

CRYPTO-GRAM
15 maggio 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 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:

- Il vincitore della Quarta edizione del concorso "Minaccia da Trama Cinematografica"
- Recensione del libro: The Science of Fear
- Un'aspettativa di privacy online
- News
- Contaminazione malevola delle scorte alimentari
- Pratiche sleali e ingannevoli di commercio dei dati
- Le news su Schneier
- Analfabetismo matematico
- Conficker
- Commenti dei lettori

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

Il vincitore della Quarta edizione del concorso "Minaccia da Trama Cinematografica"

Per questa edizione del concorso, l'obiettivo era "trovare un evento realmente accaduto da qualche parte nel mondo industrializzato (pescare fra gli eventi del Terzo Mondo è troppo facile) e fornire una teoria complottista che dimostri come i veri responsabili dietro quell'evento siano stati i terroristi".

Ho pensato che fosse sufficientemente chiaro, ma in tutta onestà i contributi non mi hanno entusiasmato più di tanto. Nulla mi ha sorpreso per la sua ingegnosità. Ci sono stati contributi che mettevano paura, e altri molto plausibili, ma è stato quasi impossibile trovarne uno che fosse agghiacciante e plausibile al tempo stesso. E mi ha sorpreso la gran quantità di persone che non si

sono nemmeno preoccupate di leggere le regole e hanno semplicemente inviato generiche minacce da trama cinematografica.

Ma dopo aver passato in rassegna i vari contributi, ho scelto un vincitore. È HJohn, per il suo collegamento sequestro-ricatto-terrorismo: “Malgrado le recenti sparatorie in chiese, case di riposo e durante escursioni di famiglia siano apparse come episodi distinti e slegati fra loro, è stato scoperto un collegamento terrificante. Tutti gli esecutori del reato avevano figli sequestrati da terroristi, e avevano ricevuto un video in cui dei terroristi incappucciati minacciavano di decapitare i bambini se i loro genitori non avessero accettato la missione suicida. Il livello di minaccia terroristica è stato aumentato a codice rosso, dato che il profiling, i legami noti e la fedina penale adesso sono del tutto inutili per stabilire chi sarà il prossimo cechino terrorista o dirottatore aereo. Chiunque ami i propri figli potrebbe essere un potenziale terrorista”.

Piuttosto plausibile, e di certo terrificante. Congratulazioni, HJohn.

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:
<http://www.schneier.com/blog/archives/2009/05/fourth_movie-pl.html>

** **

Recensione del libro: The Science of Fear

Il libro “The Science of Fear” [La Scienza della Paura] di Daniel Gardner è stato pubblicato nel luglio dello scorso anno, ma sono riuscito a leggerlo solo ora. Ho fatto male ad aspettare. Si tratta di una brillante osservazione di come gli esseri umani si confrontano con la paura: proprio il genere di cose che ho letto e di cui ho parlato negli ultimi due anni. È il libro che avrei voluto scrivere, ed è una lettura eccezionale.

Gardner tratta di come il nostro cervello processa la paura e il rischio, come valuta la possibilità e la probabilità, e come prende decisioni in situazioni di incertezza. Il libro parla di tutti quegli studi psicologici (psicologia cognitiva, psicologia evolutiva, economia comportamentale, filosofia sperimentale) che chiariscono come pensiamo e agiamo in merito alla paura. Il libro parla inoltre di come la paura venga utilizzata per influenzare le persone, da parte dei venditori, dei politici, dei mass media. E infine il libro parla di vari ambiti in cui la paura gioca un certo ruolo: salute, crimine, terrorismo.

Sono stati pubblicati molti libri di recente che applicano questi nuovi paradigmi della psicologia umana ai contesti più vari (casualità, traffico, razionalità, arte, religione, e così via), ma dopo averne letti alcuni si comincia a notare il continuo ripetersi della stessa dozzina di esperimenti psicologici. Anch’io l’ho fatto, quando ho scritto il mio intervento sulla psicologia della sicurezza. Ma il libro di Gardner è diverso: l’autore si spinge oltre, spiega più a fondo, dimostra la sua tesi attraverso gli esperimenti più oscuri che molti altri autori non si sono neanche presi la briga di cercare. Il suo stile di scrittura è al tempo stesso facile da seguire e informativo, un’ottima mescolanza di dati e aneddoti. Il fluire del libro ha un senso, e l’analisi di Gardner centra il punto.

L’unico problema che ho avuto con il volume è che Gardner non fa uso dei termini standard riferiti ai vari procedimenti euristici del cervello di cui tratta. È vero, i termini che lui utilizza sono più intuitivi ed evocativi, ma sono scorretti. Se avete già letto altri saggi sull’argomento, la cosa diventa seccante perché occorre tradurre mentalmente quelle parole nella terminologia tradizionale. E se non avete mai letto altri libri di questo settore, allora è un problema perché vi troverete inutilmente confusi quando leggerete altri volumi o articoli che trattano gli stessi argomenti.

introdursi nell'Internet Provider. Dieci anni fa, la messaggeria vocale veniva effettuata mediante una segreteria telefonica nel vostro ufficio; oggi è tutto su un computer di proprietà di una compagnia telefonica. I conti correnti si trovano su siti Web remoti protetti soltanto da password; la nostra storia creditizia viene raccolta, conservata e rivenduta da aziende che nemmeno sapevamo della loro esistenza.

E si crea una quantità sempre maggiore di dati. Gli elenchi dei libri che acquistiamo, così come di quelli che esaminiamo, vengono archiviati nei computer dei venditori di libri online. La tessera di fidelizzazione rivela al supermercato i nostri cibi preferiti. Quelle che una volta erano transazioni in contanti adesso sono transazioni in carta di credito. Una volta si pagava il pedaggio autostradale con una moneta inserita nell'apposita macchina, in totale anonimato; oggi è una registrazione EZ Pass che comunica su quale autostrada stavate transitando e a che ora. Quella che una volta soleva essere una chiacchierata faccia a faccia adesso diventa un'email, una chat, o uno scambio di SMS -- o persino una conversazione all'interno di Facebook.

Vi ricordate di quando Facebook ha recentemente cambiato i termini di servizio per avere un controllo ancora maggiore dei vostri dati? Possono farlo quando vogliono, sapete.

Non abbiamo scelta se non quella di affidare la nostra sicurezza e la nostra privacy a queste aziende, anche se sono pochissimo incentivate a proteggerci. Né ChoicePoint, Lexis Nexis, Bank of America, né T-Mobile sostengono i costi di eventuali violazioni della privacy o di qualsiasi genere di furto di identità che possa derivarne.

Tale perdita di controllo sui nostri dati ha anche altri effetti. Le protezioni contro gli abusi della polizia sono state drasticamente attenuate. I tribunali hanno stabilito che la polizia può accedere ai nostri dati senza mandato, a condizione che siano conservati presso terzi. Se la polizia vuole leggere le email sul nostro computer, deve richiedere un mandato; ma non ha bisogno di un mandato per leggere le email conservate sui nastri di backup del nostro Internet Provider.

Non si tratta di un problema di ordine tecnologico, ma di natura legale. I tribunali devono riconoscere che nell'era dell'informazione la privacy virtuale e la privacy fisica non hanno gli stessi contorni. Dovremmo poter controllare i nostri dati, a prescindere da dove siano conservati. Dovremmo poter prendere delle decisioni riguardanti la privacy e la sicurezza di quelle informazioni, e poter fare ricorso per via legale nel caso le aziende che conservano quei dati non si attengano alle nostre decisioni. E visto che la Corte Suprema ha infine stabilito che intercettare una comunicazione telefonica equivale a una perquisizione sotto il Quarto Emendamento, richiedendo quindi l'obbligo di un mandato (anche se l'intercettazione era stata effettuata negli uffici della compagnia telefonica e non nell'abitazione o nell'ufficio della persona presa di mira), analogamente la Corte Suprema deve riconoscere che leggere email private negli uffici di un Internet Provider è la stessa identica cosa.

Questo articolo è stato originariamente pubblicato sul sito SearchSecurity.com, come seconda parte di un 'botta e risposta' con Marcus Ranum.

<http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1354832,00.html>
oppure <<http://tinyurl.com/pnv8vq>>

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

News

Nuove frontiere per la biometrica. Le orecchie:

<<http://www.newscientist.com/article/mg20227035.200-our-ears-may-have-builtin-passwords.html>>

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

I movimenti oscillatori del braccio:

<http://techon.nikkeibp.co.jp/english/NEWS_EN/20090414/168716/>
Suppongo che la biometrica sia la scienza più 'in' del momento.

Sabotare un sondaggio del Time Magazine poll. Un metodo non particolarmente raffinato, ma ugualmente brillante:

<<http://musicmachinery.com/2009/04/15/inside-the-precision-hack/>>
<http://www.theregister.co.uk/2009/04/17/time_top_100_hack/>
<<http://musicmachinery.com/2009/04/27/moot-wins-time-inc-loses/>>

Campagna di reclutamento del Dipartimento per la Sicurezza Nazionale:

<http://news.yahoo.com/s/ap/20090418/ap_on_go_pr_wh/us_cyber_security>

Un aneddoto divertente sul tema 'guerra alla fotografia':

<<http://sierracharlie.wordpress.com/2009/04/10/terror/>>

Stavo per scrivere un commento sul discorso introduttivo che il Direttore Generale della NSA Alexander ha tenuto alla RSA Conference, ma non ha detto praticamente nulla di concreto.

<http://www.schneier.com/blog/archives/2009/04/nsa_at_rsa.html>

Semplice trucco di sostituzione di persona nei ristoranti:

<http://www.schneier.com/blog/archives/2009/04/low-tech_impers.html>

Criptare la propria chiavetta USB è buona cosa. Annotarsi la chiave crittografica è buona cosa. Scriverla su un pezzo di carta e attaccarlo alla chiavetta USB decisamente no.

<<http://news.bbc.co.uk/1/hi/england/lancashire/8003757.stm>>

Hackerare i satelliti militari statunitensi è una pratica più diffusa di quanto si creda:

<<http://www.wired.com/politics/security/news/2009/04/fleetcom>>

Informazioni false su Twitter: il medium stesso rende difficile autenticarle.

<http://www.schneier.com/blog/archives/2009/04/fake_facts_on_t.html>

Ricordate quella serie di arresti antiterrorismo condotti dal governo britannico, dopo che un documento segreto era stato fotografato accidentalmente? Nessuno è stato accusato:

<http://news.bbc.co.uk/2/hi/uk_news/8011955.stm>
<http://www.schneier.com/blog/archives/2009/04/how_not_to_carr.html>

Telefoni cellulari e situazioni con ostaggi:

<http://www.schneier.com/blog/archives/2009/04/cell_phones_and.html>

Questo video, apparentemente non ironico, mette in guardia sul fatto che dei malintenzionati potrebbero impersonare gli incaricati del censo per cercare di derubarvi. Ma mentre non dovrete fidarvi del documento d'identità di un estraneo, dovrete confidare nel fatto che quello stesso estraneo vi fornisca un recapito telefonico presso cui verificare quel documento. La cosa, ovviamente, non ha senso.

<<http://www.keyt.com/news/local/43392637.html>>

Prevenire la sostituzione di persona è difficile.

<<http://www.schneier.com/blog/archives/2009/01/impersonation.html>>

'No-fly' vuol dire anche 'no-flyover', cioè non sorvolare: a un aereo proveniente da Parigi e diretto in Messico non viene permesso sorvolare gli Stati Uniti.

<http://www.schneier.com/blog/archives/2009/04/no-fly_also_mea.html>

Lezioni apprese dalla sparatoria alla scuola di Columbine: a fare la vera differenza non è l'attrezzatura ad alta tecnologia, ma il personale addestrato e vigile:

<http://www.schneier.com/blog/archives/2009/04/lessons_from_th_2.html>

L'Irlanda abbandona il voto elettronico e ritorna alle schede cartacee. Un paese intelligente.

<http://www.schneier.com/blog/archives/2009/04/ireland_does_aw.html>

Una triste storia di impronte digitali e dati biometrici. Divertente e interessante:

<<http://thedailywtf.com/Articles/Cracking-your-Fingers.aspx>>

Interessante articolo del New York Times sul prepararsi a una guerra cibernetica:

<<http://www.nytimes.com/2009/04/28/us/28cyber.html>>

E un altro articolo del New York Times sulla guerra cibernetica, pubblicato due giorni dopo:

<http://www.schneier.com/blog/archives/2009/05/yet_another_new.html>

L'ultimo paragrafo dell'articolo mi ha particolarmente turbato: "L'introduzione della possibilità di una risposta nucleare a un attacco cibernetico catastrofico dovrebbe servire allo stesso scopo". La guerra nucleare non è una risposta appropriata a un attacco cibernetico.

Un professore di legge effettua ricerche in Google sul Giudice della Corte Suprema Scalia, giusto per vedere quante informazioni può raccogliere. La cosa non piace a Scalia:

<http://www.abajournal.com/weekly/fordham_law_class_collects_scalia_info_justice_is_steamed>

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

Considerazioni di sicurezza nell'evoluzione del pene umano: un affascinante estratto di biologia evolutiva.

<<http://www.scientificamerican.com/article.cfm?id=secrets-of-the-phallus>>

oppure <<http://tinyurl.com/dy8vxz>>

L'aviazione statunitense utilizza una versione sicura di MS Windows:

<http://www.schneier.com/blog/archives/2009/05/secure_version.html>

I ciarlatani nell'industria delle macchine della verità:

<http://www.schneier.com/blog/archives/2009/05/lie_detector_ch.html>

Informazioni mediche nello stato della Virginia prese in ostaggio con richiesta di riscatto:

<http://www.schneier.com/blog/archives/2009/05/virginia_data_r.html>

L'MI6 e un memory stick andato perduto:

<http://www.schneier.com/blog/archives/2009/05/mi6_and_a_lost.html>

Marc Rotenberg sulla sicurezza e la privacy:

<http://www.huffingtonpost.com/marc-rotenberg/privacy-vs-security-pr_b_71806.html>

oppure <<http://tinyurl.com/2hozm8>>

Dei ricercatori dirottano un botnet:

<http://www.schneier.com/blog/archives/2009/05/researchers_hij.html>

Il trojan Zeus prevede un'opzione di autodistruzione:

<http://voices.washingtonpost.com/securityfix/2009/05/zeustracker_and_the_nuclear_op.html>

oppure <<http://tinyurl.com/odjwx8>>

Brutto segnale. Lo vedo come un indizio che le guerre dei botnet stanno diventando sempre più serie, e che i creatori di botnet preferirebbero distruggere le proprie reti piuttosto che vederle finire nelle mani del 'nemico'.

Utilizzare telecamere di sorveglianza per rilevare la disonestà dei cassieri.

<http://www.schneier.com/blog/archives/2009/05/using_surveilla.html>

Problemi software di un rilevatore di tasso alcolico.

<http://www.schneier.com/blog/archives/2009/05/software_proble.html>

Una corte distrettuale statunitense ha stabilito che la polizia non ha bisogno di un mandato per posizionare un dispositivo di tracciamento GPS sull'auto di una persona:

<http://www.schneier.com/blog/archives/2009/05/no_warrant_requ.html>

** **

Contaminazione malevola delle scorte alimentari

Terroristi che attaccano le nostre scorte alimentari: uno scenario da incubo che è riemerso durante la recente epidemia di influenza suina. Anche se a tutta prima può sembrare un facile attacco, è importante comprendere perché non sia ancora accaduto. G.R. Dalziel, della Nanyang Technological University di Singapore ha scritto un rapporto che registra tutti i casi confermati di contaminazione alimentare malevola nel mondo dal 1950 in poi: 365 casi in tutto, più altri 126 casi non confermati. Le sue scoperte dimostrano la realtà degli attacchi alimentari di stampo terroristico.

Risulta che il 72% degli avvelenamenti di cibo sono avvenuti alla fine della catena alimentare: in casa, e tipicamente per mano di un amico, parente, vicino o collega che ha tentato di uccidere o ferire una certa persona. Un esempio caratteristico è Heather Mook di New York, che nel 2007 cercò di uccidere suo marito mettendo veleno per topi nei suoi spaghetti.

Moltissimi di questi casi hanno avuto come risultato meno di cinque morti -- Mook riuscì soltanto a ferire suo marito in quell'incidente -- anche se vi è stato un 16% di casi con cinque o più morti. Dei 19 casi che hanno registrato 10 o più vittime, quattro erano serial killer, e in un arco di parecchi anni di attività.

Un altro 23% dei casi è avvenuto nel contesto della vendita al dettaglio o dei servizi. Esempio tipico è un incidente del 1998 in Giappone, in cui fu aggiunto arsenico a del curry venduto a un festival estivo, che causò la morte di quattro persone e il ricovero in ospedale di altre 63. Solo l'11% di questi incidenti ha prodotto 100 o più morti, mentre nel 44% dei casi non vi furono decessi.

Gli incidenti di vera e propria contaminazione delle scorte alimentari sono pochissimi. Degli ignoti hanno deliberatamente contaminato una riserva d'acqua sette volte, provocando tre morti. Esiste solo un esempio di contaminazione volontaria di una coltura prima del raccolto: in Australia nel 2006, e le messe vennero ritirate prima di poter essere vendute. E nei tre casi in cui gli alimenti sono stati contaminati durante il confezionamento e la distribuzione (compreso un caso del 2005 nel Regno Unito in cui aghi e pezzi di vetro vennero mischiati all'impasto del pane) nessuno è morto o rimasto ferito.

Questo non è bioterrorismo. L'esempio più vicino al bioterrorismo è un fatto accaduto negli Stati Uniti nel 1984, in cui membri di un gruppo religioso noto con il nome di Rajneeshees contaminarono diversi ristoranti e tavole fredde con salmonella enterica typhimurium, facendo ammalare 751 persone, facendone ricoverare altre 45, ma nessuno fu ucciso. Infatti nessuno seppe della natura malevola di questo episodio finché, dopo un anno, uno dei responsabili ammise la colpa.

In quasi tutti gli incidenti alimentari sono stati utilizzati comuni veleni come il cianuro, detergenti per gli scarichi, mercurio, diserbante. Sono occorsi nove incidenti con agenti biologici fra cui salmonella, ricina e materia fecale, e otto casi di materiale radioattivo. L'avvelenamento dell'ex agente del KGB Alexander Litvinenko a Londra nel 2006, in cui venne aggiunto del polonio-210 al suo tè, è un esempio di quest'ultima categoria.

E quell'assassinio illustra precisamente il vero rischio delle contaminazioni malevole degli alimenti. Quel che viene trattato nei manuali di addestramento dei terroristi, e quel che preoccupa la CIA, è l'utilizzo di cibo contaminato in uccisioni mirate. Le quantità necessarie per compiere avvelenamenti di massa sono troppo grandi, la realtà delle scorte alimentari troppo vasta e variegata e i dettagli di un qualsiasi complotto troppo complicati e imprevedibili perché il tutto costituisca una minaccia reale. Ciò risulta lampante quando si leggono i particolari dei vari incidenti: è difficile uccidere una sola persona, e molto più difficile ucciderne una decina. Centinaia? Migliaia? Non succederà tanto presto e tanto facilmente. È molto più grande la paura del bioterrorismo, e il panico che dovesse scaturire da una minaccia bioterroristica farà del male a più persone di quante ne possa danneggiare il bioterrorismo stesso.

Molto più pericolose sono quelle contaminazioni accidentali dovute a pratiche industriali negligenti, come gli spinaci contaminati da E Coli nel 2006 e, più di recente, la salmonella nel burro di arachidi negli Stati Uniti, la contaminazione del latte in Cina nel 2008, e i bovini infetti da BSE (Encefalopatia Spongiforme Bovina) qualche anno fa. E i sistemi predisposti per trattare queste contaminazioni accidentali servono anche ad attenuare eventuali episodi intenzionali.

Nel 2004, l'allora segretario del Dipartimento della Salute e dei Servizi Umani, Tommy Thompson, dichiarò a Fox News: "Non capisco perché i terroristi non abbiano ancora attaccato le nostre scorte alimentari: sarebbe così semplice".

Beh, in realtà no, non è così semplice.

Il rapporto di Dalziel:

<http://www.rsis.edu.sg/CENS/publications/reports/RSIS_Food%20Defence_170209.pdf>
oppure <<http://tinyurl.com/r96mtj>>

La citazione di Thompson:

<<http://www.foxnews.com/story/0,2933,141044,00.html>>

Questo articolo è precedentemente apparso sul Guardian.

<<http://www.guardian.co.uk/technology/2009/may/14/bruce-schneier-bioterrorism>>
oppure <<http://tinyurl.com/pkuevo>>

** **

Pratiche sleali e ingannevoli di commercio dei dati

Sapete dove sono finiti i vostri dati ieri sera? Quasi nessuno degli oltre 27 milioni di persone che hanno risposto alle domande del quiz RealAge si è reso conto che i propri dati sanitari venivano utilizzati da compagnie farmaceutiche per sviluppare campagne di marketing via email.

Esiste un principio di base della protezione dei consumatori: il concetto di pratiche commerciali 'sleali e ingannevoli'. In sostanza, un'azienda non dovrebbe poter dichiarare una cosa e farne un'altra: vendere merci usate come nuove, mentire sull'elenco degli ingredienti di un prodotto, pubblicizzare prezzi che non sono solitamente disponibili, o affermare caratteristiche e funzionalità inesistenti, e così via.

Sepolta nel testo di 2.400 parole della policy del trattamento dei dati personali di RealAge, si può trovare questa dichiarazione: "Se si accetta di diventare un membro gratuito di RealAge, vi saranno inviate periodicamente newsletter gratuite ed email che promuovono direttamente l'uso del/dei nostro/i sito/i o l'acquisto dei nostri prodotti o servizi, e possono contenere, in toto o in parte,

annunci pubblicitari di terze parti che si riferiscono a prodotti commercializzati da partner selezionati di RealAge”.

L'azienda sostiene che quando ci si iscrive al sito Web si dà il proprio consenso a ricevere spam farmaceutico. Ma dal momento che non è precisato, non si tratta esattamente di consenso informato. E questo è ingannevole.

Il cloud computing è un'altra tecnologia dove gli utenti affidano i propri dati a fornitori di servizi. Salesforce.com, Gmail e Google Docs sono degli esempi; i vostri dati non si trovano sul vostro computer, ma da qualche parte, nella 'nuvola' (cloud), e vi accedete mediante il browser. Il cloud computing presenta notevoli vantaggi per gli utenti ed enormi potenzialità di profitto per i fornitori. È uno dei segmenti del mercato IT che sta crescendo più rapidamente (il 69% degli americani ora utilizza una qualche tipologia di servizi di cloud computing), ma l'attività commerciale è ricca di pubblicità fuorviante, se non palesemente ingannevole.

Prendiamo Google, per esempio. Il mese scorso, l'Electronic Privacy Information Center o EPIC (sono membro del consiglio di amministrazione) ha presentato un reclamo presso la Federal Trade Commission in merito ai servizi di cloud computing di Google. Sul suo sito Google rassicura ripetutamente i clienti del fatto che i loro dati sono privati e al sicuro, mentre le vulnerabilità pubblicate dimostrano il contrario. Ma a Google non sono sciocchi: i Termini di Servizio sconfessano esplicitamente qualsiasi tipo di garanzia o responsabilità per danni che potrebbero derivare da negligenza da parte di Google, deliberata imprudenza, intenti malevoli, o addirittura intenzionale inosservanza degli obblighi legali esistenti di proteggere la privacy e la sicurezza dei dati degli utenti. EPIC sostiene che questa politica sia ingannevole.

Facebook non è molto migliore. La sua Dichiarazione dei Principi, scritta in maniera leggibile (e non giuridicamente vincolante), contiene una serie di obiettivi ammirevoli, ma la sua più densa e legalistica Dichiarazione dei Diritti e delle Responsabilità ne compromette più d'uno. Un gruppo di ricerca che studia questo tipo di documentazione lo ha definito “messinscena di democrazia”: Facebook vuole mantenere l'apparenza di coinvolgere gli utenti nella direzione del servizio, senza le complicazioni di doverlo fare davvero. Ingannevole.

Questi casi non sono identici fra loro. RealAge nasconde quel che fa con i nostri dati. Google cerca al tempo stesso di rassicurarci che i nostri dati sono al sicuro e di evitare ogni responsabilità quando non lo sono. Facebook vuole commercializzare una democrazia ma di fatto è una dittatura. Il denominatore comune è il tentativo di ingannare il cliente.

Servizi di cloud computing come Google Docs, e siti di social networking come RealAge e Facebook, portano con sé notevoli rischi di privacy e sicurezza rispetto a modelli informatici tradizionali. A differenza dei dati presenti sul mio computer, che posso proteggere in qualsiasi misura ritenga adeguata, non ho alcun controllo su quei siti, né so esattamente come queste aziende proteggano la mia privacy e si occupino della mia sicurezza. Devo fidarmi di loro.

E questo può andar bene, i vantaggi possono essere certamente superiori ai rischi, ma spesso e volentieri gli utenti non possono valutare i compromessi perché queste compagnie fanno il possibile per celare i rischi.

Naturalmente le aziende non vogliono che le persone prendano decisioni informate in merito a dove lasciare i propri dati personali. RealAge non avrebbe 27 milioni di utenti se il suo sito Web dichiarasse apertamente che “vi state iscrivendo per ricevere email pubblicitarie di aziende farmaceutiche”, e Google Docs non avrebbe cinque milioni di utenti se sul sito vi fosse scritto che “Prenderemo alcuni provvedimenti per proteggere la vostra privacy ma se qualcosa va storto non siamo responsabili, non prendetevela con noi”.

E naturalmente la fiducia non è tutta bianca o tutta nera. Se, per esempio, Amazon tentasse di utilizzare le informazioni delle carte di credito dei clienti per comprarsi forniture per i propri uffici, tutti saremmo d'accordo nel dire che è scorretto. Se utilizzasse i nomi dei clienti per fare nuove proposte commerciali ai loro amici, molti di noi troverebbero questo comportamento scorretto. Quando si serve dello storico acquisti per cercare di vendere altri libri ai clienti, molti di noi apprezzano il marketing mirato. Analogamente, nessuno si aspetta la perfezione dalla sicurezza di Google. Ma se Google non sistemasse le vulnerabilità note, molti di noi lo considererebbero un problema.

Ecco perché è importante capire queste cose. Perché i mercati funzionino, gli utenti devono poter prendere delle decisioni di acquisto informate. Devono capire sia i costi che i benefici dei prodotti e dei servizi che stanno acquistando. Permettere ai venditori di manipolare il mercato mediante palesi menzogne, o celando informazioni essenziali sui loro prodotti, compromette il capitalismo; ed è per questo che il governo deve agire per garantire che i mercati funzionino senza problemi.

Il mese scorso, Mary K. Engle, Sostituto Procuratore del Bureau of Consumer Protection dell'FTC, ha dichiarato: "Il materiale di marketing di un'azienda deve essere coerente con la natura del prodotto offerto. Non basta pubblicare le informazioni a caratteri microscopici nel testo lunghissimo di un Accordo Utente online". Engle si stava riferendo alla Gestione dei Diritti Digitali (DRM) e, nello specifico, a un incidente in cui Sony utilizzò uno schema di protezione anticopia senza dichiarare pubblicamente che installava del software di nascosto sui computer dei clienti. Il DRM è diverso dal cloud computing o anche da sondaggi e quiz online, ma il principio è il medesimo.

Ancora Engle: "Se la vostra pubblicità dà e il vostro EULA [Contratto di licenza per l'utente finale] toglie, non sorprendetevi se l'FTC viene a bussare alla porta". Questa è la risposta corretta da parte del governo.

Rimandi:

<<http://www.realage.com/>>
<<http://www.nytimes.com/2009/03/26/technology/internet/26privacy.html>>
<<http://www.realage.com/corporate/privacy.aspx>>
<<http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>>
<<http://docs.google.com/support/bin/answer.py?answer=44665&topic=15119>>
<<http://docs.google.com/support/bin/answer.py?hl=en&answer=69074>>
<<http://docs.google.com/support/bin/answer.py?answer=37615&ctx=sibling>>
<<http://www.google.com/accounts/TOS?hl=en>>
<<http://www.facebook.com/topic.php?uid=54964476066&topic=7960>>
<<http://www.facebook.com/topic.php?uid=67758697570&topic=7569>>
<<http://www.lightbluetouchpaper.org/2009/03/29/commentary-on-facebooks-terms-of-service/>>
<<http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman>>
<<http://www.guardian.co.uk/technology/blog/2008/aug/06/whengoogleownsyouyourdata>>
<http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/032509_sess1.pdf>
<http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html>

Una versione di questo articolo è originariamente apparsa sul Wall Street Journal.

<<http://online.wsj.com/article/SB123997522418329223.html>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:

<http://www.schneier.com/blog/archives/2009/04/unfair_and_dece.html>

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

Le news su Schneier

Interverrò alla Computers, Freedom, and Privacy conference il 2 giugno a Washington DC.
<http://www.cfp2009.org/wiki/index.php/Main_Page>

Marcus Ranum e io abbiamo realizzato una versione video della nostra rubrica Face Off (faccia a faccia).

<http://searchsecurity.techtarget.com/video/0,297151,sid14_gci1355883,00.html>
oppure <<http://tinyurl.com/p9eznn>>

Sono stato intervistato da ThreatPost:

<<http://threatpost.com/blogs/bruce-schneier-cryptography-security-theater-and-psychology-fear>>
oppure <<http://tinyurl.com/oyyeea>>

La discussione dell'intervista su Slashdot:

<<http://it.slashdot.org/article.pl?sid=09/05/13/1822242>>

Recensioni di ristoranti a San Francisco per la RSA Conference:

<http://www.schneier.com/blog/archives/2009/04/san_francisco_r.html>

** **

Analfabetismo matematico

Questo è forse l'esempio più stupido di gestione dei rischi che abbia mai visto. È un video tratto da una puntata recente del Daily Show, sui pericoli del Large Hadron Collider. All'inizio il ritmo è un po' lento, ma poi vi è uno scambio di vedute con Walter L. Wagner, un professore di liceo, che insiste sul fatto che il dispositivo abbia una probabilità su due di distruggere il mondo:

“Se abbiamo qualcosa che può accadere, e qualcosa che non accadrà necessariamente, significa che o sta per accadere o sta per non accadere, e quindi la stima migliore è di una probabilità su due”.

“Non credo che la probabilità funzioni così, Walter”.

Seguono altri spezzoni di news show in cui questo tizio viene preso sul serio.

Parlando di matematica, quasi quattro quinti degli americani non sanno che un trilione è un milione di milioni, e molti pensano che sia meno. C'è forse da meravigliarsi perché stiamo avendo problemi nei dibattiti sul bilancio nazionale?

<<http://www.thedailyshow.com/video/index.jhtml?videoId=225921&title=Large-Hadron-Collider>>

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

<<http://econ4u.org/blog/?p=587>>

** **

Conficker

Il pesce d'aprile di Conficker, l'enorme e minacciosa tensione andata intensificandosi sempre più e poi più nulla, è un ottimo studio analitico su come consideriamo i rischi, un caso le cui lezioni sono applicabili anche molto al di fuori della sicurezza informatica. In genere, il nostro cervello non brilla molto in fatto di analisi dei rischi e delle probabilità. Tendiamo a servirci di scorciatoie cognitive invece di analisi razionali. Ciò ha funzionato bene per i rischi semplici che abbiamo incontrato sul

nostro cammino evolutivo, ma è un metodo meno efficace contro i rischi complessi che la società ci obbliga ad affrontare oggi.

Tendiamo a basare la probabilità che qualcosa accada sulla facilità con cui riusciamo a pensare a degli esempi. È per questo che la gente tende ad acquistare una polizza assicurativa contro i terremoti dopo un terremoto, quando il rischio è più basso. È per questo che chi fra noi è stato vittima di un reato tende a temere il crimine molto più di chi non ha mai avuto una simile esperienza. Ed è per questo che gli americani temono un secondo 11 settembre molto più di altri tipi di attacchi terroristici.

Abbiamo paura di essere uccisi, rapiti, violentati e assaliti da estranei, quando è molto più probabile che a commettere quei reati siano parenti o amici. Ci preoccupano più gli incidenti aerei che non quelli automobilistici, che sono molto più comuni. Tendiamo a esagerare eventi spettacolari, strani e insoliti, e minimizziamo quelli ordinari, familiari e comuni.

Inoltre tendiamo a essere più sensibili nei confronti di storie che non di dati astratti. Se vi mostrassi le statistiche sulla criminalità a New York, probabilmente non dareste gran peso a quei numeri e continuereste a pianificare la vostra vacanza. Ma se un caro amico venisse derubato laggiù, probabilmente annullereste il viaggio.

E storie specifiche, episodi particolari, sono più convincenti di fatti generali. È per questo che investiamo più denaro in polizze contro incidenti aerei che non contro incidenti di viaggio, o incidenti in generale. Oppure che, rispondendo a sondaggi, siamo propensi a pagare di più per un'assicurazione di volo che copra 'atti terroristici' che non 'tutte le cause possibili'. È per questo che, negli esperimenti condotti a proposito, le persone ritengono che specifici scenari possano accadere con maggiore probabilità rispetto a scenari generali, anche se questi ultimi includono i primi.

La scadenza di Conficker del primo aprile è stato esattamente il tipo di evento rispetto al quale gli esseri umani tendono ad avere una reazione esagerata. È una minaccia specifica, e questo ci convince della sua credibilità. È una data specifica, il che concentra la nostra paura. La nostra naturale tendenza a esagerare rende l'evento ancora più spettacolare, che a sua volta fa aumentare la paura. Il fatto che i mass media ne abbiano ripetutamente parlato, ha reso l'evento facilmente memorizzabile. E quando una storia si fa più vivida, diventa anche più convincente.

Il New York Times lo ha definito un "disastro inconcepibile", lo show televisivo 60 Minutes ha detto che avrebbe potuto "mettere fuori uso tutta Internet" e noi del Guardian abbiamo avvertito che potesse trattarsi di una "minaccia implacabile". I detrattori erano pochi e la loro voce non si è sentita granché nell'isteria generale.

Il primo aprile è passato senza incidenti, ma Conficker continua a essere pericoloso oggi come prima. Circa 2,2 milioni di computer nel mondo sono ancora infettati da Conficker.A e B, e circa 1,3 milioni sono infettati dal più temibile Conficker.C. È vero che il primo aprile Conficker.C ha tentato un nuovo trucco per auto-aggiornarsi, ma i suoi autori avrebbero potuto aggiornare il worm con un altro sistema in un giorno qualunque. Infatti lo hanno aggiornato l'8 aprile, e potrebbero farlo ancora.

E Conficker è solo uno dei tantissimi worm pericolosi gestiti da organizzazioni criminali. È arrivato con una data e tanta pubblicità (la data del primo aprile è stata più sensazionalismo che realtà) ma non è particolarmente speciale. In breve, vi sono molte organizzazioni criminali su Internet che fanno uso di worm e altre forme di malware per infettare i computer. Poi si servono di quei computer per inviare spam, commettere frodi e infettare a loro volta altri computer. I rischi sono reali e molto gravi. Fortunatamente è sufficiente mantenere aggiornato il proprio software antivirus e non fare clic su strani allegati email per avere un buon livello di protezione. Conficker si diffonde mediante una vulnerabilità di Windows che è stata riparata lo scorso ottobre. Avete l'aggiornamento automatico attivato, vero?

Ma vista la nostra natura, ci vuole un evento specifico per farci correre ai ripari.

Rimandi:

<<http://www.guardian.co.uk/technology/blog/2009/apr/01/conficker-worm-virus-april-effects>>
<<http://www.schneier.com/essay-155.html>>
<http://schneier.com/blog/archives/2007/05/rare_risk_and_o_1.html>
<<http://bits.blogs.nytimes.com/2009/03/19/the-conficker-worm-april-fools-joke-or-unthinkable-disaster/>>
<<http://www.guardian.co.uk/technology/internet>>
<<http://www.guardian.co.uk/technology/2009/mar/30/conficker-virus-computing>>
<<http://news.cnet.com/faq-conficker-time-bomb-ticks-but-dont-expect-boom/>>
<<http://blog.wired.com/27bstroke6/2009/04/conficker-war-r.html>>
<http://www.pcworld.com/article/162570/is_conficker_finally_history.html>
<http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1352838,00.html>
<<http://www.cbsnews.com/stories/2009/04/03/tech/cnettechnews/main4916468.shtml>>
<<http://www.f-secure.com/weblog/archives/00001647.html>>
<<http://blogs.iss.net/archive/confickerroundthewor.html>>
<<http://security.bkis.vn/wp-content/uploads/2009/04/conficker-statistics-v2.jpg>>
<http://www.channelregister.co.uk/2009/04/03/conficker_zombie_count/>
<http://news.cnet.com/8301-1009_3-10196122-83.html>
<<http://www.pcmag.com/article2/0,2817,2344731,00.asp>>
<<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>>

Questo articolo è precedentemente apparso sul Guardian.

<<http://www.guardian.co.uk/technology/2009/apr/23/conficker-panic>>

Una copia di questo articolo, con i rimandi integrati nel testo, è disponibile sul mio blog:

<<http://www.schneier.com/blog/archives/2009/04/conficker.html>>

** **

Commenti dei lettori

Su questi argomenti vi sono centinaia di commenti nel mio blog, molti davvero interessanti. Cercate l'argomento sul quale intendete dare la vostra opinione, e unitevi al dibattito.

<<http://www.schneier.com/blog>>

** **

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 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) 2009 - Bruce Schneier.