cose per cui si prendeva in giro l'Unione Sovietica. Alla fine si tornerà a ragionare, ma il percorso è ancora lungo.

Incidenti e campagne anti-fotografia:

<<http://nycphotorights.com/wordpress/?p=110>>

<<http://news.bbc.co.uk/2/hi/technology/7351252.stm>>

<http://www.allensphotoblog.com/blog1/2007/09/photography_terrorism.html>

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

<<http://flash.poppphoto.com/blog/2007/06/the-crime-of-ph.html>>

<<http://flash.poppphoto.com/blog/2007/10/the-crime-of-ph.html>>

<<http://flash.poppphoto.com/blog/2007/09/the-crime-of-ph.html>>

<<http://flash.poppphoto.com/blog/2007/11/the-crime-of-ph.html>>

<http://www.episcopalcafe.com/daily/war_and_peace/every_day_diplomacy.php>

oppure <<http://tinyurl.com/3x5f6c>>

<<http://www.boingboing.net/2008/05/14/bb-reader-two-fbi-ag.html>>

<http://www.andycarvin.com/archives/2008/05/almost_arrested_for_taking_photos_at_uni.html>

oppure <<http://tinyurl.com/6dq3ea>>

<http://blog.washingtonpost.com/rawfisher/2008/05/union_station_photo_follies.html

>

oppure <<http://tinyurl.com/5rp2zb>>

<http://www.amateurphotographer.co.uk/news/Antiterror_police_defend_campaign_targeting_suspicious_behaviour_of_people_with_cameras_news_195594.html>

oppure <<http://tinyurl.com/28qq9x>>

<<http://www.news.com.au/couriermail/story/0,23739,23553587-952,00.html>>

<<http://www.salon.com/tech/col/smith/2006/02/10/askthepilot173/index.html>>

oppure <<http://tinyurl.com/4x7v8z>>

<http://www.nytimes.com/2008/01/20/arts/design/20shat.html?_r=1&adxnnl=1&oref=slogin&adxnnlx=1210125984-qrPPfI/kDIEi+wMrOvtEA>

oppure <<http://tinyurl.com/5w9c3n>>

<<http://lightchasersphotography.com/blog/how-to-shoot-photographs-like-a-terrorist/>>

oppure <<http://tinyurl.com/58qz56>>

<<http://www.memphisflyer.com/memphis/Content?oid=oid%3A41348>>

"Sciocchezze":

<<http://blog.wired.com/gadgets/2008/03/uk-politician-c.html>>

Finti complotti terroristici negli Stati Uniti:

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

Minacce da trama cinematografica:

<<http://www.schneier.com/essay-087.html>>

Dati sulle fotografie scattate negli Stati Uniti:

<<http://www.nytimes.com/2005/05/05/fashion/thursdaystyles/05photos.html>>

Diritti dei fotografi:

<<http://www.sirimo.co.uk/ukpr.php>>

<<http://www.krages.com/phoright.htm>>

<<http://www.kantor.com/blog/2005/12/legal-rights-of-photographers/>>

<<http://www.artslaw.com.au/documents/files/StreetPhotographersRights.pdf>>

oppure <<http://tinyurl.com/6kyc7m>>

Il commento di una persona che addestra guardie di sicurezza:

<http://www.schneier.com/blog/archives/2008/06/the_war_on_phot.html#c275864>

oppure <<http://tinyurl.com/6on7tr>>

Questo articolo è originariamente apparso nel Guardian:

<<http://www.guardian.co.uk/technology/2008/jun/05/news.terrorism>>

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

Attraversare le frontiere con computer portatili e PDA

Il mese scorso una corte statunitense ha stabilito che gli agenti di frontiera possono effettuare ricerche nel vostro portatile (o in qualsiasi altro dispositivo elettronico) quando entrate negli Stati Uniti. Possono requisirvi il computer e scaricarne l'intero contenuto, o trattenerlo per diversi giorni. Customs and Border Patrol non ha pubblicato alcuna regolamentazione riguardante questa pratica, e io ed altri abbiamo scritto una lettera al Congresso sollecitando un'investigazione e una regolamentazione di tale pratica.

Ma in questo gli Stati Uniti non sono soli. Gli agenti di frontiera britannici requisiscono i portatili per cercare contenuti pornografici. E su Internet si riferisce che questo genere di cose accade anche in altri paesi. Non vi piacerà, ma è un fatto. Come proteggersi, dunque?

Criptare l'intero disco rigido, una misura di sicurezza che dovrete sicuramente adottare in caso il vostro computer vada perso o venga rubato, non servirà in questa circostanza. L'agente di frontiera probabilmente inizierà tutta la procedura con un "Per favore, inserisca la password". Ovviamente potete rifiutarvi, ma questo porterà a

ulteriori perquisizioni, potrebbero trattenervi ancor di più, rifiutare il vostro ingresso nel paese... Insomma, troveranno un modo per rovinarvi la giornata.

Dovrete nascondere i vostri dati. Fate in modo che una parte del disco rigido sia criptata con una chiave diversa (anche se avete già criptato l'intero disco rigido) e mantenete le informazioni sensibili in quella porzione di disco. Molti programmi vi permettono di farlo. Io utilizzo PGP Disk (www.pgp.com). Anche TrueCrypt (www.truecrypt.org) va bene, ed è gratis.

Gli agenti di frontiera potrebbero mettersi a cercare nel vostro portatile, ma sarà difficile che incontreranno la partizione criptata (come ulteriore misura cautelativa potreste renderne l'icona invisibile). E se scaricano i contenuti del disco rigido per esaminarli in un secondo momento, non avrete di che preoccuparvi.

Assicuratevi di scegliere una password crittografica forte. I dettagli sono troppo complicati per fornirvi un suggerimento veloce, ma sostanzialmente qualunque cosa facile da ricordare sarà anche facile da indovinare. Purtroppo questa non è la soluzione perfetta. Il vostro computer potrebbe aver lasciato una copia della password da qualche parte sul disco, e un software di analisi forense intelligente la troverà di certo.

La miglior difesa, pertanto, è di ripulire il portatile. Un agente di frontiera non può leggere quel che non avete. E non avete bisogno dell'archivio di email e di informazioni sui clienti degli ultimi cinque anni. Non vi servono vecchie lettere d'amore o certe foto (sapete di quali foto sto parlando). Cancellate qualunque cosa non vi serva assolutamente, e utilizzate un programma per la cancellazione sicura dei file. Già che ci siete, eliminate i cookie del browser, la cache e la cronologia. I siti Web che avete visitato non sono affari altrui. E spegnete il computer, non mettetelo in stop soltanto, prima di passare la frontiera; così facendo vengono cancellate altre cose. Pensate a tutto questo come ultima cosa da fare prima di metter via i vostri dispositivi elettronici quando vi preparate all'atterraggio. Alcune aziende ora forniscono ai propri dipendenti dei portatili forensicamente puliti per viaggiare, e permettono di scaricare le informazioni sensibili attraverso un Virtual Private Network una volta che i dipendenti sono entrati nel paese. Il lavoro svolto viene inviato con lo stesso sistema, e tutto viene cancellato prima di passare la frontiera per tornare a casa. È un'ottima idea se potete metterla in atto.

Se non vi è possibile, considerate il trasferimento dei vostri dati sensibili su una chiavetta USB o anche una scheda di memoria per fotocamera: anche le schede da 16 GB ormai hanno prezzi abbordabili. Criptate il tutto, naturalmente, perché è facile perdere un oggetto tanto piccolo. Mettetevela in tasca, e con ogni probabilità non verrà nemmeno notata anche se l'agente di frontiera si mette a perquisirvi il portatile. Se viene scoperta, potete provare a dire: "Non so che cosa contiene. Il mio capo mi ha detto di consegnarla al direttore della sede di New York". Se avete scelto una password crittografica forte, non vi importerà se la confiscano.

Infine, non dimenticate il cellulare e il PDA. Gli agenti di frontiera possono esaminare anche quelli: le email, la rubrica contatti, l'agenda. Purtroppo l'unica cosa da fare in questo caso è cancellare quei dati.

Mi rendo conto che tutto questo suoni un po' laborioso, e che è più facile ignorare queste misure e sperare di non essere perquisiti. Oggi le probabilità giocano a vostro favore, ma grazie a nuovi strumenti d'analisi forense, le ricerche automatiche stanno

diventando sempre più semplici, e il recente provvedimento stabilito da quella corte statunitense potrebbe incentivare altri paesi a fare altrettanto. Meglio stare sul sicuro.

Addendum: Molte persone mi hanno fatto notare che in questo articolo sto suggerendo di mentire a un pubblico ufficiale. Ciò è ovviamente illegale negli Stati Uniti e, suppongo, in moltissimi altri paesi; e forse non è il consiglio migliore da offrire da parte mia pubblicamente. Pertanto mettetevi d'accordo col vostro capo e con la "sede di New York".

<<http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t>>

oppure <<http://tinyurl.com/5ghk3j>>

<<http://www.eff.org/deeplinks/2008/05/border-search-answers>>

<http://www.cnet.com/8301-13739_1-9935170-46.htmlhttp://www.news.com/8301-13578_3-9892897-38.html>

oppure <<http://tinyurl.com/68xgz4>>

I miei consigli sulla scelta di password sicure:

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

Questo articolo è originariamente apparso sul Guardian:

<<http://www.guardian.co.uk/technology/2008/may/15/computing.security>>

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

News

Terroristi che attaccano attraverso i condizionatori d'aria:

<http://www.schneier.com/blog/archives/2008/05/terrorists_atta.html>

Esiste un bug nel generatore di numeri casuali in Debian Linux, ed è presente dal settembre 2006. È una cosa grave. I numeri casuali vengono usati estesamente in crittografia, per sicurezza a breve e lungo termine. E, come abbiamo visto in questa sede, è molto facile creare accidentalmente vulnerabilità di sicurezza nei generatori di numeri casuali, ed è estremamente difficile scoprirle dopo. Ai tempi in cui la NSA si metteva a indebolire periodicamente la crittografia commerciale, la loro tecnica preferita era quella di ridurre l'entropia del generatore di numeri casuali.

<<http://metasploit.com/users/hdm/tools/debian-openssl/>>

<<http://www.debian.org/security/2008/dsa-1571>>

<<http://milw0rm.com/exploits/5622>>

<http://blog.sesse.net/blog/tech/2008-05-14-17-21_some_maths.html>

<<http://taint.org/2008/05/13/153959a.html>>

<<http://www.xkcd.com/424/#>>

Un dirottatore di aerei -- un vero dirottatore, uno con precedenti esperienze di dirottamenti aerei -- stava lavorando presso l'aeroporto di Heathrow.

<<http://www.telegraph.co.uk/news/uknews/1964930/Afghan-hijacker-'working-at-Heathrow'.html>>

oppure <<http://tinyurl.com/5puo9b>>

Le compagnie aeree stanno guadagnando grazie alle regole della TSA sui documenti con foto. Se il documento d'identità di un viaggiatore non corrisponde al suo biglietto, la compagnia aerea gli permette di cambiare il biglietto pagando 100 dollari. Tutto questo è completamente assurdo. Se le cose venissero fatte come si deve, l'addetto della TSA che controlla biglietto e documento d'identità potrebbe facilmente stabilire se i nomi sono identici. Invece il passeggero è costretto a rivolgersi di nuovo alla compagnia aerea che, dietro pagamento, cambia il nome sul biglietto in modo che corrisponda al documento di identità. Questo secondo sistema non è più sicuro. Se mai lo è di meno. Ma le regole sono regole, e questo è ciò che deve accadere.

<<http://www.cnn.com/2008/TRAVEL/traveltips/05/15/ticketing.errors/index.html>>
oppure <<http://tinyurl.com/3qwoqp>>

Una vignetta sul tema:

<<http://hubert.mycomicspage.com/mikeluckovich/2008/05/22>>

Spiare i monitor altrui utilizzando oggetti riflettenti:

<<http://government.zdnet.com/?p=3825>>

<<http://www.infsec.cs.uni-sb.de/~unruh/publications/reflections.pdf>>

Uno studio affascinante su rischio e cultura, condotto dal Cultural Cognition Project alla Yale Law School:

<<http://research.yale.edu/culturalcognition/content/view/124/89/>>

<http://www.schneier.com/blog/archives/2008/05/risk_and_cultur.html>

Vi è una battaglia in corso fra BlackBerry e il governo indiano in merito alle chiavi crittografiche e alla possibilità di intercettare il traffico email:

<http://www.schneier.com/blog/archives/2008/05/blackberry_givi_1.html>

Ottimo articolo del Rolling Stone sulla sorveglianza in Cina:

<http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print>

oppure <<http://tinyurl.com/66r9z6>>

Il Regno Unito vuole monitorare tutte le chiamate telefoniche e i messaggi email -- per combattere il terrorismo, naturalmente.

<<http://news.bbc.co.uk/1/hi/uk/7409593.stm>>

<http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article3965033.ece>

oppure <<http://tinyurl.com/5eafvt>>

<<http://www.guardian.co.uk/politics/2008/may/20/justice.privacy>>

<<http://news.bbc.co.uk/go/em/fr/-/1/hi/technology/7410885.stm>>

Il codice Fermilab, sia la sfida iniziale che la decodifica:

<<http://it.slashdot.org/it/08/05/16/146252.shtml>>

<<http://it.slashdot.org/it/08/05/20/0114211.shtml>>

The Onion sulle teorie complottiste dell'11 settembre, sulla sicurezza aeroportuale e sul voto:

<http://www.theonion.com/content/video/9_11_conspiracy_theories>

<http://www.theonion.com/content/video/reporters_expose_airport_security>

oppure <<http://tinyurl.com/2au7aq>>

<http://www.theonion.com/content/video/diebold_accidentally_leaks>

Uno spray nasale di ossitocina aumenta la fiducia verso gli estranei. In ogni caso, se permettete a qualcuno di spruzzare una sostanza nel vostro naso, probabilmente avete già una certa fiducia in lui.

<<http://news.bbc.co.uk/1/hi/health/7412438.stm>>

Ecco il testo e il filmato degli interventi di Dan Geer a Source Boston 2008 -- sostanzialmente una riunione di L0pht con amici. Dan Geer parla di sicurezza, monocultura, metrica, evoluzione, e così via. Molte divagazioni, ma comunque interessante.

<<http://geer.tinho.net/geer.sourceboston.txt>>

<<http://sourceboston2008.blip.tv/file/759111/>>

Non è che non pensavamo fosse possibile tracciare le persone mediante i loro cellulari; era solo questione di tempo prima che qualcuno iniziasse a farlo.

<http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ece>

oppure <<http://tinyurl.com/466pjc>>

<<http://spyblog.org.uk/2008/05/path-intelligence-phorm-for-shopping-centres.html>>

oppure <<http://tinyurl.com/6a6zcx>>

<<http://spyblog.org.uk/2008/05/path-intelligence-footpathtm-a-few-more-details.html>>

oppure <<http://tinyurl.com/5dj2tg>>

Rilevatore di esplosivi spray:

<<http://www.rsc.org/AboutUs/News/PressReleases/2008/GlowingExplosiveDetector.asp>>

>

oppure <<http://tinyurl.com/5mf7r8>>

Materiale interessante sugli strumenti di sicurezza a linea di comando incorporati in Windows:

<http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1303709,00.html>

oppure <<http://tinyurl.com/6npur9>>

<http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1313370,00.html>

oppure <<http://tinyurl.com/5wq86b>>

Nolan Bushnell sostiene che il trusted computing metterà fine alla pirateria. Heh, proprio divertente.

<http://www.schneier.com/blog/archives/2008/05/tpm_to_end_pira.html>

Jared Diamond scrive sul sentimento di vendetta e la natura umana:

<http://www.newyorker.com/reporting/2008/04/21/080421fa_fact_diamond>

Bletchley Park potrebbe chiudere per mancanza di fondi:

<<http://resources.zdnet.co.uk/articles/imagegallery/0,1000002003,39415278,00.htm>>

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

Per effettuare una donazione:

<<http://www.bletchleypark.org.uk/shop/changeDonate.rhtm/-1>>

<<http://www.bletchleypark.org.uk/content/contact/donation.rhtm>>

Electronic Crime Scene Investigation: A Guide for First Responders [Indagine elettronica della scena di un crimine: una guida per i primi soccorritori], Seconda edizione, National Institute of Justice, U.S. Department of Justice, aprile 2008.

<<http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>>

Questo articolo sostiene che l'Esercito Popolare di Liberazione cinese è responsabile, fra le altre cose, del blackout dell'agosto 2003. Tutto questo è un tale ammasso di sciocchezze che non so da dove cominciare. Ho già parlato di quel blackout: i guasti informatici furono provocati da Blaster. Ovviamente, interruzioni della rete elettrica di così vasta portata non sono mai una cosa sola. Si tratta di un piccolo problema che si trasforma in una serie di problemi più grandi mediante un effetto valanga. Ma il problema scatenante è stato la rete elettrica.

<http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php>

La teoria smontata da Wired:

<<http://blog.wired.com/27bstroke6/2008/05/did-hackers-cau.html>>

Il mio intervento in merito al blackout:

<<http://www.schneier.com/essay-002.html>>

Questo filmato è bellissimo. Una troupe televisiva di Washington DC si reca a Union Station per intervistare qualcuno della Amtrak in merito a persone a cui è stato impedito di scattare foto, malgrado non esista alcuna normativa che lo vieti. Mentre il portavoce della Amtrak sta spiegando che non esiste alcuna policy contro la fotografia, una guardia si avvicina alla troupe e cerca di impedirle di filmare, dicendo che è contro le regole.

<<http://www.myfoxdc.com/myfox/pages/Home/Detail;jsessionid=C5EB861DC520F425C08BB9C1199CDDE5?contentId=6664418&version=2&locale=EN-US&layoutCode=VSTY&pageId=1.1.1&sflg=1>>

oppure <<http://tinyurl.com/4xr58o>>

<http://theonlinephotographer.typepad.com/the_online_photographer/2008/06/union-station-p.html>

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

The Center for American Progress ha pubblicato il proprio studio sull'identificazione e sulle tecnologie di identificazione: "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society" [La linea di demarcazione dell'identità: affrontare le problematiche di identificazione e di autenticazione nella società americana]. Ero uno dei partecipanti al progetto che ha creato questo studio, e vale la pena leggerlo. Fra le altre cose, lo studio identifica sei principi per i sistemi di identificazione: 1) ottenere sicurezza reale o simili obiettivi, 2) precisione, 3) inclusione, 4) imparzialità e precisione, 5) efficaci meccanismi di indennità, 6) finanziamenti equi per i sistemi.

<http://www.americanprogress.org/issues/2008/06/id_divide.html>

Una brillante truffa a base di micro-depositi: "Michael Largent, 22 anni, di Plumas Lake, California, pare abbia sfruttato una incongruenza di una comune procedura che entrambe le aziende seguono quando un cliente collega per la prima volta il proprio conto di intermediazione a un conto bancario. Per verificare che il numero di conto e le informazioni di routing siano corrette, l'azienda di intermediazione versa automaticamente piccoli 'micro-depositi' (che ammontano da 2 cent a un dollaro) sul conto, e chiedono al cliente di verificare l'avvenuto accredito. Pare che Largent abbia utilizzato uno script automatico per aprire 58.000 conti di intermediazione online, collegando ognuno di essi a un gruppo di conti correnti online, e accumulando migliaia di dollari in micro-depositi.

<<http://blog.wired.com/27bstroke6/2008/05/man-allegedly-b.html>>

E questo è un brillante furto in un museo:

<http://www.schneier.com/blog/archives/2008/06/clever_museum_t.html>

Dei ricercatori presso l'Università di Washington hanno dimostrato quanto siano pessime le tattiche della MPAA / RIAA / ecc. riuscendo a ingannare le stampanti sulla propria rete. Queste stampanti, che non possono scaricare nulla, hanno ricevuto nove avvisi di arresto per violazione di copyright:

<<http://bits.blogs.nytimes.com/2008/06/05/the-inexact-science-behind-dmca-takedown-notice/>>

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

<<http://dmca.cs.washington.edu/>>

Ottimo prodotto per alimentare la paura: un kit di sopravvivenza in caso di emergenza in metropolitana.

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

In India i Sikh possono portare coltelli a bordo degli aerei. Come la sicurezza in aeroporto sia in grado di riconoscere un Sikh non viene spiegato, però.

<<http://fateh.sikhnet.com/sikhnet/discussion.nsf/ca32680024ff68b487256a08007e86d8/e3121b2ca1969bec87256d42003f211a!OpenDocument>>

oppure <<http://tinyurl.com/4uw9ts>>

Stanno installando delle difese preventive sugli autobus per evitare che qualche terrorista voglia reinterpretare il film "Speed" nella vita reale:

<http://www.nypost.com/seven/06082008/news/regionalnews/busting_terror_114567.htm>

oppure <<http://tinyurl.com/5p5kaj>>

FakeTV è un dispositivo antifurto che simula un televisore.

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

La TSA ha una nuova regola per i documenti di identità con foto: a chi si rifiuta di mostrare un documento identificativo per principio non sarà permesso volare, ma chi dichiarerà di aver perduto i documenti potrà imbarcarsi. Mi sento molto ben protetto contro tutti quei terroristi che non sanno mentire.

<http://www.tsa.gov/press/happenings/enhance_id_requirements.shtm>

<http://news.cnet.com/8301-13739_3-9962760-46.html>

Non credo che servano ulteriori prove per dimostrare che l'obbligo di avere con sé un documento d'identità non ha niente a che vedere con la sicurezza, e ha tutto a che vedere con il controllo.

<<http://www.schneier.com/essay-008.html>>

<<http://www.schneier.com/essay-052.html>>

<<http://www.schneier.com/essay-132.html>>

<<http://techliberation.com/2008/06/09/id-checks-are-about-control-not-security/>>

oppure <<http://tinyurl.com/57gyym>>

<http://www.concurringopinions.com/archives/2008/06/the_new_tsa_ide.html>

Secrecy, il film:

<<http://www.secrecyfilm.com/index.html>>

<<http://www.cqpolitics.com/wmspage.cfm?parm1=5&docID=hsnews-000002721511>>

oppure <<http://tinyurl.com/5gpd9g>>

<<http://www.imdb.com/title/tt1157709/>>

<<http://www.imdb.com/title/tt1157709/externalreviews>>

Non riesco a dare un senso a questa storia. Kaspersky Lab sta lanciando un lavoro di calcolo distribuito internazionale per craccare una chiave RSA a 1024 bit utilizzata dal virus Gpcode. Dal loro sito Web: "Secondo le nostre stime, per craccare una chiave del genere saranno necessari circa 15 milioni di moderni computer che svolgano calcoli per un anno". Che cosa stanno fumando a Kaspersky? Non abbiamo mai fattorizzato un numero a 1024 bit -- almeno, non al di fuori di un'agenzia governativa segreta -- e probabilmente sarà necessario molto più di un anno di lavoro di 15 milioni di computer. L'attuale record di fattorizzazione è un numero di 1023 bit, ma si tratta di un numero speciale che è più facile da fattorizzare rispetto a un numero che è il prodotto di due numeri primi, come quelli utilizzati nella RSA. Per craccare la chiave di Gpcode sarà necessaria molta più bravura matematica di quella che ci si può ragionevolmente aspettare chiedendo educatamente in Internet. È necessario comprendere le migliori ottimizzazioni attuali, matematiche e computazionali, del Number Field Sieve, e distribuire in modo intelligente le parti che possono essere distribuite. Non basta limitarsi a pubblicare i prodotti e sperare per il meglio.

<<http://forum.kaspersky.com/lofiversion/index.php/t71652.html>>

<http://news.cnet.com/8301-10784_3-9965381-7.html>

<<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9094818>>

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

Documenti top secret del governo britannico su al Qaeda dimenticati su un treno a Londra. Oops.

<http://news.bbc.co.uk/2/hi/uk_news/7449255.stm>

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

Email dopo il Ratto Salvifico

È facile farsi quattro risate guardando il sito You've Been Left Behind [Non Siete Stati Scelti], che pretende di inviare email automatiche ai vostri amici dopo il Ratto Salvifico:

"I non salvati verranno 'lasciati alle spalle' sulla terra per passare attraverso il 'periodo di tribolazione' dopo il 'Ratto Salvifico'... Con il nostro servizio potrete inviare loro una lettera di amore e la richiesta di ricevere Cristo un'ultima volta. Potrete inoltre dar loro un po' di aiuto per vivere il loro tempo residuo. Nella parte cifrata del vostro account potete offrire loro accesso ai vostri conti bancari, di intermediazione, ai vostri oggetti di valore nascosti, alle vostre procure (non ne avrete più bisogno, e questo dono manderà un messaggio d'amore). Non vi saranno corpi, quindi l'organo competente per l'autenticazione dei testamenti ci metterà 7 anni per trasmettere i vostri beni al parente più prossimo. 7 anni è tutto quel che rimane, per cui il Governo dell'Anticristo otterrà i vostri beni a meno che non li rendiate disponibili in altro modo".

Ma che succede se il creatore di questo sito non è così scrupoloso come dà a intendere? Che succede se fa uso di tutte quelle informazioni, conti correnti, password, combinazioni di casseforti, ecc., PRIMA di qualsiasi Ratto Salvifico? E anche se si trattasse di un onesto credente, questo mi sembra un bersaglio enormemente allettante per qualunque aspirante ladro di identità.

E, se siete curiosi, così funziona il meccanismo di innesco della procedura:

“Abbiamo impostato un sistema per inviare i documenti via email, agli indirizzi da voi forniti, 6 giorni dopo il ‘Ratto Salvifico’ della Chiesa. Questo avviene quando 3 dei nostri 5 membri della squadra sparsi per gli Stati Uniti non effettuano il login passato un periodo di 3 giorni. Altri 3 giorni vengono concessi come misura di sicurezza in caso di falsi inneschi del sistema”.

Il sito dichiara che i dati possono essere cifrati, ma pare che la chiave crittografica sia conservata nel server insieme ai dati.

<<http://www.youvebeenleftbehind.com/index-3.html>>

Questo è un sito simile, gestito da atei, così possono garantire che verranno ‘lasciati alle spalle’ e che potranno distribuire tutti i messaggi:

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

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

Le firme via fax

Le firme sui fax sono un caso veramente curioso. È facilissimo tagliare e incollare (letteralmente, con forbici e colla) la firma di chiunque su un documento così che sembri vera quando si invia un fax. C’è così poca sicurezza nelle firme via fax che è incredibile che continuino a essere accettate.

Eppure e così, nelle situazioni più varie. Ho firmato contratti librari, autorizzazioni di carte di credito, accordi di non divulgazione e ogni genere di documento finanziario -- tutti via fax. Sul computer ho persino un file con la mia firma scansionata, così che posso inserirla in qualsiasi documento e mandarlo via fax direttamente dal computer senza nemmeno effettuare una stampa. Che caspita sta succedendo qui?

E, soprattutto, perché si continua a ricorrere alle firme via fax dopo anni e anni di esperienza? Perché non si sentono molte storie di firme falsificate utilizzando un fax?

La risposta si ottiene considerando le firme sui fax non come una isolata misura di sicurezza, ma nel contesto dell’intero sistema. Le firme via fax funzionano perché i fax firmati esistono all’interno di un contesto di comunicazione più ampio.

In uno studio del 2003, “Economics, Psychology, and Sociology of Security” [Economia, Psicologia e Sociologia della Sicurezza], il professor Andrew Odlyzko considera le firme via fax e conclude: “Anche se le firme sui fax sono ormai molto diffuse, il loro utilizzo rimane ristretto. Non vengono impiegate per chiudere contratti di un certo valore, come acquisti di immobili. Ciò significa che l’insicurezza delle comunicazioni via fax non è semplice da sfruttare per ottenere guadagni consistenti. Un’ulteriore misura di protezione contro l’abuso dell’insicurezza dei fax è data dal contesto in cui gli stessi fax vengono utilizzati. Vi sono i registri delle chiamate effettuate per trasmettere i fax, tracciati cartacei all’interno delle aziende, e così via. Inoltre, improvvisi trasferimenti di

grandi somme di denaro innescano immediatamente una verifica. Di conseguenza è difficile riuscire a effettuare una frode con mezzi puramente tecnici”.

Ha ragione. Ripensandoci, non vi sono poi tanti modi con cui un criminale potrebbe servirsi di un documento falsificato inviato via fax per frodarmi. Immagino che un cliente senza scrupoli a cui faccio consulenze potrebbe falsificare la mia firma su di un accordo di non divulgazione e poi denunciarmi, ma non mi pare che ne valga la pena. E se il mio broker ricevesse un documento via fax con la mia firma per autorizzare un bonifico verso un conto bancario nigeriano, sicuramente mi chiamerebbe prima di approvarlo.

Neanche le firme delle carte di credito vengono verificate di persona, e ormai posso acquistare di tutto per telefono con una carta di credito, quindi non vi sono nuovi rischi, e poi Visa sa come esaminare le transazioni in caso di frode. Molte aziende accettano ordini di acquisto via fax, anche per grossi quantitativi, ma esiste un audit trail fisico, e la merce viene spedita a un indirizzo vero e proprio -- probabilmente un indirizzo che il venditore ha già utilizzato in precedenza. Le firme sono una specie di lubrificante di mercato: nella maggior parte dei casi contribuiscono a far andare avanti le cose senza intoppi.

Ma non sempre.

Il 30 ottobre 2004, Tristian Wilson è stato rilasciato da un penitenziario di Memphis grazie a un messaggio falso spedito via fax. Non si trattò nemmeno di un capolavoro di falsificazione. Non era stampato sulla carta intestata del West Memphis Police Department. Il nome del poliziotto era scritto erroneamente. E la data e l'ora in cima al fax indicavano chiaramente che il messaggio era stato inviato da un vicino McDonald's.

Il successo di questa frode non ha niente a che vedere con il fatto che il messaggio è stato mandato via fax. Ha funzionato perché il penitenziario aveva delle pessime procedure di verifica. Non hanno notato alcuna discrepanza nel fax. Non hanno notato il numero di telefono da cui il fax era stato spedito. Non hanno chiamato per verificare che la comunicazione fosse ufficiale. Il penitenziario era abituato a ricevere ordini di scarcerazione via fax, e ha semplicemente trattato questo ennesimo fax senza riflettere. Sarebbe stato diverso se il messaggio fasullo fosse stato inviato per posta o con un corriere?

Certo, le firme sui fax esistono sempre all'interno di un contesto, ma a volte sono il fulcro di quel contesto. Se si riesce a imitare una buona parte del contesto, o se coloro che ricevono la comunicazione via fax sono troppo presi da se stessi per accorgersi di qualcosa, allora è possibile farla franca.

E questo è parte del processo di sicurezza. Le stesse firme non sono definite con precisione. A volte un documento è valido anche se non è firmato: una persona con entrambe le mani ingessate può ugualmente acquistare una casa. A volte un documento non è valido anche se firmato: il firmatario potrebbe essere ubriaco o avere una pistola puntata alla testa. O potrebbe essere un minore. A volte non basta una firma valida: negli Stati Uniti esiste un'intera infrastruttura di "notary publics" (soggetti abilitati all'autenticazione delle firme) che servono da testimoni oculari durante la firma di documenti. Quando ho iniziato a inviare la mia dichiarazione dei redditi in forma elettronica, ho dovuto firmare un documento dichiarando che non avrei firmato i documenti della dichiarazione dei redditi. E le banche non si scomodano nemmeno per

verificare le firme su assegni per cifre minori di 30.000 dollari: è più economico gestire la frode a fatto compiuto che prevenirla.

Nel corso dei secoli, i sistemi legali e finanziari hanno lentamente stabilito quali sono i controlli aggiuntivi richiesti nel trattare le firme e in quali circostanze effettuarli.

Quegli stessi sistemi saranno in grado di inquadrare anche le firme sui fax, ma ci vorrà tempo. Ed è a questo punto che vi saranno potenziali problemi. Il fax è già una tecnologia in declino. In pochi anni sarà in gran parte obsoleto, rimpiazzato da PDF inviati via email e da altre forme di documentazione elettronica. In passato abbiamo avuto tempo di comprendere come interagire con le nuove tecnologie. Ora, prima di riuscire a istituzionalizzare queste misure, probabilmente quelle tecnologie saranno obsolete.

Ciò significa che la gente finirà col trattare le firme sui fax (o qualsiasi altra soluzione che le sostituirà) esattamente come normali firme su documenti cartacei. E a volte tale assunzione sarà fonte di problemi.

Ma non provocherà nessun disastro sociale. La storia di Wilson è notevole più che altro perché è davvero eccezionale, fuori dalla norma. E poi fu arrestato nuovamente a casa sua dopo una settimana. Le firme sui fax possono essere una novità, ma le firme fasulle sono sempre state una possibilità. I nostri sistemi legali e finanziari devono affrontare il problema sottostante -- l'autenticazione fasulla -- invece di concentrarsi sulla tecnologia del momento. I sistemi devono potersi difendere contro la possibilità di firme false, a prescindere dal mezzo con cui arrivano.

Lo studio di Odlyzko:

<<http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf>>

Tristian Wilson:

<<http://www.theeveningtimes.com/articles/2004/11/04/news/news5.txt>>

Questo articolo è originariamente apparso su Wired.com:

<http://www.wired.com/politics/security/commentary/securitymatters/2008/05/securitymatters_0529>

oppure <<http://tinyurl.com/3eoj8w>>

Un'altra storia di un fax falsificato: "Un tribunale federale dichiara colpevole un avvocato di New York dell'accusa di aver falsificato l'ordinanza di un giudice".

<<http://www.law.com/jsp/article.jsp?id=1124960718229>>

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

La guerra alle T-shirt

La sicurezza dell'aeroporto di Heathrow, Londra, non ha permesso a una persona di imbarcarsi su un aereo perché indossava una T-shirt dei Transformers su cui era disegnata una pistola.

È facile ridere e tirare avanti. Ci si chiede quanto stupidi possano essere gli addetti alla sicurezza. Ma vi è una lezione di sicurezza molto più importante, qui. Effettuare uno screening è difficile, e per ogni falsa minaccia sulla quale gli screener si soffermano, aumenta la possibilità che le vere minacce passino inosservate. A una festa l'altra sera, una persona mi ha raccontato della volta in cui ha fatto passare per errore un grosso coltello al checkpoint di sicurezza. Lo screener ha messo da parte la sua valigia, l'ha perquisita, e ne ha estratto una bottiglia d'acqua.

Non sono soltanto le bottiglie d'acqua e le T-shirt e i gioielli a forma di pistola -- questo genere di cose ci rende tutti meno sicuri.

<<http://www.thesun.co.uk/sol/homepage/news/article1234193.ece>>
<<http://news.bbc.co.uk/1/hi/england/london/7431640.stm>>

Screening di sicurezza:

<http://www.schneier.com/blog/archives/2006/03/airport_passeng.html>

Non portare a bordo gioielli a forma di pistola:

<http://www.kelownadailycourier.ca/top_story.php?id=112322&type=Local>

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

Le news su Schneier/BT Counterpane

Registrazione audio dell'intervento di Schneier al Weisman Art Museum a Minneapolis il 27 marzo.

<<http://weisman.umn.edu/exhibits/Shambroom/audio.html>>

Un filmato del discorso di Schneier alla Hack-in-the-Box conference a Dubai il 16 aprile.

<<http://videos.hitbsecconf.org/1.html>>

Una Domanda e Risposta pubblicata da CSO Magazine:

<http://www.csoonline.com/article/373414/Bruce_Schneier_Q_A_The_Endless_Broadening_of_Security>

oppure <<http://tinyurl.com/52vbh2>>

Un articolo su Schneier pubblicato da "The Star" in Malesia:

<<http://star-techcentral.com/tech/story.asp?file=/2008/6/5/itfeature/1337626&sec=itfeature>>

oppure <<http://tinyurl.com/6bv2j>>

Una frottola su Schneier: "Bruce Schneier and the King of the Crabs" [Bruce Schneier e il Re dei Granchi]

<http://www.vivtek.com/fiction/singularity_tales/tale_crab.html>

Un divertente poster motivazionale con un'immagine di Schneier:

<http://www.thesatya.com/blog/2008/06/bruce_security.html>

Schneier parlerà alla Supernova conference a San Francisco il 17 giugno:

<<http://www.supernova2008.com/>>

Schneier intervorrà agli Studi Interdisciplinari sull'Information Security a Monte Verità in Svizzera.

<<http://isis.epfl.ch/MV/index.html>>

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

Ancora sulle telecamere nei sedili degli aerei

Ne ho già parlato una volta sul mio blog: si tratta di un sistema di telecamere montate nei sedili degli aerei che cercano di rilevare i terroristi prima che agiscano e mettano in pratica qualunque cosa abbiano preparato. Incredibilmente, l'Unione Europea sta "testando" questo sistema.

È davvero una stupidaggine. Tutto ciò che farà sarà creare falsi allarmi. Nessuno conosce quali caratteristiche facciali siano indicative di un terrorista. E come caspita è possibile "testare" il sistema senza veri terroristi? E in ogni caso, che succede quando scatta l'allarme? Come può un preavviso di dieci secondi salvare delle vite umane?

Certo, si può inventare una tattica terroristica in cui un sistema del genere, assumendo che funzioni davvero, possa salvare delle persone -- ma è esattamente la definizione di minaccia da trama cinematografica. Perché non investiamo questi soldi in qualcosa che sia efficace in molte più situazioni che non soltanto in alcune, accuratamente selezionate?

<http://www.reghardware.co.uk/2008/05/31/airliner_security_safee/>

<http://www.schneier.com/blog/archives/2007/02/the_doghouse_on.html>

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

Come vendere la sicurezza

Nelle vendite è risaputo che è più facile vendere a qualcuno qualcosa che vuole rispetto a una difesa contro qualcosa che vuole evitare. La gente è riluttante ad acquistare polizze di assicurazioni, dispositivi per la sicurezza domestica, o qualsiasi strumento di sicurezza informatica. Non è che non comprano mai queste cose, ma è sempre una lotta difficile.

I motivi sono psicologici. Ed è la stessa dinamica, che si tratti di un produttore di sicurezza nel tentativo di vendere i propri prodotti o servizi, di un CIO che prova a convincere l'amministrazione a investire in sicurezza, o di un funzionario di sicurezza che cerca di implementare una policy di sicurezza per gli impiegati della sua azienda.

È anche vero che più si comprende l'acquirente, meglio si può vendere.

Partiamo anzitutto dalla prospect theory, la teoria che sta alla base del settore nuovamente popolare dell'economia comportamentale. La prospect theory fu sviluppata da Daniel Kahneman e Amos Tversky nel 1979 (Kahneman proseguì e vinse un premio

nobel per questo e altri simili lavori) per spiegare come le persone prendono decisioni e accettano compromessi riguardanti il rischio. Prima di questa ricerca, gli economisti avevano un modello di "uomo economico", un essere razionale che affronta i compromessi basandosi su una serie di calcoli logici. Kahneman e Tversky dimostrarono che le persone vere sono molto più indefinibili e capricciose.

Ecco un esperimento che illustra la prospect theory. Prendiamo delle persone riunite in una stanza e dividiamole in due gruppi. Al primo gruppo si chiederà di scegliere fra queste due alternative: un guadagno sicuro di 500 dollari e la probabilità al 50% di guadagnare 1.000 dollari. Al secondo gruppo si chiederà di scegliere fra queste due alternative: una perdita sicura di 500 dollari e la probabilità al 50% di perdere 1.000 dollari.

Questi due compromessi sono molto simili, e secondo l'economia tradizionale, che si stia valutando un guadagno o una perdita non fa differenza: le persone decidono in base a semplici calcoli del risultato relativo. Alcune persone preferiscono le sicurezze e altre preferiscono prendersi dei rischi. Che il risultato sia una perdita o un guadagno non influenza i conti, e quindi non dovrebbe influire sui risultati. Questa è economia tradizionale e viene chiamata utility theory, teoria dell'utilità.

Ma gli esperimenti di Kahneman e Tversky hanno contraddetto la teoria dell'utilità. Di fronte a un guadagno, l'85% dei soggetti ha scelto la certezza del guadagno minore rispetto al rischio di un guadagno maggiore. Ma di fronte a una perdita, circa il 70% dei soggetti ha preferito scegliere il rischio di una perdita maggiore rispetto alla certezza di una perdita minore.

Questo esperimento, ripetuto più volte da molti ricercatori, con soggetti di età, sesso, culture, persino razze differenti, ha dato gli stessi risultati. In diretta contraddizione rispetto all'idea tradizionale di "uomo economico", la prospect theory riconosce che le persone danno un valore soggettivo alle perdite e ai guadagni. Abbiamo evoluto un bias cognitivo: una coppia euristica. Uno, un guadagno sicuro è meglio della probabilità di un guadagno maggiore (in altre parole, meglio un uovo oggi che una gallina domani). Due, una perdita sicura è peggio della probabilità di una perdita maggiore. Naturalmente non si tratta di regole rigide. Solo uno sciocco accetterebbe 100 dollari sicuri di fronte al 50% di probabilità di ottenere 1.000.000 di dollari. Ma a meno di imprevisti, tendiamo a evitare il rischio quando si tratta di guadagni e tendiamo ad accettare il rischio quando si tratta di perdite.

Questo bias cognitivo è così potente che può portare a risultati incoerenti dal punto di vista logico. Si cerchi in Google "Asian Disease Experiment" per averne un esempio quasi surreale. Descrivere la stessa politica di scelte in modi diversi -- dire "200 vite salvate su 600" oppure "400 vite perse su 600" -- può portare a reazioni di rischio completamente differenti.

Da un punto di vista evolutivo, il bias ha senso. È una strategia di sopravvivenza migliore accettare piccoli guadagni invece di rischiarli per ottenere guadagni maggiori, e rischiare grosse perdite invece di accettare perdite di minor entità. I leoni inseguono i giovani o feriti perché l'investimento necessario per ucciderli è più basso. Prede più mature e in salute sarebbero forse più nutrienti, ma vi è il rischio di saltare completamente il pranzo se tali prede riuscissero a fuggire. E un pasto, anche piccolo, aiuterà il leone a tirare avanti un altro giorno. Arrivare in fondo alla giornata di oggi è più importante della possibilità di avere cibo domani. Analogamente è meglio rischiare

una perdita più grande che non accettarne una minore. Dato che gli animali tendono a vivere sul filo del rasoio tra fame e riproduzione, ogni perdita di cibo, grande o piccola che sia, può essere qualcosa di grave. Perché in entrambi i casi il rischio è la morte, e la scelta migliore è rischiare tutto senza aver nulla da perdere.

Come spiega la prospect theory la difficoltà di vendere la prevenzione di una falla di sicurezza? È la scelta fra una piccola perdita sicura (il costo del prodotto di sicurezza) e il rischio di una perdita ben più grande: per esempio, il risultato dell'attacco ai danni di una rete. Naturalmente in vendita c'è ben di più. Il compratore deve essere convinto che il prodotto funzioni, e deve comprendere le minacce contro di lui e il rischio che possa accadere qualcosa di grave. Ma a meno di imprevisti, i compratori preferiscono correre il rischio e pensare alla possibilità che tale attacco non avvenga, piuttosto che patire la perdita certa rappresentata dall'acquisto del prodotto di sicurezza.

Chi vende sicurezza lo sa, anche se non ne capisce le ragioni, e cerca continuamente di presentare i propri prodotti in un'ottica di risultati positivi. Ecco perché si vedono slogan che trasmettono sostanzialmente questo messaggio: "Noi ci prendiamo cura della sicurezza, così che voi possiate concentrarvi sulla vostra attività", o modelli di redditività del capitale investito accuratamente congegnati per dimostrare quanto può essere redditizio acquistare un prodotto di sicurezza. Ma questi non sembrano funzionare mai. La sicurezza è fondamentalmente una vendita negativa.

Una soluzione è quella di alimentare la paura. La paura è un'emozione primaria, molto più antica della nostra capacità di calcolare compromessi. E quando la gente è spaventata davvero, è disposta a tutto pur di scacciare quella sensazione; esistono un'infinità di ricerche in ambito psicologico che lo dimostrano. Ogni venditore di allarmi antifurto vi dirà che la gente compra soltanto dopo essere stata derubata, o dopo che un loro vicino è stato derubato. E le paure alimentate dall'11 settembre, e le politiche intorno all'11 settembre, hanno creato un'intera industria dedicata all'antiterrorismo. Quando le emozioni hanno la meglio in questo modo, è difficile che le persone si mettano a pensare razionalmente.

Alimentare il terrore, anche se efficace, non è un metodo molto etico. La soluzione migliore è quella di non vendere la sicurezza direttamente, ma di includerla come parte di un prodotto o servizio più generali. La vostra auto è dotata di funzioni di sicurezza incorporate, non vengono vendute separatamente. Stesso dicasi per la vostra casa. E dovrebbe essere la stessa cosa anche per computer e reti. I produttori devono inserire la sicurezza all'interno dei prodotti e dei servizi che le persone vogliono veramente. I CIO dovrebbero includere la sicurezza come parte integrante di ogni cosa per la quale calcolano un budget. La sicurezza non dovrebbe essere una policy distinta per i dipendenti di un'azienda, ma andrebbe integrata in una policy IT più generale.

La sicurezza, intrinsecamente, significa evitare un negativo, per cui non si può ignorare il bias cognitivo radicato in profondità nel cervello umano. Ma se lo si comprende, sarà meno difficile da superare.

Questo articolo è originariamente apparso su CIO:
<[http://www.cio.com/article/367913/How to Sell Security](http://www.cio.com/article/367913/How_to_Sell_Security)>

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

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.