

CRYPTO-GRAM  
15 dicembre 2009

Scritta da Bruce Schneier  
Chief Security Technology Officer di BT  
e-mail: [schneier@schneier.com](mailto: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:

- Terroristi che prendono di mira eventi di alto profilo
- Eric Schmidt sulla Privacy
- News
- Una tassonomia dei dati del social networking
- La psicologia dell'essere truffati
- Le news su Schneier
- Reagire alle vulnerabilità di sicurezza
- Commenti dei lettori

\*\* \*\*

Terroristi che prendono di mira eventi di alto profilo

Leggendo una notizia dell'Associated Press sull'aumento di sicurezza intorno a importanti eventi di football americano, mi ha colpito in particolar modo questa frase: " 'Gli eventi di alto profilo sono il genere di cosa che i gruppi terroristici vorrebbero interrompere', ha detto Anthony Mangione, capo del dipartimento di Miami dell'U.S. Immigration and Customs Enforcement".

Questa è certamente una convinzione comune, ma vi sono prove tangibili per dimostrarne la fondatezza? I terroristi dell'11 settembre avrebbero potuto benissimo scegliere una data diversa e un evento importante -- sportivo o di altra natura -- ma non lo hanno fatto. I dinamitardi dei treni di Londra e Madrid avrebbero potuto benissimo scegliere eventi di maggior profilo da bombardare, ma non lo hanno fatto. I terroristi di Mumbai hanno scelto un giorno qualsiasi e dei bersagli qualunque. Aum Shinrikyo ha scelto un giorno qualsiasi e delle linee ferroviarie comunissime. Timothy McVeigh scelse il banale Federal Building di Oklahoma City. I terroristi irlandesi scelsero, e i terroristi palestinesi continuano a scegliere, bersagli ordinari, comuni. In parte si può attribuire questa scelta al fatto che i bersagli comuni sono più semplici da attaccare, ma non del tutto.

Gli unici esempi di terroristi che scelgono bersagli o eventi di alto profilo sono quegli idioti aspiranti terroristi che non sarebbero stati capaci di combinare nulla se non fossero stati incitati da un informatore del governo. Prove tutt'altro che convincenti.

Sì, ho visto il film "Black Sunday". Ma esiste qualche ragione per credere che i terroristi vogliano prendere di mira questo genere di eventi, oltre alle proiezioni delle nostre paure e pregiudizi sui moventi dei terroristi?

La notizia dell'Associated Press:

<[http://www.huffingtonpost.com/2009/12/03/orange-bowl-pro-bowl-and-n\\_379052.html](http://www.huffingtonpost.com/2009/12/03/orange-bowl-pro-bowl-and-n_379052.html)>

oppure <<http://tinyurl.com/yhc9kpe>>

Gli idioti aspiranti terroristi:

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

Qualche anno fa scrissi sulla sicurezza e i playoff di baseball (World Series).

<<http://www.schneier.com/essay-065.html>>

\*\* \*\*

Eric Schmidt sulla Privacy

Schmidt ha detto:

"Ritengo che il giudizio sia importante. Se c'è qualcosa che non volete che gli altri vengano a sapere, forse dovrete cominciare col non farla. Se avete davvero bisogno di quel genere di privacy, la realtà dei fatti è che i motori di ricerca, Google compreso, conservano queste informazioni per un certo periodo, ed è importante, per esempio, che negli Stati Uniti tutti siamo soggetti al Patriot Act; è quindi possibile che tutte quelle informazioni vengano presentate alle autorità se ne viene fatta richiesta".

Ecco la mia risposta (che risale al 2006):

“La privacy ci protegge dagli abusi di chi detiene il potere, anche se non stiamo facendo niente di male mentre veniamo sorvegliati.

“Non facciamo niente di male quando facciamo l’amore o andiamo al bagno. Non stiamo volontariamente nascondendo nulla di particolare quando cerchiamo un angolo tranquillo per riflettere o conversare. Teniamo diari privati, cantiamo nella privacy della doccia, scriviamo lettere ad amanti segreti per poi bruciarle. La privacy è un’esigenza umana essenziale.

[...]

“Perché se veniamo osservati in ogni cosa che facciamo, siamo costantemente esposti a correzioni, giudizi, critiche, persino al plagio della nostra unicità. Diventiamo bambini, incatenati e sotto continua osservazione, sempre col terrore che, oggi o in un futuro incerto, la trama di azioni che ci lasciamo alle spalle possa essere ripresa per implicarci, per mano di qualsiasi autorità ora concentrata su quelle azioni innocenti, che in passato erano anche private. Perdiamo la nostra individualità, perché tutto quel che facciamo è osservabile e registrabile.

[...]

“Questa è la perdita di libertà che affrontiamo quando veniamo privati della nostra privacy. Questa era la vita nell’ex Germania dell’Est o nell’Iraq di Saddam Hussein. E sarà il nostro futuro se lasciamo che un “occhio” costantemente invadente entri a osservare la nostra vita privata.

“In troppi definiscono il dibattito secondo la linea ‘sicurezza di contro alla privacy’. La vera scelta è invece libertà in opposizione al controllo. La tirannia, che si sviluppi dalla minaccia di un attacco straniero o dalla continua sorveglianza interna da parte delle autorità, è sempre tirannia. La libertà richiede la sicurezza senza intrusione: sicurezza PIÙ privacy. L’onnipresente sorveglianza da parte delle forze dell’ordine è la pura e semplice definizione di uno stato di polizia. Ed è per questo che dovremmo difendere la privacy anche quando non abbiamo nulla da nascondere”.

Le osservazioni di Schmidt:

<<http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people>>

Il mio articolo sul valore della Privacy:

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

Si veda anche lo scritto di Daniel Solove: “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy” [‘Non ho nulla da nascondere’ e altri malintesi in ambito di privacy].

<[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=998565](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565)>

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

News

Ricerca interessante sulle reazioni del pubblico alle minacce terroristiche. Non c'è da sorprendersi: la paura rende le persone deferenti, docili e diffidenti, e politici e venditori hanno imparato a trarre vantaggio da questi sentimenti.

<[http://www.schneier.com/blog/archives/2009/11/public\\_reaction.html](http://www.schneier.com/blog/archives/2009/11/public_reaction.html)>

Jennifer Merolla ed Elizabeth Zechmeister hanno scritto un libro, "Democracy at Risk: How Terrorist Threats Affect the Public" [Democrazia a rischio: come le minacce terroristiche incidono sul pubblico]. Non l'ho ancora letto.

<<http://www.amazon.com/gp/product/0226520552/counterpane/>>

Un'immagine divertente: rilevamento anti-malware e il Cavallo di Troia originale.

<<http://www.sampsonuk.net/B3TA/TrojanHorse.jpg>>

Uno studio nel British Journal of Criminology sostiene che il drogare un drink ai fini del cosiddetto 'date rape' (stupro perpetrato da persona nota alla vittima) sia sostanzialmente una leggenda urbana. L'ipotesi: perpetuare la paura di questo genere di violenza sessuale permette a genitori e amici di mettere in guardia le ragazze sull'eccesso di alcool senza criticarne le scelte personali. Il finto spauracchio consente alle persone di evitare di parlare delle vere problematiche sottostanti.

<[http://www.schneier.com/blog/archives/2009/11/a\\_useful\\_side-e.html](http://www.schneier.com/blog/archives/2009/11/a_useful_side-e.html)>

Serrature che aprono porte se si batte un ritmo particolare.

<<http://www.engadget.com/2009/11/04/secret-knock-door-lock-defends-home-from-rhythmically-impaired/>>

oppure <<http://tinyurl.com/yes7sy5>>

<<http://spritesmods.com/?art=knock2open>>

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

Brillante ricerca nell'ambito del "quantum ghost imaging". Malgrado il nome, non ha nulla a che vedere con la meccanica quantistica. È un modo di utilizzare una macchina fotografica e una fonte luminosa per produrre immagini di oggetti che la macchina fotografica non può vedere.

<<http://www.newscientist.com/article/dn13825>>

<<http://www.globalsecurity.org/military/library/news/2009/11/mil-091102-afps05.htm>>

oppure <<http://tinyurl.com/yzo22l8>>

<[http://arxiv1.library.cornell.edu/PS\\_cache/arxiv/pdf/0807/0807.2614v1.pdf](http://arxiv1.library.cornell.edu/PS_cache/arxiv/pdf/0807/0807.2614v1.pdf)>

oppure <<http://tinyurl.com/y9cxzvb>>

Quanto sono intelligenti i terroristi islamici? Secondo "Organizational Learning and Islamic Militancy" [Apprendimento organizzativo e militanza islamica] scritto da Michael Kenney per il Dipartimento di Giustizia Statunitense il maggio scorso, non molto.

<[http://www.schneier.com/blog/archives/2009/11/how\\_smart\\_are\\_i.html](http://www.schneier.com/blog/archives/2009/11/how_smart_are_i.html)>

Una ricerca sul pugnalarle le persone con oggetti che possono essere ammessi dalla sicurezza aeroportuale.

<[http://www.ncbi.nlm.nih.gov/pubmed/17325460?itool=EntrezSystem2.PEntrez.Pubmed.Pubmed\\_ResultsPanel.Pubmed\\_RVDocSum&ordinalpos=257](http://www.ncbi.nlm.nih.gov/pubmed/17325460?itool=EntrezSystem2.PEntrez.Pubmed.Pubmed_ResultsPanel.Pubmed_RVDocSum&ordinalpos=257)>

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

Attacchi di tipo Denial-of-service contro CALEA:

<<http://www.schneier.com/blog/archives/2009/11/denial-of-servi.html>>

Divertente: non farà molta carriera.

<<http://failblog.org/2009/11/07/career-fair-fail/>>

Si veda la didascalia della foto originale per sapere come sono realmente andate le cose.

<<http://www.flickr.com/photos/paperghost/776598575/in/set-72157600761788702/>>

oppure <<http://tinyurl.com/ykrxc8o>>

Decodificato il codice segreto di Al Qaeda: forse è una storia vera, forse no.

<[http://www.schneier.com/blog/archives/2009/11/al\\_qaeda\\_secret.html](http://www.schneier.com/blog/archives/2009/11/al_qaeda_secret.html)>

Decertificare piloti 'terroristi':

<[http://www.schneier.com/blog/archives/2009/11/decertifying\\_te.html](http://www.schneier.com/blog/archives/2009/11/decertifying_te.html)>

Norbt (no robot) è un'applicazione Web a bassa sicurezza che consente di criptare pagine Web. Si può creare e criptare una pagina Web. La chiave di decodifica è la risposta a una domanda: chi conosce la risposta può visualizzare la pagina. Non vedo una grande utilità in questa applicazione.

<<https://norbt.com/>>

Questo studio di Cormac Herley (Microsoft Research), che parla di utenti che rifiutano razionalmente i consigli di sicurezza, suona proprio come me:

<<http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf>>

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

Un articolo analogo sulla sicurezza usabile:

<<http://cacm.acm.org/magazines/2009/11/48419-usable-security-how-to-get-it/fulltext>>

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

Se in un mondo online si permette ai giocatori di penalizzarsi a vicenda, si apre la strada all'estorsione.

<[http://www.schneier.com/blog/archives/2009/11/virtual\\_mafia\\_i.html](http://www.schneier.com/blog/archives/2009/11/virtual_mafia_i.html)>

Un articolo lungo, dettagliato, e di ottima qualità sugli attacchi terroristici di Mumbai dell'anno scorso.

<<http://www.vqronline.org/webexclusive/2009/11/19/motlagh-mumbai-attacks/>>

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

Il mio breve commento a seguito degli attacchi.

<[http://www.schneier.com/blog/archives/2008/12/lessons\\_from\\_mu.html](http://www.schneier.com/blog/archives/2008/12/lessons_from_mu.html)>

Wikileaks ha pubblicato intercettazioni di dati trasmessi dai pager a New York l'11 settembre 2001. È inquietante scoprire che qualcuno, probabilmente nemmeno un'entità governativa, stava periodicamente intercettando gran parte del traffico

dati (o forse tutto il traffico) dei pager in lower Manhattan già nel 2001. Di chi si trattava? Per quale motivo? Non lo sappiamo.

<[http://www.schneier.com/blog/archives/2009/11/leaked\\_911\\_text.html](http://www.schneier.com/blog/archives/2009/11/leaked_911_text.html)>

Questa intervista del 1996 con lo psichiatra Robert DuPont era parte di un programma Frontline intitolato "Nuclear Reaction" [Reazione Nucleare]. DuPont parla del ruolo che gioca la paura nella percezione della potenza nucleare. È un po' lo stesso genere di cose che dico anch'io, ma sono particolarmente interessanti i suoi commenti sulla familiarità e di come essa attenui la paura.

<<http://www.pbs.org/wgbh/pages/frontline/shows/reaction/interviews/dupont.html>>

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

Per cui, oltre a varie altre ragioni, il terrorismo fa paura perché è un fenomeno così raro. Quando è più consueto (come nel Regno Unito durante le agitazioni in Irlanda del Nord, o in Israele oggi), le persone reagiscono in maniera più razionale.

<[http://www.schneier.com/blog/archives/2009/11/fear\\_and\\_overre.html](http://www.schneier.com/blog/archives/2009/11/fear_and_overre.html)>

Un mio lungo articolo sulla condotta dello stato di guerra cibernetica; molti link.

<[http://www.schneier.com/blog/archives/2009/12/cyberwarfare\\_po.html](http://www.schneier.com/blog/archives/2009/12/cyberwarfare_po.html)>

Questa ricerca è incentrata sull'analisi delle caratteristiche radio dei singoli chip RFID e sulla conseguente creazione di una 'impronta digitale'. È una cosa sensata: identificare e separare i singoli segnali radio basandosi sulle loro caratteristiche di trasmissione è un procedimento che risale alla Seconda Guerra Mondiale. Ma sebbene lo scopo primario della ricerca sia utilizzare questo metodo come misura anti-contraffazione, ritengo che potrebbe essere usato più probabilmente come strumento di identificazione e sorveglianza. Anche se la comunicazione è interamente criptata, questa tecnologia potrebbe venire utilizzata per identificare il singolo chip in modo inequivocabile.

<<http://dailyheadlines.uark.edu/16260.htm>>

Con Windows Volume Shadow Copy, può essere impossibile cancellare un file in modo sicuro.

<<http://blog.szynalski.com/2009/11/23/volume-shadow-copy-system-restore/>>

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

Sprint fornisce alle forze dell'ordine statunitensi i dati di posizionamento cellulare dei propri clienti:

<[http://www.schneier.com/blog/archives/2009/12/sprint\\_provides.html](http://www.schneier.com/blog/archives/2009/12/sprint_provides.html)>

Usare documenti falsi per ottenere un passaporto USA valido:

<[http://www.schneier.com/blog/archives/2009/12/using\\_fake\\_docu.html](http://www.schneier.com/blog/archives/2009/12/using_fake_docu.html)>

Nessuna credenziale può essere più sicura dei documenti che la generano e delle procedure di emissione di tali documenti.

Un articolo sulla 'epidemiologia emotiva' del New England Journal of Medicine. Suona familiare.

<[http://www.schneier.com/blog/archives/2009/12/emotional\\_epide.html](http://www.schneier.com/blog/archives/2009/12/emotional_epide.html)>

La TSA ha pubblicato accidentalmente le proprie procedure operative standard:

<[http://www.schneier.com/blog/archives/2009/12/tsa\\_publishes\\_s.html](http://www.schneier.com/blog/archives/2009/12/tsa_publishes_s.html)>  
Potrebbe aver compromesso un programma di intelligence:  
<[http://politics.theatlantic.com/2009/12/did\\_the\\_tsa\\_compromise\\_an\\_intelligence\\_program.php](http://politics.theatlantic.com/2009/12/did_the_tsa_compromise_an_intelligence_program.php)>  
oppure <<http://tinyurl.com/y96ngm5>>

Non ci sono novità sul responsabile per la sicurezza cibernetica designato da Obama:

<[http://www.schneier.com/blog/archives/2009/12/obamas\\_cybersec\\_1.html](http://www.schneier.com/blog/archives/2009/12/obamas_cybersec_1.html)>  
Per la cronaca (visto che di tanto in tanto girano queste voci), non sono interessato a ricoprire quel ruolo.

Wondermark sulle password:  
<<http://wondermark.com/576/>>

Sono iniziati colloqui sul controllo delle armi cibernetiche fra Stati Uniti e Russia:  
<[http://www.schneier.com/blog/archives/2009/12/usrussia\\_cyber.html](http://www.schneier.com/blog/archives/2009/12/usrussia_cyber.html)>

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

#### Una tassonomia dei dati del social networking

All'Internet Governance Forum a Sharm El Sheikh questa settimana si è parlato dei dati del social networking. Qualcuno ha fatto notare come esistano svariati tipi di dati, e che sarebbe utile poterli distinguere. Questa è la mia tassonomia dei dati del social networking.

1. Dati di servizio. I dati di servizio sono quelle informazioni che è necessario fornire al sito di social networking per poterne fare uso. Tali informazioni potrebbero comprendere nome e cognome, età e numero di carta di credito.
2. Dati divulgati, pubblici. Sono i contenuti che si pubblicano sulle proprie pagine: entrate di blog, fotografie, messaggi, commenti, eccetera.
3. Dati affidati. È ciò che si pubblica sulle pagine di altre persone. In sostanza, si tratta dello stesso tipo di dati divulgati visti prima, ma la differenza è che non si ha il controllo di questi dati: qualcun altro lo ha (la persona sulla cui pagina si è scritto o commentato, per esempio).
4. Dati accidentali. I dati accidentali (o casuali, o accessori, ecc.) sono quelle informazioni che altre persone scrivono su di noi. Anche in questo caso, si tratta dello stesso tipo di dati divulgati visti al punto 2, ma la differenza è che 1) non abbiamo il controllo su queste informazioni, e 2) non le abbiamo nemmeno create noi.
5. Dati comportamentali. Sono le informazioni sulle nostre abitudini che il sito di social networking raccoglie registrando quel che facciamo e con chi lo facciamo.

I vari siti di social networking offrono agli utenti diritti diversi a seconda del tipo di dati. Certe informazioni sono sempre private, altre possono essere rese private, altre ancora sono sempre pubbliche. Alcuni dati possono essere modificati o eliminati (conosco un sito che permette di modificare o cancellare i dati affidati in un arco di 24 ore) e altri no. Alcuni dati possono essere visualizzati e altri no.

E le persone *\*dovrebbero\** avere diritti diversi a seconda del tipo di dati. È ovvio che a tutti dovrebbe essere permesso modificare ed eliminare i propri dati divulgati. È meno ovvio capire quali siano i diritti nel caso dei dati affidati. Ancora meno ovvio il caso dei dati accidentali. Se pubblicate delle foto di una festa e io compaio in quelle foto, è nel mio diritto obbligarvi a togliere quelle foto o almeno a sfuocare il mio viso? E che dire dei dati comportamentali? Spesso sono l'elemento fondamentale del modello di business di un sito di social networking. Altrettanto spesso non ci importa se il sito li sfrutta per produrre pubblicità mirata, ma probabilmente non siamo così tolleranti sul fatto che il sito possa vendere quei dati a terze parti.

Mentre proseguono i nostri dibattiti sui tipi di diritti fondamentali che hanno le persone rispetto ai propri dati, questa tassonomia potrà essere uno strumento utile.

Molta discussione sul mio blog:

<[http://www.schneier.com/blog/archives/2009/11/a\\_taxonomy\\_of\\_s.html](http://www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html)>

Un'altra categorizzazione che si incentra sulla destinazione dei dati invece che sul livello di fiducia:

<<http://mechpoe.blogspot.com/2009/11/another-categorization-of-social.html>>

oppure <<http://tinyurl.com/y9q5exr>>

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

La psicologia dell'essere truffati

Si tratta di uno studio molto interessante: "Understanding scam victims: seven principles for systems security" di Frank Stajano e Paul Wilson. Paul Wilson produce e appare nello show televisivo inglese The Real Hustle, che effettua dimostrazioni di truffe e raggiri mediante candid camera. (Non esiste un DVD dello show, ma si possono trovare degli spezzoni su YouTube). Frank Stajano proviene dal Laboratorio Informatico dell'Università di Cambridge.

Lo studio descrive una dozzina di scenari di truffa, di per sé molto divertenti, e quindi elenca e spiega sei principi psicologici generali che vengono utilizzati dai truffatori:

1. Il principio della distrazione. Mentre si è distratti da ciò che attrae la nostra attenzione, l'imbroglione può fare quello che vuole e non ce ne accorgeremo.



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

## Reagire alle vulnerabilità di sicurezza

Il mese scorso alcuni ricercatori hanno scoperto una vulnerabilità di sicurezza nel protocollo SSL, che viene utilizzato per proteggere informazioni sensibili sul Web. Si usa questo protocollo per il commercio elettronico, per l'interfaccia Web della posta elettronica, e nei siti di social networking. In sostanza gli hacker potrebbero dirottare una sessione SSL ed eseguire comandi all'insaputa sia del client che del server. L'elenco dei prodotti colpiti da tale vulnerabilità è enorme.

Se vi sembra un problema grave, avete ragione. È grave di sicuro. Detto questo, che cosa dovrete fare adesso? Dovreste smettere di utilizzare SSL finché non viene riparata la vulnerabilità, e pagare gli acquisti Internet per telefono? Dovreste scaricare una qualche protezione? Dovreste intraprendere qualche altra azione per porre rimedio al problema? E quale?

Se leggete la stampa IT con regolarità, noterete questo genere di interrogativi emergere in continuazione. La risposta in merito a questa precisa vulnerabilità, come per la stragrande maggioranza delle altre vulnerabilità di cui si legge, è la stessa: non fate nulla. Proprio così, nulla. Non fatevi prendere dal panico. Non cambiate il vostro comportamento abituale. Ignorate il problema e lasciate che siano i produttori di software a occuparsene.

Vi sono diverse ragioni per giustificare questa risposta. In primo luogo, è difficile riuscire a distinguere quali vulnerabilità sono gravi e quali non lo sono. Vulnerabilità come questa appaiono molte volte in un mese. Riguardano software diversi, sistemi operativi diversi, e diversi protocolli Web. La stampa a volte ne parla, a volte no, in modo abbastanza casuale; solo perché se ne dà notizia, non significa che una certa vulnerabilità sia per forza grave.

In secondo luogo, è difficile capire se è possibile farci qualcosa. Molte vulnerabilità colpiscono sistemi operativi o protocolli Internet. L'unica contromisura efficace sarebbe quella di non usare il computer. Alcune vulnerabilità hanno conseguenze sorprendenti. La vulnerabilità di SSL di cui si è parlato poco sopra, per esempio, potrebbe essere utilizzata per compromettere Twitter. Ve lo aspettavate? Io no di certo.

In terzo luogo, le probabilità che una determinata vulnerabilità possano colpirci direttamente sono ridotte. Vi sono molti pesci su Internet, e voi siete solo uno dei miliardi di possibili bersagli.

In quarto luogo, spesso noi (ossia gli utenti finali) non possiamo farci nulla. Queste vulnerabilità colpiscono client e server, privati cittadini e aziende. Non abbiamo un diretto controllo su molti dei nostri dati, perché si trovano sui server di posta elettronica basata sul Web, in qualche database aziendale, o in una applicazione di cloud computing. Se una vulnerabilità prende di mira i computer su cui gira Facebook, per esempio, i nostri dati sono a rischio, che noi effettuiamo il login o meno.

È molto più intelligente avere sempre una serie ragionevole di pratiche di sicurezza basilari, e di continuare a metterle in atto. Fra queste ricordo:

1. Installare un programma antivirus se avete Windows, e configurarlo in modo da aggiornarsi quotidianamente. Non importa quale sia; si assomigliano un po' tutti. Per Windows, a me piace particolarmente la versione gratuita di AVG Internet Security. Gli utenti Mac e Linux possono ignorare questo suggerimento, dato che gli autori di virus prendono di mira il sistema operativo con la quota di mercato maggiore.

2. Configurare correttamente il sistema operativo e il router. I sistemi operativi di Microsoft vengono installati con parecchie funzioni di sicurezza abilitate per default, ed è un'ottima cosa. Ma è altrettanto importante far controllare la configurazione del router da qualcuno che se ne intenda.

3. Attivare gli aggiornamenti automatici del software. Questo è il meccanismo con cui il software si aggiorna e si ripara da solo in background, senza che si debba far nulla. Assicurarsi che sia attivato per il computer, il sistema operativo, il software di sicurezza, e per qualsiasi applicazione che disponga di tale opzione. Sì, occorre attivarlo per ogni software, dato che spesso i meccanismi di aggiornamento automatico sono distinti.

4. Usare il buonsenso quando si tratta di Internet. Questa può essere la cosa più difficile e più importante da mettere in pratica. Sappiate distinguere quando un'email è genuina e quando è meglio non fare clic su link o allegati. Sappiate capire quando un sito Web è sospetto. Sappiate percepire quando qualcosa non quadra.

5. Effettuare backup regolarmente. Questo è essenziale. Se si viene colpiti da un virus e simili, potrebbe essere necessario reinstallare il sistema operativo e le applicazioni. Un buon backup mette al sicuro dalla perdita di dati (documenti, fotografie, musica) nel caso occorresse procedere in questo senso.

Tutto qui. Potrei fornire un elenco più lungo e articolato di pratiche informatiche sicure, ma questa versione semplificata dovrebbe essere sufficiente a mantenervi al sicuro. Dopodiché, abbiate fiducia nei produttori. Hanno passato tutto il mese scorso nel disperato tentativo di sistemare la vulnerabilità SSL, e passeranno tutto questo mese cercando di fare il possibile per sistemare qualunque nuova vulnerabilità sia apparsa nel frattempo. Lasciamo che sia un loro problema.

La vulnerabilità SSL:

<<http://www.eweekurope.co.uk/news/security-researchers-uncover-ssl-vulnerability-2355>>

oppure <<http://tinyurl.com/yge9not>>

<[http://www.linuxtoday.com/news\\_story.php3?ltsn=2009-11-06-008-35-NW-DV-NT](http://www.linuxtoday.com/news_story.php3?ltsn=2009-11-06-008-35-NW-DV-NT)>

oppure <<http://tinyurl.com/yb9pxsa>>

<<http://isc.sans.org/diary.html?storyid=7534>>

<[http://searchsecurity.techtarget.com/news/article/0,289142,sid14\\_gci1373678,00.html](http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1373678,00.html)>

oppure <<http://tinyurl.com/yhw7vvhb>>  
<<http://www.tombom.co.uk/blog/?p=85>>  
<<http://www.securityfocus.com/bid/36935/info>>

La vulnerabilità SSL utilizzata per compromettere Twitter:  
<[http://www.techworld.com.au/article/326496/ssl\\_flaw\\_could\\_been\\_used\\_hack\\_twitter](http://www.techworld.com.au/article/326496/ssl_flaw_could_been_used_hack_twitter)>

oppure <<http://tinyurl.com/yevj4uv>>  
<<http://www.eweek.com/c/a/Security/Researcher-Demonstrates-SSL-Vulnerability-on-Twitter-291904/>>  
oppure <<http://tinyurl.com/yejjhkz>>

L'antivirus AVG:  
<<http://lifehacker.com/5401255/best-antivirus-application-avg>>

Il mio articolo del 2004 sull'utilizzo sicuro del personal computer:  
<[http://www.schneier.com/blog/archives/2004/12/safe\\_personal\\_c.html](http://www.schneier.com/blog/archives/2004/12/safe_personal_c.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, 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](mailto:crypto-gram@communicationvalley.it)

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

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di BT Counterpane e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Frequentemente scrive e partecipa a conferenze sulla sicurezza informatica e sulla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

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

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

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

Copyright (c) 2009 - Bruce Schneier.