CRYPTO-GRAM
15 novembre 2009

Scritta da Bruce Schneier
Chief Security Technology Officer di BT
e-mail: schneier@schneier.com
Web: <http://www.schneier.com>

Edizione italiana curata da Communication Valley, Business Unit di Security Reply.
<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-0910.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:

Al di là dei teatrini della sicurezza
Paura e reazioni eccessive
News
Politiche di tolleranza zero
La sicurezza in un'economia basata sulla reputazione
Le news su Schneier
Il braccio di ferro del discorso commerciale
Il Canile: ADE 651
Attacchi di tipo 'Evil Maid' contro dischi criptati
Sono ancora utili gli antivirus?
Commenti dei lettori

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

## Al di là dei teatrini della sicurezza

[Mi è stato chiesto di scrivere questo articolo per il "New Internationalist" (n. 427, novembre 2009, pp. 10-13). Nulla che non abbia già detto in precedenza, ma sono molto soddisfatto di come sia venuto il pezzo].

Il terrorismo è un fenomeno raro, molto più raro di quanto si pensi. È raro perché il numero di persone che intendono commettere atti terroristici è molto ristretto, ed eseguire un complotto di matrice terroristica è molto più arduo di quanto la televisione lo faccia sembrare. Le difese migliori contro il terrorismo sono in gran parte invisibili: investigazione, intelligence e risposta alle emergenze. Ma anche queste difese sono meno efficaci per la nostra protezione rispetto alla nostra condotta politica e sociale, a livello nazionale e internazionale. Tuttavia i nostri leader eletti non la pensano così, ed è molto più probabile che implementino una messinscena di sicurezza contro le minacce da trama cinematografica.

Una minaccia da trama cinematografica è uno scenario di attacco estremamente specifico. Che si tratti di terroristi muniti di polverizzatori usati in agricoltura, di terroristi che contaminano le forniture di latte, o terroristi che prendono di mira i giochi olimpici, sono le storie a far leva sulle nostre emozioni, in una forma molto più intensa di qualsiasi serie di dati impersonali. Sono le storie quelle che temiamo. E non solo vicende ipotetiche: terroristi che fanno schiantare aerei contro gli edifici, terroristi che nascondono bombe nelle proprie scarpe o in bottiglie d'acqua, e terroristi muniti di bombe e armi da fuoco che conducono un attacco coordinato contro una città sono minacce da trama cinematografica ancor più paurose perché sono fatti realmente accaduti.

Il 'security theater', ovvero la messinscena, il teatrino della sicurezza, si riferisce a misure di sicurezza che fanno sentire le persone più sicure senza far nulla di concreto per migliorarne davvero la sicurezza. Un esempio: i controlli dei documenti con foto, sempre più diffusi nei palazzi di uffici. Nessuno ha mai spiegato perché il verificare che qualcuno abbia un documento con foto sia un'effettiva misura di sicurezza, ma certo dà un'impressione di sicurezza avere una guardia in uniforme che controlla i documenti. Un altro esempio in ambito di sicurezza aeroportuale: truppe della Guardia Nazionale stanziate negli aeroporti nei mesi successivi all'11 settembre, con armi prive di munizioni. Altri esempi comprendono il sistema basato sui colori per indicare i livelli di minaccia, le continue molestie ai danni dei fotografi, e i metal detector sempre più diffusi in hotel e palazzi di uffici a seguito degli attacchi terroristici di Mumbai.

È ragionevole affermare come alcuni bersagli siano innegabilmente più allettanti di altri: gli aerei, perché un ordigno di ridotte dimensioni può provocare la morte di tutti gli occupanti; i monumenti, per il loro significato a livello nazionale; eventi nazionali, per la presenza della televisione e dei media; i trasporti, perché la maggioranza dei lavoratori li utilizza quotidianamente. Ma in un grande paese vi sono letteralmente milioni di bersagli potenziali (solo negli Stati Uniti vi sono cinque milioni di edifici commerciali), e centinaia di potenziali tattiche terroristiche; è impossibile difendere tutti i luoghi da ogni possibile minaccia, ed è impossibile prevedere quale tattica e quale bersaglio sceglieranno i terroristi per il prossimo attacco.

## Percezione e realtà

La sicurezza è al tempo stesso una percezione e una realtà. La propensione alla messinscena di sicurezza proviene dall'interazione fra il pubblico e i suoi leader. Quando le persone sono spaventate hanno bisogno di qualcosa che le faccia sentire sicure, anche se non le protegge per davvero. I politici ovviamente vogliono fare qualcosa in risposta alla crisi, anche se quel qualcosa non ha alcun senso.

Spesso, quel 'qualcosa' è legato direttamente ai particolari di un evento recente: si confiscano liquidi, si controllano le scarpe e si proibiscono i taglierini sugli aerei. Ma a essere importanti non sono le tattiche e il bersaglio dell'attacco precedente, se mai del prossimo. Queste contromisure sono efficaci soltanto se riusciamo a indovinare che cosa stanno architettando i prossimi terroristi. Se spendiamo miliardi di dollari per proteggere le ferrovie e i terroristi piazzano un ordigno esplosivo in un centro commerciale, abbiamo buttato via il denaro. Se concentriamo la sicurezza aeroportuale sul controllo delle scarpe e sul sequestro dei liquidi, e i terroristi nascondono gli esplosivi nella loro biancheria intima e utilizzano esplosivi solidi, è tutto denaro sprecato. Ai terroristi non importa il bersaglio che faranno saltare in aria, e il nostro obiettivo non dovrebbe semplicemente limitarsi a costringere i terroristi a effettuare una lieve modifica alle loro tattiche o bersagli.

La nostra predilezione per le trame terroristiche da film ci rende ciechi alle minacce più generali. E il teatrino della sicurezza consuma risorse che sarebbe meglio investire altrove.

Un attacco terroristico è una serie di eventi, di passaggi: grosso modo si possono distinguere in pianificazione, reclutamento, finanziamento, esercitazione, esecuzione, conseguenze. Le nostre difese più efficaci si trovano all'inizio e alla fine di questo processo -- intelligence, investigazione e risposta alle emergenze -- e le difese meno efficaci sono quelle che richiedono di indovinare correttamente l'intero complotto. Quando parlo di intelligence e investigazione non mi riferisco ai sistemi di data mining e di intercettazione all'ingrosso che sono stati proposti e, in alcuni casi, implementati. Anche quelle sono storie da trama cinematografica senza alcuna provata efficacia. Parlo proprio del classico tipo di indagine in cui si segue una serie di indizi e di prove; è il sistema che ha funzionato per decenni.

Sfortunatamente per i politici, le misure di sicurezza che funzionano sono in gran parte invisibili. Alcune di queste misure comprendono l'aumento delle capacità di raccolta di informazioni di intelligence da parte dei servizi segreti, l'assunzione di esperti culturali e interpreti/traduttori della lingua araba, il costruire legami con le comunità islamiche a livello nazionale e internazionale, finanziamenti per rafforzare le forze dell'ordine -- sia le sezioni investigative per evitare attacchi terroristici, sia i sistemi di comunicazione di emergenza una volta che il disastro è avvenuto -- nonché arrestare i cospiratori senza troppi sensazionalismi da parte dei media. Non comprendono nuove leggi estese di polizia o spionaggio. Le nostre forze di polizia non hanno bisogno di nuove leggi per combattere il terrorismo; ciò di cui necessitano sono finanziamenti privi di orientamento politico. Queste misure di sicurezza non servono a fare della buona televisione, e non aiutano in tempi di rielezioni. Ma funzionano e affrontano la realtà della sicurezza invece della percezione.

L'arresto dei 'dinamitardi liquidi' a Londra è un esempio: i terroristi sono stati catturati grazie a un lavoro di intelligence e di polizia alla vecchia maniera. La loro scelta di

bersaglio (aerei) e tattica (esplosivi liquidi) non ha influito minimamente; sarebbero stati arrestati comunque.

Ma anche se si mettono in pratica tutte queste contromisure non possiamo trascurare la percezione della sicurezza, perché è il nostro metodo di superare collettivamente i danni psicologici provocati dal terrorismo. Però non è il teatrino della sicurezza ciò di cui abbiamo bisogno, ma appelli diretti a quel che proviamo. Il sistema migliore per aiutare le persone a sentirsi sicure è agire in maniera sicura intorno a esse. Invece di reagire al terrorismo con paura, noi (e i nostri leader) dobbiamo reagire in maniera indomita.

Non lasciarsi terrorizzare

Non lasciandoci andare a reazioni eccessive, non reagendo alle minacce da trama cinematografica, non mettendoci sulla difensiva: così dimostriamo la resistenza della nostra società, nelle nostre leggi, nella cultura, nelle libertà. C'è differenza fra l'essere indomiti e la retorica arrogante del 'avanti, fatevi sotto!'. C'è differenza fra l'accettare i rischi intrinseci in una società libera e aperta, e l'esagerare le minacce.

Dovremmo trattare i terroristi come criminali qualsiasi, e offrire loro tutti i benefici di una giustizia vera e aperta -- non soltanto perché dimostra il nostro carattere indomito, ma perché ci rende tutti più sicuri. Quando una società comincia ad aggirare le sue proprie leggi, i rischi per la sua stabilità futura sono molto più grandi del terrorismo.

Sostenendo la vera sicurezza anche se è invisibile, e dimostrando uno spirito indomito malgrado la paura sia più conveniente da un punto di vista politico, richiede coraggio. La demagogia è facile. Ciò di cui abbiamo bisogno sono leader che vogliano fare quel che è giusto e al tempo stesso dire la verità.

Malgrado la retorica del terrore suggerisca l'opposto, il terrorismo non è una minaccia trascendente. Un attacco terroristico non può distruggere lo stile di vita di un paese: è solo la nostra reazione a quell'attacco che può causare un simile danno. Più mettiamo a rischio le nostre stesse leggi, più trasformiamo gli edifici in fortezze, più riduciamo le libertà e i diritti civili che stanno alla base delle nostre società, più contribuiamo a fare il lavoro dei terroristi al loro posto.

Guardiamo come hanno reagito i londinesi a seguito degli attentati dinamitardi ai servizi pubblici nel 2005. In tutto il chiasso e l'allarmismo dei politici e dei media, c'era anche una traccia, una scia di risolutezza. Le persone non sono cadute vittima del terrore. Il giorno dopo hanno ripreso a utilizzare treni e autobus e sono andate avanti a vivere la propria vita. L'obiettivo del terrorismo non è l'uccisione; il terrorismo attacca la mente e si serve delle vittime come accessori. Se non ci lasciamo terrorizzare, togliamo ai terroristi la loro arma principale: la nostra paura.

Oggi possiamo proiettare questo spirito indomito eliminando tutte le misure di sicurezza istituite dopo l'11 settembre e basate essenzialmente sulla paura, e tornare ai livelli precedenti. I nostri leader hanno perso credibilità, e per riottenerla è necessario diminuire le iperboli. Eliminare i sistemi intrusivi di sorveglianza all'ingrosso e i nuovi poteri da stato di polizia. Ripristinare la sicurezza aeroportuale a metodi e livelli anteriori all'11 settembre. Togliere la spavalderia dalla nostra politica estera. Mostrare al mondo che il nostro sistema giudiziario è all'altezza della sfida del terrorismo.

Smettere di dire alla gente di riferire qualsiasi attività sospetta: non serve ad altro che a renderci reciprocamente sospettosi, e ad aumentare la paura e il sentimento di impotenza.

Il terrorismo è sempre stato un fenomeno raro, e malgrado tutto quel che abbiamo sentito riguardo all'11 settembre che avrebbe cambiato il mondo, rimane un fenomeno raro. Persino l'11 settembre non è riuscito a uccidere tante persone quante ne muoiono ogni mese negli Stati Uniti a causa di incidenti stradali. Eppure resiste il mito secondo cui il terrorismo è cosa facile. È facile immaginare trame terroristiche, sia su larga scala -- stile "contaminare le riserve alimentari" -- sia su scala ridotta -- stile "dieci tizi con automobili e armi da fuoco". I film e la televisione alimentano questo mito, per cui molte persone si sorprendono della scarsità degli attacchi in città occidentali dopo l'11 settembre. Sicuramente i successi di intelligence e investigazione hanno reso le cose più difficili ai terroristi, ma soprattutto perché è davvero difficile mettere a punto un attacco terroristico. È arduo trovare dei volontari, coordinare i piani ed eseguirli -- ed è facile commettere errori.

Anche l'antiterrorismo non è cosa facile, specialmente quando abbiamo la tendenza psicologica a mandare tutto all'aria. Dall'11 settembre in avanti ci siamo imbarcati in strategie di difesa di bersagli specifici e tattiche specifiche, reagendo in maniera eccessiva a ogni video terroristico, alimentando paure, demonizzando gruppi etnici, e trattando i terroristi come fossero avversari militari veri e propri, come se avessero il potere di distruggere un intero paese o uno stile di vita -- e tutto questo non fa altro che avvantaggiare i terroristi. Sarebbe meglio far leva sulle forze intrinseche alle moderne democrazie e ai vantaggi naturali che abbiamo sui terroristi: la nostra adattabilità e il nostro istinto di sopravvivenza, la nostra rete internazionale di leggi e di forze dell'ordine, e le libertà e i diritti civili che rendono la nostra società così invidiabile. Il nostro stile di vita è abbastanza aperto da rendere il terrorismo un evento raro; siamo abbastanza attenti da fermare molti dei complotti terroristici esistenti, e sufficientemente indomiti da superare quei rarissimi complotti terroristici che hanno successo. Non serve fingere altrimenti.

Commenti:
<http://www.motherjones.com/kevin-drum/2009/11/security-theater>
<http://jamesfallows.theatlantic.com/archives/2009/11/the_right_kind_of_security.php>
<http://www.economist.com/blogs/gulliver/2009/11/the_future_of_security.cfm>

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

Paura e reazioni eccessive

Essere prede è un lavoraccio. Guardate gli uccellini alla mangiatoia. Sono costantemente in guardia, e si allontaneranno dal cibo (dal facile nutrimento) al minimo rumore o movimento. Dato che non ho mai visto un predatore attaccare un uccello a una mangiatoia, sembra un gran spreco di energie da parte dell'uccello a fronte di una minaccia che non è poi così seria.

Valutare il rischio e reagire di conseguenza è una delle cose più importanti che una creatura vivente deve affrontare. L'amigdala, un'antica parte del cervello la cui evoluzione risale ai pesci primitivi, è preposta a tale funzione. È la responsabile del riflesso di lotta-o-fuga. Adrenalina nel flusso sanguigno, aumento del battito cardiaco, aumento della tensione muscolare, mani sudate: segno che l'amigdala è in azione. Ed è veloce, più rapida della coscienza: mostrate a qualcuno un serpente e la sua amigdala reagirà ancor prima che la sua mente cosciente registri il fatto che sta osservando un serpente.

La paura sta alla base di ogni genere di comportamento animale. Il raggrupparsi in banchi, stormi, greggi, sono tutte misure di sicurezza. Non solo è meno probabile che un membro del gruppo venga mangiato, ma ogni membro del gruppo può dedicare meno tempo a guardarsi dai predatori. Animali tanto diversi come il calabrone e la scimmia evitano il cibo in zone in cui è altamente probabile incontrare predatori. Diverse specie di prede hanno sviluppato svariati richiami di allarme, alcuni sorprendentemente specifici. E certe specie di prede si sono evolute al punto di reagire agli allarmi lanciati da altre specie.

Il biologo evolutivo Randolph Nesse ha studiato le difese animali, in special modo quelle che sembrano essere reazioni esagerate. La maggioranza di tali difese sono sistemi tutto-o-nulla, una creatura non reagisce con vie di mezzo. Uccelli che volano via, oloturie che espellono i loro stomaci, e il vomitare, sono tutti degli esempi. Servendosi della teoria della rilevazione del segnale, Nesse ha dimostrato che ci si aspetta di avere molti falsi allarmi con le difese di tipo tutto-o-nulla. "Il principio del rilevatore di fumo mostra come l'eccessiva reazione di molte difese sia un'illusione. Le difese appaiono esageratamente reattive perché sono 'poco costose' rispetto ai mali da cui proteggono, e perché spesso gli errori derivanti da difese troppo scarse costano molto più cari di errori derivanti da un eccesso di difesa".

Pertanto, secondo la teoria, se il volare costa 100 calorie, sia in termini di volo che di tempo di mancato nutrimento, e vi è 1 possibilità su 100 di essere mangiati se non si vola via, a scopo di sopravvivenza è conveniente consumare ripetutamente fino a 10.000 calorie per volar via al minimo movimento anche se il tasso di falsi allarmi è del 99%. Ogni specie animale ha le proprie statistiche, ma tutte hanno evoluto per perfezionare quel compromesso.

Tutto questo ha senso, finché le condizioni in cui le specie hanno evoluto cambiano più rapidamente delle possibilità di reazione del processo evolutivo. Anche se vi sono molti meno predatori in città, gli uccellini alla mia mangiatoia reagiscono come se si trovassero nella foresta primitiva. Persino gli uccelli in una voliera allo zoo non si rendono conto che il contesto è cambiato.

Gli esseri umani non sono diversi, e al tempo stesso lo sono moltissimo. Anche noi proviamo paura e reagiamo attraverso l'amigdala, ma siamo anche dotati di un cervello cosciente che può ignorare quelle reazioni. E anche noi viviamo in un mondo molto diverso da quello in cui ci siamo evoluti. Le nostre difese istintuali possono essere ottimizzate per i rischi 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 2009. Ma possiamo spingerci al di là della paura, e pensare alla sicurezza in maniera realmente razionale.

Troppo spesso, purtroppo, non lo facciamo. In materia di rischi tendiamo a essere pessimi giudici. Reagiamo in modo esagerato di fronte a rischi rari, ignoriamo i rischi a lungo termine, ingigantiamo quei rischi che sono anche moralmente offensivi. Spesso non sappiamo calcolare i rischi (le minacce, le probabilità, i costi). Quando abbiamo paura, quando siamo veramente impauriti, faremmo praticamente qualsiasi cosa pur di scacciare quella paura. Tanto i politici quanto i commercianti hanno imparato a far leva sulla paura per indurci a fare quel che vogliono.

Una notte durante il mese scorso, mi trovavo in un albergo e fui svegliato da un allarme acuto e fortissimo. Era impossibile ignorarlo, ma ho soppesato i rischi e ho deciso di fare ciò che qualsiasi persona ragionevole avrebbe fatto in tale frangente: sono rimasto a letto e ho aspettato che spegnessero l'allarme. Non c'era motivo di vestirsi, scendere dieci piani di scale e uscire al freddo per quel che inevitabilmente si sarebbe rivelato un falso allarme. Gli incendi di grave entità negli alberghi sono molto rari. A differenza degli uccelletti nella voliera, sapevo come comportarmi.

Potete non essere d'accordo con la mia valutazione dei rischi, e sono sicuro che molti dei clienti dell'albergo sono usciti e si sono riuniti nel punto prefissato in caso di emergenza. Ma è importante riconoscere che la capacità di avere questo tipo di discussione è unicamente umana. Ed è necessario che un tale dibattito avvenga sempre, che si tratti dell'installazione di un antifurto domestico, delle più recenti misure di sicurezza della TSA, o della potenziale invasione militare di un altro paese. Queste cose non fanno parte della nostra storia evolutiva -- non possediamo un istinto naturale per reagire a esse. Le nostre paure spesso sono mal calibrate, e la razionalità è l'unico strumento per controllarle.

Questo articolo è originariamente apparso su DarkReading.com.
<http://www.darkreading.com/blog/archives/2009/11/its_hard_work_b.html>

Comportamenti animali:
<http://judson.blogs.nytimes.com/2009/09/29/where-tasty-morsels-fear-to-tread/>
oppure <http://tinyurl.com/yhosh54>
<http://judson.blogs.nytimes.com/2009/10/06/leopard-behind-you/>

Lo studio di Nesse:
<http://www-personal.umich.edu/~nesse/Articles/Nesse-DefenseReg-EHB-2005.pdf>
oppure <http://tinyurl.com/yz8zmxh>

La valutazione dei rischi:
<http://www.schneier.com/essay-162.html>
<http://www.schneier.com/essay-171.html>
<http://www.schneier.com/essay-170.html>
<http://www.schneier.com/essay-155.html>

Gli incendi negli alberghi sono molto rari:
<http://www.emergency-management.net/hotel_fire.htm>

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

News

Un fuggiasco è stato catturato dopo aver aggiornato il suo status in Facebook:
<http://www.schneier.com/blog/archives/2009/10/helpful_hint_fo.html>

Sei anni di 'Martedì delle patch' di Microsoft:
<http://www.schneier.com/blog/archives/2009/10/six_years_of_pa.html>

Un contatore di carte automatizzato rileva i contatori di carte umani; è sufficiente avere un computer che possa tener traccia di ogni carta da gioco:
<http://www.schneier.com/blog/archives/2009/10/computer_card_c.html>

Una donna pubblica una storia tremenda che tratta degli abusi che ha subito da parte della TSA, e la TSA risponde pubblicando un video che dimostra che la donna stava mentendo.
<http://www.schneier.com/blog/archives/2009/10/tsa_successfull.html>

Un uomo in Australia ha ricevuto una condanna ridotta grazie alla crittografia:
<http://www.news.com.au/couriermail/story/0,23739,26232570-952,00.html>

Secondo Steve Ballmer l'insuccesso di Windows Vista è da imputare alla sicurezza:
<http://www.schneier.com/blog/archives/2009/10/ballmer_blames.html>

James Bamford sulla NSA:
<http://www.schneier.com/blog/archives/2009/10/james_bamford_o.html>

La CIA investe nel data mining delle reti sociali:
<http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/>
oppure <http://tinyurl.com/yl3zud2>
<http://www.visibletechnologies.com/press/pr_20091019.html>

Una storia interessante che risale al 2006 di un hack ai danni di Wal-Mart proveniente, con ogni probabilità, da Minsk.
<http://www.wired.com/threatlevel/2009/10/walmart-hack/>

Ross Anderson ha realizzato un'ottima pagina di risorse su sicurezza e psicologia:
<http://www.cl.cam.ac.uk/~rja14/psysec.html>

Best Buy vende un dispositivo di sorveglianza per soli 99,99 dollari.
<http://www.bestbuy.com/site/olspage.jsp?skuId=9540703&productCategoryId=pcmcat193100050013&type=product&id=1218123143064>
oppure <http://tinyurl.com/yf2nsb8>
Si può anche utilizzare un iPhone allo scopo:
<http://ephermata.livejournal.com/204026.html>

Un articolo essenziale sulla TSA scritto da un ex assistente capo di polizia:
<http://www.hlswatch.com/2009/10/15/%E2%80%9Cdo-i-have-the-right-to-refuse-this-search%E2%80%9D/>
oppure <http://tinyurl.com/ydbox3o>
Un secondo articolo a continuazione del primo, scritto dallo stesso autore:

<http://www.hlswatch.com/2009/11/10/where-are-all-the-white-guys-update-on-do-i-have-the-right-to-refuse-this-search/>

Il Sostituto Direttore del National Intelligence for Collection tiene una conferenza stampa sul nuovo centro per la raccolta dati in Utah.
<http://link.brightcove.com/services/player/bcpid25071315001?bclid=28735328001&bctid=46104965001>
oppure <http://tinyurl.com/yfzb7qm>
Trascrizione:
<http://www.dni.gov/speeches/20091023_speech.pdf>

"Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" [Possibilità della Repubblica Popolare Cinese di condurre una guerra cibernetica e di sferrare attacchi sfruttando la rete], preparato per la US-China Economic and Security Review Commission, Northrop Grumman Corporation, 9 ottobre 2009.
<http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>
oppure <http://tinyurl.com/ygcmh9b>

Scoiattoli 'terroristi' che attaccano la nostra infrastruttura critica.
<http://notionscapital.wordpress.com/2009/10/24/terrorists-strike-u-s-infrastructure/>
oppure <http://tinyurl.com/ykgtadb>
Abbiamo un bias cognitivo che ci induce a ingigantire i rischi provocati da altri esseri umani e a minimizzare i rischi causati dagli animali (e ancor più da fenomeni naturali).

Per facilitare le sue indagini su Wall Street, l'FBI si è servita di DCSNet, il suo sistema di sorveglianza su larga scala.
<http://www.wallstreetandtech.com/blog/archives/2009/10/how_prosecutors.html;jsessionid=0RDUIPWAEEFWFQE1GHPCKHWATMY32JVN>
oppure <http://tinyurl.com/yhnt22q>

Rilevare terroristi annusando la paura:
<http://www.schneier.com/blog/archives/2009/11/detecting_terro.html>

Nello "Open Access Journal of Forensic Psychology" vi è uno studio che tratta dei problemi legati alla sicurezza non scientifica: "A Call for Evidence-Based Security Tools" [Un appello a strumenti di sicurezza basati sulle prove]:
<http://www.schneier.com/blog/archives/2009/11/the_problems_wi_1.html>

Mossad ha hackerato il computer di un ufficiale siriano; era stato lasciato incustodito in una stanza d'albergo.
<http://www.haaretz.com/hasen/spages/1125312.html>
Tenete presente l'attacco 'evil maid': se un aggressore riesce ad avere temporaneamente accesso diretto al vostro computer può aggirare la protezione crittografica.
<http://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html>

Di recente ho parlato della difficoltà di implementare in modo ottimale il controllo degli accessi basato sul ruolo, e di come la ricerca a Dartmouth abbia dimostrato che

l'approccio migliore è di consentire agli utenti tutto l'accesso necessario a svolgere il proprio lavoro, per poi effettuare l'auditing delle operazioni. Questo studio interessante, intitolato "Laissez-Faire File Sharing" [Condivisione di file permissiva] cerca di formalizzare quel tipo di controllo accessi.
<http://www.cs.columbia.edu/~smb/papers/nspw-use.pdf>
<http://www.schneier.com/essay-288.html>

Mi sono astenuto dal commentare in merito al caso contro Najibullah Zazi, semplicemente perché spesso capita che i dettagli riportati dalla stampa hanno ben poco a che fare con la realtà dei fatti. Il mio sospetto era che il tizio fosse (come in molti altri casi analoghi) un idiota incapace di fare davvero del male e che fosse stato trasformato in uno spauracchio per motivi politici. Tuttavia John Mueller (del quale ho già parlato in precedenza) ha fatto le ricerche del caso.
<http://www.schneier.com/blog/archives/2009/11/john_mueller_on_1.html>

Ricerca interessante: "Countering Kernel Rootkits with Lightweight Hook Protection" [Contrastare i rootkit kernel con una protezione leggera degli hook], di Zhi Wang, Xuxian Jiang, Weidong Cui e Peng Ning.
<http://www.schneier.com/blog/archives/2009/11/protecting_oss.html>

I ladri negli aeroporti preferiscono rubare bagagli di colore nero. Il perché è ovvio, a pensarci bene.
<http://www.schneier.com/blog/archives/2009/11/thieves_prefer.html>

Abbiamo notato molte dicerie in merito ad attacchi contro la rete elettrica, sia negli Stati Uniti che altrove, di gente che effettuerebbe hack mirati alla rete elettrica. Il Presidente Obama ne ha parlato nel suo discorso sulla sicurezza cibernetica: "In other countries cyberattacks have plunged entire cities into darkness" (In altri paesi gli attacchi cibernetici hanno sprofondato intere città nell'oscurità). Pare che la fonte di queste voci di corridoio sia stata il Brasile.
<http://www.schneier.com/blog/archives/2009/11/hacking_the_bra.html>

Condivisione delle informazioni fra FBI/CIA/NSA prima dell'11 settembre:
<http://www.schneier.com/blog/archives/2009/11/fbiciansa_infor.html>

Blowfish nella narrativa:
<http://www.schneier.com/blog/archives/2009/11/blowfish_in_fic.html>

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

Politiche di tolleranza zero

Alcune storie recenti hanno illustrato gli effetti assurdi delle politiche di tolleranza zero per le armi in un distretto scolastico del Delaware: un alunno di prima elementare espulso per aver portato un attrezzo da campeggio a scuola, un tredicenne espulso dopo che un altro studente gli ha fatto cadere in grembo un coltellino a serramanico, e uno studente di seconda media espulso per aver tagliato della carta con un coltello multiuso per un progetto scolastico. 'Dov'è finito il buon senso?' strillano gli editoriali.

Queste cosiddette politiche di tolleranza zero sono in realtà politiche di discrezionalità zero. Sono politiche che devono essere seguite alla lettera, non è permessa alcuna discrezionalità legata alla situazione. Le incontriamo ogni volta che passiamo attraverso i checkpoint di sicurezza negli aeroporti: niente liquidi, gel o aerosol. In alcuni luoghi di lavoro tali politiche sono in vigore per gli incidenti legati a molestie sessuali; in alcuni sport, una sostanza proibita, se trovata in un campione di urina, significa sospensione immediata, anche se quella sostanza è stata prescritta per un reale problema di salute. I giudici hanno discrezionalità zero quando si trovano di fronte alle cosiddette "mandatory sentencing laws", ossia leggi per condanne obbligatorie: dopo il terzo arresto per reati di droga si va in prigione, condanna obbligatoria per lo "statutory rape" (rapporti sessuali con un minore anche consenziente), e così via. Una catena di ristoranti nazionale non servirà hamburger 'al sangue', nemmeno se ci si offre di firmare una liberatoria. Ogni volta che sentite dire "Queste sono le regole, e non ci posso far nulla" -- e chi ve lo dice non vi sta mentendo per liberarsi di voi -- vi state scontrando con una politica di discrezionalità zero.

Queste politiche ci fanno infuriare perché sono cieche di fronte alle circostanze. Un editoriale dopo l'altro ha denunciato le sospensioni di bambini delle scuole elementari per offese che chiunque con un briciolo di buonsenso giudicherebbe accidentali e innocue. Internet è piena di studi che dimostrano come le regole della TSA sono prive di senso e a volte neanche migliorano la sicurezza. Ne ho trattate alcune. Quel che vogliamo è che chi si trova coinvolto in quelle situazioni eserciti discrezionalità.

Tuttavia sono stati proprio i problemi legati alla discrezionalità il motivo che ha fatto nascere quelle politiche obbligatorie. La discrezionalità è spesso applicata in maniera disorganica e incoerente. Il preside di una scuola potrebbe gestire il problema dei coltelli nelle aule in una maniera, e un altro preside in un'altra. La vostra condanna per droga può dipendere da quanto comprensivo il giudice si mostra nei vostri confronti, o se sta avendo una brutta giornata.

Ancora peggio, la discrezionalità può portare alla discriminazione. Le scuole avevano già stabilito dei divieti sulle armi prima delle politiche di tolleranza zero, ma insegnanti e presidi facevano rispettare le regole in maniera sproporzionata e a scapito degli studenti afroamericani. Anche le condanne penali variavano a seconda della razza. Il vantaggio delle norme e delle leggi a discrezionalità zero è che garantiscono che tutti siano trattati equamente.

Inoltre le norme a discrezionalità zero proteggono contro eventuali cause legali. Se le regole vengono applicate in maniera coerente e uniforme, nessun genitore, nessun viaggiatore, nessun imputato può sostenere di essere stato ingiustamente discriminato.

Pertanto la scelta è questa. O vogliamo che le regole siano rispettate equamente in tutti i casi, il che significa limitare la discrezionalità di coloro che rappresentano l'autorità in quel momento e in quel contesto, oppure vogliamo una risposta più sfumata a qualunque sia la situazione, il che significa dare maggiore discrezionalità a chi è coinvolto nella situazione.

Ovviamente c'è ben altro oltre a questo. Il problema delle norme a tolleranza zero sulle armi non è che sono rigide, ma che sono scritte male.

Che cosa costituisce un'arma? È un'arma qualsiasi coltello, non importa quanto piccolo? Le sanzioni devono essere le stesse sia per un alunno di prima elementare che per uno studente del liceo? È importante considerare le intenzioni? Quando un'aspirina usata per i crampi mestruali diventa "possesso di droga", è ovvio che ci si trova di fronte a una norma mal scritta.

La situazione è la medesima anche in ambito di sicurezza aeroportuale e di condanne penali. È più facile seguire norme semplici e ad ampio spettro (richiedono inoltre un minor sforzo intellettivo da parte di chi le fa rispettare), ma sono quasi sempre molto meno sfumate di quanto richieda la nostra complessa società. Purtroppo, più le regole si fanno complesse, più sono aperte all'interpretazione, e chi deve interpretare si ritrova con una maggiore discrezionalità.

La soluzione è combinare le due cose, le regole e la discrezionalità, con procedure che ne prevengano l'abuso. Che si forniscano delle regole, ma che non siano talmente rigide da precludere una pur minima interpretazione. Che si dia alle persone nella specifica situazione -- gli insegnanti, gli agenti di sicurezza all'aeroporto, gli agenti di polizia, i giudici -- la discrezionalità necessaria ad applicare le regole al contesto. Ma -- e questa è la parte più importante -- che si permetta alle persone di fare ricorso nel caso si sentano trattate ingiustamente. Ed effettuare un auditing costante degli esiti per garantire che non vi siano discriminazioni o favoritismi. A funzionare è la combinazione dei quattro elementi: regole più discrezionalità più ricorso più auditing.

Tutti i sistemi devono prevedere una qualche forma di risarcimento, che si tratti di un contesto pubblico come un'aula di tribunale, o chiuso e segreto come la TSA. Dare discrezionalità alle persone presenti in una situazione serve a creare un processo di appello più efficiente, dato che il primo livello di appello può essere gestito sul luogo.

A Zachary, il bambino del Delaware che è stato sospeso per aver utilizzato un utensile da campeggio (una combinazione di forchetta, cucchiaio e coltello) per mangiarsi il pranzo, la punizione è stata revocata all'unanimità dal comitato scolastico. È stata la decisione giusta. E tutti gli altri studenti i cui genitori non sono stati altrettanto decisi o capaci di sfruttare i media per trasformare la difficile situazione del proprio figlio in una storia nazionale? Il buonsenso nell'applicare le regole è importante, ma lo è altrettanto un accesso equo a tale buonsenso.

Questo articolo è originariamente apparso sul sito Web della Minnesota Public Radio.
<http://minnesota.publicradio.org/display/web/2009/11/03/schneier/>

<http://www.nytimes.com/2009/10/12/education/12discipline.html>
<http://www.philly.com/inquirer/opinion/20091016_Editorial__Zero_common_sense.html>
oppure <http://tinyurl.com/yls568f>
<http://www.lancastereaglegazette.com/article/20091020/OPINION04/910200313/Let-reason-be-driver-of-effective-zero-tolerance-policy>
oppure <http://tinyurl.com/yhcvxpu>
<http://www.dallasnews.com/sharedcontent/dws/dn/localnews/columnists/jragland/stories/DN-ragland_17met.ART.State.Edition1.4c22b1f.html>
oppure <http://tinyurl.com/yh7ehpn>
<http://www.htrnews.com/article/20091017/MAN06/910170416>
<http://www.baylor.edu/lariat/news.php?action=story&story=63347>

<http://www.sdnn.com/sandiego/2009-10-20/columns/marsha-sutton-zero-tolerance-equals-zero-brain-function>
oppure <http://tinyurl.com/ygfhysa>
<http://www.delmarvanow.com/article/20091020/DW02/910200338>

Un altro esempio:
Un ex-soldato che ha consegnato alla polizia un fucile abbandonato rischia almeno cinque anni di prigione per "aver fatto il proprio dovere".
<http://www.thisissurreytoday.co.uk/news/Ex-soldier-faces-jail-handing-gun/article-1509082-detail/article.html>
oppure <http://tinyurl.com/y9spuad>

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

La sicurezza in un'economia basata sulla reputazione

In passato il nostro rapporto con i computer era di natura tecnica. Ci importava sapere che processore avevano e quali software giravano su di essi. Conoscevamo bene le nostre reti e come funzionavano. Eravamo esperti, oppure dipendevamo da qualcun altro per le conoscenze tecniche. E la sicurezza faceva parte di quel bagaglio di conoscenze.

Tutto questo sta cambiando. Accediamo alla nostra posta elettronica dal Web, da qualsiasi computer o dai nostri smartphone. Usiamo Facebook, Google Docs, persino le reti dell'azienda in cui lavoriamo, a prescindere dall'hardware e dal tipo di rete. Oggi, specialmente per i più giovani, i dettagli tecnici non hanno più una grande importanza. L'informatica è un'infrastruttura, un bene di prima necessità. Riguarda sempre meno i prodotti e sempre più i servizi. Ormai ci aspettiamo che funzioni, come la rete telefonica, l'elettricità o la rete dei trasporti.

Le infrastrutture si possono estendere su uno spettro piuttosto ampio, da generiche ad altamente specializzate. L'elettricità e l'acqua sono generiche: chi ne sia il fornitore non ha molta importanza. I servizi di telefonia cellulare, di carta di credito, di fornitura di accesso Internet e le linee aeree sono per lo più infrastrutture generiche. Fra i servizi di infrastrutture più specializzate troviamo l'esercizio di ristoranti, parrucchieri e i siti di social networking. Servizi altamente specializzati comprendono la preparazione fiscale per attività commerciali complesse, consulenze di gestione, servizi legali e sanitari.

Le vendite di questi servizi sono spinte da due fattori: prezzo e fiducia. Più un servizio è generico, più sarà il prezzo l'elemento dominante. Più è specializzato, più sarà la fiducia a dominare. Il settore IT è una sorta di caso a parte, perché una gran parte di esso è gratuita. Pertanto, sia per i servizi IT specializzati ove il prezzo è meno importante, sia per i servizi IT generici (come Facebook) in cui non esiste un prezzo, l'elemento sempre più forte sarà la fiducia. Il settore IT sta diventando un'economia basata sulla reputazione, e ciò presenta implicazioni interessanti in materia di sicurezza.

Alcuni anni fa, le compagnie di carte di credito più importanti iniziarono a preoccuparsi per i ripetuti furti di numeri di carta di credito dai database dei rivenditori. Temevano che quei furti potessero minare la fiducia che il pubblico riponeva nella carta di credito

come sistema sicuro di pagamento su Internet. Sapevano che i rivenditori avrebbero protetto i database solo fino al punto in cui la minaccia costituiva un pericolo per i rivenditori stessi, non per l'industria intera. Quindi si riunirono e produssero uno standard di sicurezza chiamato PCI. Tale standard viene fatto rispettare dall'intera industria, un'industria che si è resa conto che la propria reputazione era più importante dei database dei rivenditori.

Un'economia basata sulla reputazione significa che i fornitori di infrastruttura si interessano maggiormente della sicurezza che non i propri clienti. L'ho capito dieci anni fa con la mia azienda. Offrivamo servizi di monitoraggio di rete a grandi imprese, e la sicurezza della nostra rete interna era molto più profonda di quella dei nostri clienti. I nostri clienti proteggevano le proprie reti -- dopotutto è per questo che ci ingaggiavano -- ma limitatamente al valore delle loro reti. Se avessimo compromesso i dati di un nostro cliente, avremmo perduto la fiducia di tutti i clienti.

Ho sentito la stessa storia a una conferenza ENISA lo scorso giugno, a Londra, quando un consulente IT raccontò che aveva iniziato a criptare il suo portatile anni prima rispetto ai suoi clienti. I suoi clienti potevano anche decidere che il rischio di perdere i propri dati non valesse la fatica di imparare a utilizzare la crittografia, ma lui sapeva che se avesse perso i dati di un cliente, avrebbe rischiato di perdere tutti i suoi clienti.

Più il settore IT diventa un'infrastruttura, un bene di prima necessità, più i fornitori di servizi tenderanno a migliorare la sicurezza a livelli superiori rispetto a quanto i loro clienti avrebbero fatto per se stessi.

Nel settore IT, i clienti arrivano a conoscere la reputazione di un'azienda da svariate fonti: articoli su riviste, recensioni di analisti, segnalazioni di colleghi, premi, certificazioni e via dicendo. Naturalmente questo funziona soltanto se i clienti ottengono informazioni precise. In un'economia basata sulla reputazione, le aziende sono spinte a nascondere i propri problemi di sicurezza.

Tutti abbiamo sperimentato un'economia basata sulla reputazione: i ristoranti. Alcuni ristoranti hanno un'ottima reputazione e sono frequentati costantemente da clienti abituali. Quando un ristorante si fa una cattiva reputazione, la gente smette di andarci e l'attività chiude. I ristoranti per turisti (la cui attrazione principale è l'ubicazione, e chi li frequenta spesso non sa nulla della loro reputazione) possono prosperare anche se non offrono un servizio eccellente. E a volte un ristorante riesce a mantenere la propria reputazione anche per molto tempo dopo che il suo cibo e il servizio hanno smesso di essere quelli di una volta, magari grazie a una segnalazione in una rivista, o perché è un ristorante che 'tutti sanno' essere il luogo ideale per occasioni speciali, e così via.

L'economia basata sulla reputazione è tutt'altro che perfetta.

Questo articolo è originariamente apparso sul Guardian.
<http://www.guardian.co.uk/technology/2009/nov/11/schneier-reputation-it-security>
oppure <http://tinyurl.com/yha3nbj>

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

Le news su Schneier

Interverrò all'Internet Governance Forum a Sharm el-Sheikh, Egitto, il 16 e 17 novembre.
<http://igf09.eg/home.html>

Interverrò al 2009 SecAU Security Congress a Perth il 2 e 3 dicembre.
<http://scissec.scis.ecu.edu.au/conferences2008/>

Interverrò a un evento dell'Open Rights Group a Londra il 4 dicembre.
<http://www.openrightsgroup.org/blog/2009/bruce-schneier-event>

Interverrò al primo IEEE Workshop on Information Forensics and Security a Londra l'8 dicembre.
<http://www.wifs09.org/>

Sarò allo UCL Centre for Security and Crime Science a Londra il 7 dicembre.
<http://www.cscs.ucl.ac.uk/>

Sarò allo Young Professionals in Foreign Policy a Londra il 7 dicembre.
<http://www.ypfp.org/content/event/London>

Interverrò alla Iberic Web Application Security Conference a Madrid il 10 dicembre.
10-11 dicembre 2009
<http://www.ibwas.com/>

Un articolo su di me in una rivista del Lussemburgo.
<http://www.paperjam.lu/archives/2009/11/2310_Technologie_Security/index.html>
oppure <http://tinyurl.com/y95mcpq>

Una mia intervista è stata pubblicata su CNet.com:
<http://news.cnet.com/8301-27080_3-10381460-245.html?tag=newsLeadStoriesArea.1>
oppure <http://tinyurl.com/yf5otcu>

Video di una mia intervista, condotta alla Information Security Decisions conference a Chicago in ottobre.
<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1372839,00.html>
oppure <http://tinyurl.com/yk4othd>

Un mese fa, ThatsMyFace.com mi ha consultato per la realizzazione di una 'action figure' di Bruce Schneier. Costa 100 dollari. Mi piacerebbe poter dire cose come "metà del ricavato andrà all'EPIC e alla EFF", ma non è così. Quello è il prezzo del prodotto su ordinazione. Non riceverò nemmeno una royalty. L'azienda sta cercando di abbassare il prezzo, e ha detto che metterà sul sito Web una foto della figurina vera e propria. Ho detto loro che a 100 dollari nessuno la comprerà, ma a 40 dollari potrebbe essere un buffo omaggio per una persona che lavora nell'IT. Per cui scrivete email all'azienda se siete interessati, e se l'interesse è sufficiente, accetteranno ordinazioni per grandi quantità.
<http://www.thatsmyface.com/f/bruce_schneier>

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

Il braccio di ferro del discorso commerciale

Qualche anno fa, un'azienda iniziò a vendere un liquido con codici identificativi sospesi al suo interno. L'idea era quella di spalmarlo sui nostri oggetti come prova di possesso. Commentai dicendo che avrei spalmato il liquido sugli oggetti altrui e poi avrei chiamato la polizia.

Mi sono ricordato questo esempio di recente, quando un gruppo di scienziati israeliani ha dimostrato che è possibile fabbricare campioni di DNA da usare come prova. Quindi adesso, invece di lasciare il vostro DNA sulla scena del delitto, potete lasciare un campione di DNA fasullo. E non è nemmeno necessario fabbricarlo. Nel romanzo "Halting State" di Charlie Stross, i criminali contaminano una scena del delitto spargendo dappertutto i contenuti del sacco di un aspirapolvere, che contengono appunto il DNA di decine (se non di centinaia) di persone.

Questo genere di cose va avanti da sempre. È un braccio di ferro, e quando cambia la tecnologia, cambia anche l'equilibro fra aggressore e difensore. Ma quando i rilevamenti sono compiuti da sistemi automatizzati, i risultati sono diversi. Il software di riconoscimento facciale può essere ingannato dalla chirurgia plastica, o a volte basta anche una fotografia. E quando diventa difficile ingannare questi sistemi, i criminali li ingannano a un diverso livello. Il rilevamento computerizzato offre al difensore economie di scala, ma l'aggressore può servirsi di quelle medesime economie di scala per sconfiggere il sistema di rilevamento.

Google, per esempio, possiede sistemi antifrode che rilevano e bloccano quegli inserzionisti che cercano di gonfiare i propri guadagni facendo clic in continuazione sui propri annunci AdSense. Allora certi inserzionisti hanno creato dei bot che facevano clic ripetutamente sugli annunci AdSense dei loro concorrenti, cercando di convincere Google a espellerli dal sistema.

Analogamente, quando Google ha iniziato a penalizzare la visibilità di un sito nei risultati del motore di ricerca perché quel sito aveva un 'brutto vicinato' (backlink forniti da link farm, siti per adulti o di gioco d'azzardo, o spam per i blog), sono cominciati i sabotaggi: certe imprese hanno costruito delle link farm e hanno lasciato commenti spam nei blog contenenti link ai siti dei loro concorrenti.

La stessa cosa sta accadendo con Yahoo Answers. All'inizio le aziende lasciavano delle risposte ad hoc per spingere i propri prodotti, ma poi Yahoo ha iniziato a vigilare. Allora le aziende hanno realizzato dei bot in modo da far apparire i loro concorrenti come abusivi. Esistono dei bot in Facebook che fanno la stessa cosa.

Il mese scorso, Google ha introdotto Sidewiki, una funzione del browser che permette di leggere e pubblicare commenti praticamente per ogni sito. Privati e industrie sono già preoccupati degli effetti che potrebbero causare alla loro attività commerciale questi commenti senza freni, e come possono controllarli. Sono certo che Google dispone di sistemi sofisticati pronti a rilevare certi interessi commerciali che cercano di

approfittarsi del sistema, ma Google è pronta ad affrontare interessi commerciali che cercano di danneggiare i concorrenti? E vogliamo proprio dare a un'azienda il potere di decidere quali commenti dovrebbero essere promossi e quali cancellati?

Ogni volta che si costruisce un sistema che si basa sul rilevamento e l'identificazione, si invitano i criminali a sovvertire tale sistema in modo che rilevi e identifichi qualcun altro. A volte ciò è difficile e complesso: lasciare le impronte digitali di un'altra persona in una scena del reato è difficile, così come è difficile usare la maschera con il volto di qualcun altro per ingannare una guardia davanti a una telecamera di sorveglianza. A volte è semplice. Ma quando si tratta di sistemi automatici, spesso è molto semplice. E qui non stiamo parlando di criminali inveterati che cercano di incastrarsi a vicenda, ma di interessi commerciali convenzionali.

Con sistemi che sorvegliano i commenti e i link su Internet, nei messaggi commerciali c'è sempre di mezzo il denaro, per cui si può stare certi che qualcuno se ne approfitterà. È questo il braccio di ferro. Viene costruito un sistema di rilevamento, e i criminali cercheranno di incastrare qualcun altro. Viene costruito un sistema per rilevare la frode, e i criminali cercheranno di incastrare qualcun altro incastrando qualcun altro ancora. Viene costruito un sistema per rilevare la frode della frode e... beh, si può veramente andare avanti all'infinito. Il discorso commerciale non sparirà da Internet: possiamo solo sperare che i sistemi sociali che utilizziamo non saranno contaminati al punto da non essere più di alcuna utilità.

Questo articolo è originariamente apparso sul Guardian.
<http://www.guardian.co.uk/technology/2009/oct/15/bruce-schneier-internet-security>
oppure <http://tinyurl.com/yfbsb42>

Identificatore liquido "Smart Water":
<http://www.schneier.com/blog/archives/2005/02/smart_water.html>

Falsificare campioni di DNA:
<http://www.nytimes.com/2009/08/18/science/18dna.html>

Ingannare il software di riconoscimento facciale:
<http://staging.spectrum.ieee.org/computing/embedded-systems/computerized-facerecognition-technology-foiled>
oppure <http://tinyurl.com/yz9x4pf>
<http://www.theregister.co.uk/2009/02/19/facial_recognition_fail/>

Google AdSense:
<http://www.wmtips.com/adsense/what-you-need-know-about-adsense.htm>

Sidewiki:
<http://www.google.com/sidewiki/intl/en/index.html:>
<http://www.pcworld.com/article/172490/google_sidewiki_a_first_look.html>
oppure <http://tinyurl.com/lgpxp8>

Preoccupazioni in merito a Sidewiki:
<http://impactiviti.wordpress.com/2009/09/29/googles-sidewiki-game-changer-for-pharma-social-media/>

oppure <http://tinyurl.com/yl4ul3g>
<http://www.4hoteliers.com/4hots_fshw.php?mwi=4448>
<http://talkbiz.com/blog/google-steals-the-web/>

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

Il Canile: ADE 651

Un bastone da rabdomante per trovare esplosivi in Iraq:
<http://www.schneier.com/blog/archives/2009/11/the_doghouse_ad.html>

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

Attacchi di tipo 'Evil Maid' contro dischi criptati

All'inizio di questo mese, Joanna Rutkowska ha implementato l'attacco di tipo 'Evil Maid' [lett. 'cameriera malefica'] contro TrueCrypt. Lo stesso genere di attacco dovrebbe funzionare contro qualunque crittografia completa di interi dischi, compresi PGP Disk e BitLocker. In sostanza, l'attacco funziona così:

Passo 1: L'aggressore ottiene l'accesso al vostro computer spento e lo avvia da un volume esterno. L'aggressore scrive un bootloader hackerato nel vostro sistema, poi lo spegne nuovamente.

Passo 2: Avviate il vostro computer, che eseguirà il boot attraverso il bootloader hackerato dell'aggressore, e inserite la chiave crittografica. Una volta sbloccato il disco, il bootloader modificato entra in azione e potrebbe fare di tutto, dall'installare malware per catturare la chiave e inviarla da qualche parte via Internet, o archiviarla in qualche zona del disco per essere estratta in un secondo momento, qualunque cosa.

È facile capire perché viene soprannominato attacco della 'cameriera malefica'. Uno scenario plausibile è che si lascia il proprio computer criptato nella stanza d'albergo quando si esce a cena, e la cameriera si intrufola nella stanza e installa il bootloader modificato. La stessa cameriera potrebbe tornare la sera successiva ed eliminare ogni traccia delle sue azioni.

Questo attacco sfrutta la stessa vulnerabilità dell'attacco "Cold Boot" dell'anno scorso, e dell'attacco "Stoned Boot" di quest'anno, e non esiste una difesa vera e propria contro questo genere di cose. Una volta lasciato il controllo fisico del proprio computer, tutto è possibile. Dal CRN: "Simili attacchi hardware erano fra i motivi principali per cui a Mark Bergman, CTO di Symantec, è stato recentemente consigliato da 'agenzie di tre lettere del Governo degli Stati Uniti' di utilizzare sia un computer portatile che un secondo dispositivo mobile durante il suo viaggio in Cina".

PGP riassume il problema nel proprio blog. "Nessun prodotto di sicurezza oggi sul mercato può proteggervi se il computer in questione è stato compromesso da malware

dotato di permessi amministrativi di livello root. Detto questo, esistono molte difese basate sul buonsenso contro 'Cold Boot', 'Stoned Boot', 'Evil Maid', e molti altri attacchi ancora senza nome e non ancora pubblicizzati".

Le difese sono essenzialmente autenticazioni a due fattori: un token che non lasciate nella stanza d'albergo e che quindi non può essere utilizzato dalla cameriera. La cameriera potrebbe sempre compromettere la macchina, ma occorre più lavoro che non semplicemente conservare la password per usi futuri. Mettere i dati in una chiavetta USB e portarla con sé non serve: quando tornate al computer inserirete la chiavetta in una macchina compromessa.

La vera difesa è il trusted boot, il boot fidato, una funzione che dovrebbe permettere il Trusted Computing. E l'unico modo per averlo è dalla crittografia per hard disk fornita da Microsoft BitLocker, se il vostro computer è dotato di un modulo TPM versione 1.2 o successiva.

Nel frattempo chi cripta i propri dischi rigidi o partizioni di dischi rigidi, deve rendersi conto che la criptatura offre meno protezioni di quanto sia portato a credere. È una protezione efficace contro chi confisca o ruba il computer e poi cerca di accedere ai dati. Non protegge contro un aggressore che ha accesso al computer in un intervallo di tempo durante il quale anche il legittimo proprietario lo sta utilizzando.

Attacchi di tipo 'Evil Maid':
<http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html>
oppure <http://tinyurl.com/yzbbgc3>

Attacchi 'Cold Boot' e 'Stoned Boot':
<http://citp.princeton.edu/memory/>
<http://www.stoned-vienna.com/>
<http://blogs.zdnet.com/security/?p=4662&tag=nl.e019>
<http://www.crn.com.au/News/155836,safety-first-for-it-executives-in-china.aspx>
oppure <http://tinyurl.com/p2wqxq>

Il commento di PGP:
<http://blog.pgp.com/index.php/2009/10/evil-maid-attack/>

Trusted Computing:
<http://www.schneier.com/blog/archives/2005/08/trusted_computi.html>

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

Sono ancora utili gli antivirus?

Questo articolo è originariamente apparso su "Information Security Magazine" come seconda parte di un 'botta e risposta' con Marcus Ranum. Potete leggere la parte di Marcus qui:
<http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1373562,00.html>
oppure <http://tinyurl.com/yz2rtbs>

La sicurezza non è mai una questione di bianco o nero. Se una persona chiede "Per avere la sicurezza migliore, devo fare A o B?", quasi invariabilmente la risposta sarà entrambi. Ma la sicurezza è sempre un compromesso. Spesso è impossibile fare sia A che B (non c'è tempo di fare entrambe le cose, è troppo costoso farlo, ecc.) e occorre scegliere. In tal caso si guarda ad A e B e si effettua la scelta migliore. Ma quasi sempre è più sicuro fare entrambe le cose.

Sì, i software antivirus sono diventati meno efficaci di fronte alla maggior frequenza di nuovi virus e alla maggior velocità con cui i vecchi virus mutano. Sì, le aziende che producono antivirus cercano costantemente di stare al passo con la situazione, cercando di creare firme per i nuovi virus. Sì, gli antivirus basati sulle firme non serviranno a proteggersi in presenza di un virus nuovo, prima che la sua firma sia aggiunta al programma di rilevamento. Un antivirus non è affatto una panacea.

D'altra parte, un programma antivirus con firme aggiornate vi proteggerà da molte altre minacce. Servirà a proteggersi da virus, spyware, Trojan, da ogni genere di malware. Si eseguirà in background, automaticamente, e non si noterà alcun degrado delle prestazioni del computer. E -- e qui viene il bello -- può essere gratuito. AVG non costa nulla. Per me questo è un compromesso facile, e lo è certamente per l'utente medio che fa clic su allegati che non dovrebbe toccare, che scarica cose che non dovrebbe scaricare, e che non capisce come funziona esattamente il Firewall di Windows.

Di certo la sicurezza sarebbe migliore se le persone si servissero di programmi che generano white list (liste bianche) come Bit9 Parity e Savant Protection -- e io consiglio personalmente Anti-Malware di Malwarebytes -- ma molti utenti avranno difficoltà con questo genere di software. L'utente medio probabilmente si libererà degli avvisi a video come "State cercando di eseguire un programma non presente nella white list" senza nemmeno leggerli; oppure, ancor peggio, si chiederà perché il suo computer non funziona quando cerca di far girare un nuovo software. Il reparto IT medio di un'azienda non ha un'idea precisa del software che sta girando su tutti i computer aziendali, e non vuole avere il carico amministrativo di gestire ogni richiesta di cambiamento. E neanche le white list sono una panacea: per esempio non difendono contro malware che si attacca a file dati (pensiamo ai virus delle macro di Word).

Una delle ultimissime tendenze nel settore IT è la cosiddetta 'consumerizzazione', e se non ne sapete già qualcosa, presto ne sentirete parlare spesso. È l'idea per cui le nuove tecnologie, i bei gadget tecnologici che vogliono tutti, verranno messi a disposizione prima per il mercato consumer, e poi per quello business. Per il settore business questo significa che le persone (dipendenti, clienti, partner) accederanno alle reti aziendali da qualunque luogo si trovino, con qualsiasi hardware e software avranno a disposizione. Potrà essere il computer che hanno ricevuto una volta assunti, o il loro computer di casa, lo stesso che usano i loro figli; o magari il loro cellulare o PDA, o un computer nell'area commerciale di un albergo. La vostra impresa non avrà modo di sapere quali strumenti staranno impiegando e, cosa ancor più importante, non avrete alcun controllo della situazione.

In questo tipo di ambiente, i computer si collegheranno fra loro senza molta fiducia reciproca. Computer non fidati si collegheranno a reti non fidate. Computer fidati si

collegheranno a reti non fidate. L'intero concetto di 'informatica sicura' prenderà tutt'altra sfumatura di significato: ognun per sé. Una rete aziendale avrà bisogno di un prodotto antivirus semplice, ottuso e basato sulle firme, da sistemare all'ingresso della rete. E il singolo utente avrà bisogno di un simile prodotto per proteggere il proprio computer.

Morale: il software antivirus non è necessario né sufficiente per la sicurezza, ma rimane una buona idea. Non si tratta di una panacea che vi protegge magicamente, né si tratta di uno strumento obsoleto rispetto alle attuali minacce. È una contromisura fra le più economiche, semplici ed efficaci. Non ho ancora abbandonato il mio programma antivirus, né ho intenzione di farlo nel breve termine.

Problemi con i programmi antivirus:
<http://www.csoonline.com/article/495827/Experts_Only_Time_to_Ditch_the_Antivirus_>
oppure <http://tinyurl.com/nqo68f>
<http://www.computerworld.com/s/article/print/9077338/The_future_of_antivirus>
oppure <http://tinyurl.com/yfrv86s>
<http://www.pcworld.com/article/130455/is_desktop_antivirus_dead.html>
<http://www.businessweek.com/technology/content/jan2007/tc20070122_300717.htm>
oppure <http://tinyurl.com/ycdkmd3>

AVG:
<http://free.avg.com/us-en/homepage>

Consumerizzazione:
<http://arstechnica.com/business/news/2008/07/analysis-it-consumerization-and-the-future-of-work.ars>
oppure <http://tinyurl.com/yd6kxgs>

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

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>

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

Dal 1998 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, Business Unit di Security Reply.
<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) 2009 - Bruce Schneier.