

CRYPTO-GRAM
15 maggio 2007

Scritta da Bruce Schneier
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA
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-0705.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:

- Un mercato per i prodotti di sicurezza scadenti
- Occorre davvero temere il "Grande Fratello"?
- Un video per addestrare i cittadini contro il terrorismo
- News
- Saper individuare ciò che non quadra e i cittadini informatori
- Ancora sul REAL ID
- Ubicazione di minor rischio per un ordigno ("Least risk bomb location")
- Appunti di ingegneria sociale
- Le news su Schneier/BT Counterpane
- Un campanello anti-spam del 1933
- La segretezza contribuisce a proteggere le informazioni personali?
- Vale la pena effettuare dei test di penetrazione?
- Abbiamo veramente bisogno di un'industria della sicurezza?
- Commenti dei lettori

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

Un mercato per i prodotti di sicurezza scadenti

Più di un anno fa parlai del rischio sempre maggiore di perdere i propri dati dovuto al fatto che è possibile archiviare una quantità sempre più grande di informazioni in dispositivi sempre più minuscoli. Attualmente mi servo di un memory stick USB da 4 GB per il mio backup quando sono in viaggio. È una soluzione molto comoda e che apprezzo, ma se dovessi smarrire quest'oggettino metterei a rischio tutti i miei dati.

La soluzione più ovvia a questo problema è la crittografia, infatti uso PGPdisk, ma Secustick sembra un prodotto migliore: cancella automaticamente tutte le informazioni in esso contenute dopo un numero prestabilito di tentativi falliti di inserimento password. L'azienda produttrice si lascia andare a una serie di impressionanti dichiarazioni: il prodotto è stato commissionato e infine approvato dall'intelligence service francese; il prodotto viene utilizzato da svariate entità militari e banche; la tecnologia di Secustick è rivoluzionaria, eccetera.

Purtroppo l'unico aspetto davvero impressionante di Secustick è la sua arroganza e insolenza, messa a nudo quando Tweakers.net ne ha totalmente annientato la sicurezza. Non esiste alcuna funzione di autodistruzione delle informazioni. La protezione mediante password può essere aggirata facilmente. I dati non sono nemmeno criptati. Come dispositivo di memorizzazione sicuro, Secustick si rivela piuttosto inutile.

Superficialmente, questa non è altro che l'ennesima storia di un prodotto-burla di sicurezza. Ma sorge una domanda più profonda: perché esistono in commercio così tanti prodotti di sicurezza scadenti? Non è semplicemente perché progettare ottima sicurezza sia difficile (lo è, in effetti), e neanche perché un individuo qualsiasi sia in grado di ideare un prodotto di sicurezza che egli stesso non può penetrare. Perché i prodotti di sicurezza mediocri battono i migliori sul mercato?

Nel 1970, l'economista americano George Akerlof scrisse uno studio intitolato "The Market for 'Lemons'" [Il mercato dei 'bidoni'], che stabilì la teoria dell'informazione asimmetrica. Egli poi ottenne un Premio Nobel per il suo lavoro, che osserva quei mercati in cui il venditore conosce molte più informazioni sul prodotto rispetto all'acquirente.

Akerlof dimostrò le proprie teorie servendosi del mercato delle auto usate. Il mercato delle auto usate racchiude sia ottime macchine, sia macchine scadenti (i 'bidoni'). Il venditore sa qual è l'automobile buona e quella mediocre, ma l'acquirente non è in grado di distinguerle, almeno finché non ha effettuato l'acquisto. Vi risparmio la parentesi matematica, ma la conclusione è che l'acquirente basa il prezzo d'acquisto sul valore di un'auto usata di media qualità.

Questo significa che le automobili migliori non vengono vendute: il loro prezzo è troppo alto. Il che significa a sua volta che i proprietari di queste auto migliori non le mettono sul mercato. E qui inizia la spirale. La rimozione delle auto di buona qualità dal mercato riduce il prezzo medio che gli acquirenti sono disposti a pagare, di conseguenza le macchine di ottima qualità non si vendono più e spariscono dal mercato. Poi spariscono quelle di buona qualità, e così via finché non rimangono che i bidoni.

In un mercato in cui il venditore è in possesso di maggiori informazioni sul prodotto rispetto all'acquirente, i prodotti peggiori possono far uscire i migliori dal mercato.

Il mercato dei prodotti di sicurezza informatica presenta molte delle caratteristiche del "mercato dei bidoni" di Akerlof. Prendiamo per esempio il mercato delle chiavette USB con crittografia. Molte aziende realizzano prodotti di questo tipo; Kingston Technology me ne ha inviato uno per posta qualche giorno fa. Ma nemmeno io saprei dire se l'offerta di Kingston sia migliore di Secustick o se sia migliore di qualsiasi altra chiavetta USB criptata. Tutte sfruttano i medesimi algoritmi. Tutte le aziende promettono la

massima sicurezza. E se io non sono in grado di distinguere fra le varie offerte di questo genere, figuriamoci la maggior parte dei consumatori.

Naturalmente, è molto più costoso produrre un'unità USB davvero sicura. Progettare una sicurezza efficace richiede tempo, e significa giocoforza limitare le funzionalità. Effettuare verifiche di sicurezza di buon livello richiede un tempo ancora maggiore, specialmente se il prodotto è buono. Ciò significa che il prodotto meno sicuro costerà meno, arriverà prima sul mercato, e avrà un maggior numero di funzionalità. In questo mercato, la chiavetta USB più sicura ha già perso in partenza.

Sto notando questa dinamica sempre più frequentemente nell'ambito della sicurezza informatica. Alla fine degli anni Ottanta e nei primi Novanta esistevano più di un centinaio di firewall in competizione fra loro. I pochi che prevalsero non erano i firewall più sicuri, ma quelli più facili da impostare, più semplici da usare e che non infastidivano troppo gli utenti. Dato che gli acquirenti non potevano impostare la propria decisione di acquisto sul valore in termini di sicurezza di un prodotto rispetto a un altro, si sono basati su questi altri criteri. Il mercato dei sistemi anti-intrusione (IDS) si è evoluto allo stesso modo, e prima di questo il mercato degli antivirus. I pochi prodotti che hanno avuto successo non sono stati i più sicuri, perché gli acquirenti non erano in grado di notare le differenze fra di essi.

Come si può risolvere la questione? Occorre quel che gli economisti chiamano "segnale", qualcosa che possa aiutare chi compra a distinguere, a notare le differenze. Le garanzie sono uno dei segnali più diffusi. In alternativa, un meccanico indipendente può distinguere una buona automobile da un bidone, e un acquirente può affidarsi alla sua esperienza in materia. La vicenda di Secustick lo dimostra. Se esiste un gruppo di supporto per i consumatori che possiede l'esperienza necessaria per valutare i vari prodotti, allora è possibile smascherare i bidoni.

Per esempio, pare che Secustick sia stato ritirato dalle vendite.

Ma le verifiche di sicurezza sono costose e lente, ed è semplicemente impossibile per un laboratorio indipendente testare ogni prodotto. Purtroppo lo smascheramento di Secustick è un'eccezione e non la norma. Si trattava di un dispositivo poco sofisticato, e semplice da denunciare una volta che qualcuno si è preso la briga di esaminarlo. Un prodotto software più complesso (come un firewall, un IDS...) è molto difficile da verificare per bene. E naturalmente, quando i test si sono conclusi, il produttore ne ha già introdotta una nuova versione sul mercato.

In realtà dobbiamo affidarci a una serie di segnali mediocri per distinguere i buoni prodotti di sicurezza da quelli scadenti. La standardizzazione è uno di questi segnali. Lo standard crittografico AES, estremamente diffuso, ha ridotto (anche se non eliminato del tutto) la quantità di orribili algoritmi di crittografia presenti sul mercato. La reputazione è già un segnale più comune: si scelgono prodotti di sicurezza basandosi sulla reputazione dell'azienda che li produce, sulla reputazione di qualche guru della sicurezza a essi associato, sulle varie recensioni a riguardo, sui consigli di colleghi o su quanto riportano i media.

Tutti questi segnali hanno i loro inconvenienti. Anche le recensioni dei prodotti, che dovrebbero essere esaurienti almeno quanto quella di Tweakers su Secustick, raramente lo sono. Molte recensioni che mettono a confronto differenti firewall si concentrano su elementi che gli autori degli articoli possono facilmente misurare, come

La raccolta di informazioni in "1984" era intenzionale; oggi è involontaria. Nella società dell'informazione noi ci troviamo a generare dati spontaneamente. Nel mondo di Orwell le persone erano per natura anonime; oggi noi tutti lasciamo tracce digitali dappertutto.

Lo stato di polizia di "1984" era centralizzato; oggi è decentralizzato. Le compagnie telefoniche sanno chi chiamate, le compagnie delle carte di credito sanno dove fate i vostri acquisti e Netflix sa quali film guardate. Il vostro Internet Provider può leggere le vostre email; il telefonino può tracciare i vostri movimenti e i supermercati possono controllare ciò che preferite comprare. Non esiste un'unica entità governativa che raccoglie tutti questi dati, perché non ce n'è bisogno. Come ha detto Neal Stephenson, la minaccia non è più rappresentata dal Grande Fratello, ma da migliaia di Piccoli Fratelli.

Il Grande Fratello di "1984" era condotto dallo stato; il Grande Fratello di oggi viene condotto dal mercato. Data broker come ChoicePoint e agenzie di credito come Experian non stanno cercando di creare uno stato di polizia, ma solo di ricavare profitti. Ovviamente queste compagnie approfitteranno dei documenti di identità nazionali, sarebbero degli stupidi a non farlo. E il tipo di correlazioni, di data mining e di precise categorizzazioni che queste entità sono in grado di effettuare sono la ragione per cui il governo degli Stati Uniti compra da loro le informazioni commerciali.

Gli stati di polizia stile "1984" necessitavano di un gran numero di persone. La Germania dell'Est si serviva di un informatore ogni 66 cittadini. Oggi non c'è motivo di assumere persone per osservare altre persone; ci sono i computer che possono fare questo lavoro.

Gli stati di polizia stile "1984" erano molto costosi. Oggi la memorizzazione dei dati si sta facendo sempre più economica. Se è troppo caro salvare certe informazioni oggi, sarà fattibile nel giro di pochi anni.

Infine, lo stato di polizia di "1984" fu costituito deliberatamente, mentre oggi sta emergendo spontaneamente. Non vi è motivo di postulare una forza di polizia malevola e un governo che tentano di sconvolgere le nostre libertà. I processi informatici producono naturalmente dati personalizzati; le compagnie li archiviano a scopo di marketing e finiranno con l'essere utilizzati anche dalle forze dell'ordine più oneste e benintenzionate.

Certo, il Grande Fratello orwelliano possedeva una spietata efficienza che è difficile immaginare in un governo attuale. Ma questo non vuol dire assolutamente nulla. Uno stato di polizia approssimativo e inefficiente non è tanto migliore: basta guardare il film "Brazil" per rendersi conto di quanto possa essere pauroso un simile scenario. Alcuni accenni già si possono trovare nella no-fly list, totalmente anomala e inefficace, e negli innumerevoli quanto inutili progetti per categorizzare segretamente le persone a seconda del loro potenziale coefficiente di rischio terroristico. Gli stati di polizia sono intrinsecamente inefficienti, e non c'è ragione di assumere che quelli odierni possano essere più efficienti di quanto non sono.

Il timore non è tanto un governo orwelliano che crei intenzionalmente lo stato totalitario supremo, anche se potrebbe essere una tesi facilmente sostenibile visti i programmi statunitensi di sorveglianza telefonica, le intercettazioni illegali, il data mining su vastissima scala, un documento d'identità nazionale che nessuno vuole, e i vari abusi del Patriot Act. Il grosso guaio è che noi stessi stiamo creando tutto questo,

come sottoprodotto naturale della società dell'informazione. Stiamo costruendo l'infrastruttura informatica che permette a governi, multinazionali, organizzazioni criminali e anche a giovanissimi hacker di registrare tutto ciò che facciamo con estrema facilità e persino di cambiare i nostri voti elettorali. E continueremo a farlo a meno di non approvare leggi che regolamentino la creazione, l'utilizzo, la protezione, la rivendita e il trattamento dei dati personali. È proprio l'atteggiamento di considerare insignificante questo problema la causa del problema stesso.

Questo articolo è apparso nel numero di maggio di "Information Security" come seconda parte di un 'botta e risposta' con Marcus Ranum.

<http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1253144,00.html>

oppure <<http://tinyurl.com/2a8wvf>>

L'intervento di Marcus:

<http://www.ranum.com/security/computer_security/editorials/point-counterpoint/bigbrother.html>

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

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

Un video per addestrare i cittadini contro il terrorismo

Secondo un video di addestramento della Polizia dello stato del Michigan, i sette indizi di attività terroristica sono:

- Sorveglianza
- Deduzione
- Verifiche di sicurezza
- Acquisizione di scorte
- Persone sospette che appaiono 'fuori luogo'
- Verifiche/prove
- Disposizione di risorse o mettersi in posizione

Mi piacciono soprattutto le scene dove appaiono cittadini preoccupati che chiamano la polizia. Qualcuno vuol provare a indovinare la quantità di falsi allarmi che si arriverebbe ad avere se tutti iniziassero a fare telefonate di questo genere?

<<http://www.hanford.gov/oci/video/7signsofterrorism.wmv>>

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

News

Il Dipartimento per la Sicurezza Nazionale non ha più un grado di sicurezza cibernetica insufficiente; questa volta ha ottenuto un D. Il resto del governo degli Stati Uniti non

ha dato risultati molto buoni. Otto dei ventiquattro dipartimenti (compreso il Dipartimento della Difesa) hanno fallito. Nel complesso, il governo federale ha ricevuto un C- (migliore del D+ ottenuto l'anno scorso).

<http://news.zdnet.com/2100-1009_22-6175666.html>

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=13&articleId=9016363&intsrc=hm_topic>

oppure <<http://tinyurl.com/29rdav>>

Un'ennesima reazione esagerata a Boston in tema di antiterrorismo; questa volta si tratta di zaini lasciati sospesi sugli alberi vicino alle scuole. Tutte queste persone stanno forse cercando di essere stupide a tutti i costi? Il terrorismo è sempre stato difficile. Adesso basta appendere degli zaini agli alberi vicino alle scuole.

<<http://news.bostonherald.com/localRegional/view.bg?articleid=193808>>

Non lasciatevi terrorizzare!

<<http://www.schneier.com/essay-124.html>>

Negli Stati Uniti non esiste solo una watch list: ve ne sono molte.

<<http://www.wired.com/politics/onlinerights/news/2007/04/watchlist3>>

Frustrare i rapinatori di banca usando la gentilezza: pare funzioni molto bene. Di questo sistema di sicurezza approvo la capacità di fallire elegantemente in caso di un falso allarme. Non c'è nulla di male a essere gentilissimi con un cliente legittimo.

<<http://www.eyewitnessnewstv.com/global/story.asp?s=6365459&ClientType=Printable>>

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

Arrestare ragazzini: una tendenza inquietante. La polizia non dovrebbe farsi coinvolgere da questo genere di questioni. Le forze di polizia non sono addestrate per gestire ragazzini così giovani, e i ragazzini a loro volta non traggono alcun beneficio dall'essere sbattuti in galera dopo aver preso loro le impronte digitali.

<<http://welcome-to-pottersville.blogspot.com/2007/04/bob-herbert-6-year-olds-under-arrest.html>>

oppure <<http://tinyurl.com/25btu7>>

Un ulteriore sviluppo per l'Inghilterra così amante delle telecamere di sorveglianza: telecamere che "predicono" i reati. Lo si potrebbe considerare come un altro passo verso il psicoreato, ma a quanto mi è dato vedere, il sistema raccoglie semplicemente delle prove su individui ritenuti sospetti, tanto per non lasciare nulla al caso. Assumendo che le informazioni vengano cancellate subito dopo, è un metodo molto meno invasivo rispetto all'avvicinare fisicamente qualcuno a caccia di chissà quale psicoreato. I costi dei falsi allarmi sono minimi. Dubito che funzioni così bene come sostiene l'articolo, ma le cose potrebbero migliorare in 5-10 anni. Per esempio, oggi si stanno effettuando molte ricerche nell'ambito delle espressioni microfacciali per rilevare menzogne e altri pensieri. Questo è il genere di progresso tecnologico che va affrontato in termini di sicurezza, privacy e libertà.

<<http://www.timesonline.co.uk/tol/news/uk/crime/article1655200.ece>>

Esiste una tecnologia che sfrutta dati biometrici legati alla pressione dei tasti per stabilire se qualcun altro sta scrivendo la vostra password. Mi sembra una buona idea. Finché la tecnologia non viene perfezionata sarebbe preferibile non bloccare automaticamente gli utenti, e il rapporto tra falsi positivi e falsi negativi dovrebbe

essere adeguatamente regolato, ma se si riesce a far funzionare questa tecnologia nella maniera giusta, il risultato sarà un ulteriore livello di autenticazione "gratuito".

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

<http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article1667057.ece>

oppure <<http://tinyurl.com/23u7zg>>

Hacking ai danni delle Poste Statunitensi affinché la posta venga inviata in paesi "proibiti":

<<http://englishrussia.com/?p=334#more-334>>

Osservate il video di come le autorità australiane reagiscono quando qualcuno, a seconda che sia vestito come un turista americano o arabo, si mette a filmare il Sydney Harbor Bridge e un reattore nucleare. Riassunto: l'arabo viene intercettato nel giro di tre minuti in entrambi i casi, mentre al turista americano vengono date indicazioni su come entrare nella centrale nucleare. La morale per i terroristi è: vestitevi come un americano. (Tra parentesi, Lucas Heights è un reattore di ricerca: produce isotopi medici e vengono effettuate delle ricerche. Non viene generata energia).

<<http://youtube.com/watch?v=McB9tsabPn0>>

Secondo l'Internet Crime Complaint Center, e come è stato riportato nel "U.S. News and World Report", la frode nelle aste online e il mancato invio di oggetti regolarmente acquistati sono in assoluto i reati più comuni in Internet. Il furto di identità è quasi al fondo della classifica. "I federali avvertono che queste cifre non rappresentano un campione scientifico della quantità dei reati nella Rete. Fanno notare, per esempio, che il numero elevato di reclami per frode d'asta è dovuto in parte a eBay e ad altri giganti dell'e-commerce che offrono ai clienti link diretti al sito web IC3. Ed è difficile stabilire la grandezza del maggiore flagello del Web, la pedopornografia, basandosi soltanto sulle lamentele. Questa indagine è comunque un'utile fotografia della situazione, anche se ci dice ciò che già sappiamo: che l'Internet, come qualsiasi altro ambito della nostra vita, è piena di malintenzionati. State all'erta".

<http://www.usnews.com/usnews/news/badguys/070416/top_10_internet_crimes_of_2006.htm>

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

A seguito della sparatoria alla Virginia Tech University, Yale ha provato a vietare l'utilizzo di armi fasulle sul palcoscenico. Sarei tentato di fare una battuta sulla messinscena di sicurezza a teatro, ma qui siamo nella stupidità più assoluta. Non solo questa idea non rende nessuno più sicuro, ma non aiuta nemmeno a sentirsi più sicuri.

<<http://www.yaledailynews.com/articles/view/20843>>

L'ordine è stato rapidamente annullato, senza alcuna dimostrazione di buon senso:

<<http://yaledailynews.com/articles/view/20913>>

Un interessante sfogo di un poliziotto. Riassunto: la gente si serve dei poliziotti come sostegni nelle proprie dispute personali.

<<http://syracuse.craigslit.org/about/best/lax/151590579.html>>

Se la polizia mette in atto programmi per consentire ai comuni cittadini di segnalare sospetti terroristi, questo è il genere di risultato che si otterrà.

Un professore di inglese ha lasciato uno scatolone di carta da riciclare ed è stato segnalato per il suo aspetto mediorientale:

<<http://altnet.org/rights/50939/>>

Innescare ordigni esplosivi mediante i comandi a distanza solitamente utilizzati per aprire e chiudere le automobili:

<http://www.schneier.com/blog/archives/2007/04/triggering_bomb.html>

Un commento sulla sicurezza di Vista e sul monopolio di Microsoft:

<http://www.schneier.com/blog/archives/2007/04/commentary_on_v_1.html>

Richard Clarke sulla teoria dei terroristi come "cagnolini":

<http://www.nydailynews.com/opinions/2007/04/25/2007-04-25_put_bushs_puppy_dog_terror_theory_to_sle.html>

oppure <<http://tinyurl.com/2a9gqd>>

"Get Fuzzy" è una delle mie strisce di fumetti preferite. Una delle più recenti parlava di sicurezza.

<<http://www.comics.com//comics/getfuzzy/archive/getfuzzy-20070424.html>>

Se volete che la vostra tecnologia di sicurezza venga tenuta in considerazione per le prossime Olimpiadi di Londra del 2012, dovete essere uno dei maggiori sponsor dell'evento. Ho già sostenuto più volte come la sicurezza sia generalmente solo una parte di un contesto ben più vasto, ma qui siamo ai limiti del ridicolo.

<<http://www.itpro.co.uk/blogs/editorial-blogs/davey-winder/195108/no-medals-for-uk-government-over-london-olympics-security.thtml>>

oppure <<http://tinyurl.com/25c3z4>>

A East Belfast, degli scassinatori hanno dato un allarme bomba. I residenti hanno evacuato le loro case, e gli scassinatori hanno potuto svaligiare tranquillamente otto case vuote in tutto l'isolato. Ho già parlato di questo genere di cosa in passato: a volte è possibile che gli aggressori sfruttino le stesse procedure di sicurezza a loro vantaggio. Era il punto 4 del mio "procedimento a cinque punti" in "Beyond Fear" (pag. 14-15). Un documento di identità nazionale rende il furto di identità maggiormente redditizio; obbligare le persone affinché estraggano i loro computer portatili ai checkpoint di sicurezza in aeroporto contribuisce a rendere il furto di portatili sempre più diffuso. Morale: non è possibile concentrarsi solo su una delle tante minacce. Occorre esaminare la vasta gamma di minacce e fare attenzione a come la sicurezza implementata per una minaccia possa influire sulle altre.

<http://news.bbc.co.uk/1/hi/northern_ireland/6580873.stm>

Un brillante hack ai danni degli annunci Google:

<http://blog.washingtonpost.com/securityfix/2007/04/virus_writers_taint_google_ad.html>

oppure <<http://tinyurl.com/2q5o6d>>

È in atto un'azione legale di categoria contro TJX intentata da vari gruppi bancari che accusano TJX di non aver protetto le informazioni dei clienti con adeguate misure di sicurezza e per essersi comportata men che onestamente per quanto concerne la gestione dei dati. Questo caso potrebbe creare un nuovo precedente in ambito legale, e vale la pena osservarlo da vicino. (Faccio il tifo per il querelante).

<http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1252778,00.html>

oppure <<http://tinyurl.com/2g49sy>>

Ulteriori dettagli sul furto:

<http://online.wsj.com/article_email/SB117824446226991797-1MyQjAxMDE3NzA4NDIwNDQ0Wj.html>
oppure <<http://tinyurl.com/2wqamx>>
<<http://wifinetnews.com/archives/007604.html>>

I telefoni criptati sono un gran business in Italia come difesa contro le intercettazioni:
<http://www.nytimes.com/2007/04/30/business/worldbusiness/30encrypt.html?_r=1&oref=slogin>
oppure <<http://tinyurl.com/yrxrs9>>

Ecco un taser mascherato da assorbente interno. Verità o burla?
<http://www.americaninventorspot.com/security_system>

Un braccio di ferro di sicurezza fra ovidotti e falli delle anatre: una ricerca interessante dell'università di Yale:
<<http://www.nytimes.com/2007/05/01/science/01duck.html?ex=1335672000&en=4de6291bb177dfbf&ei=5090&partner=rssuserland&emc=rss>>
oppure <<http://tinyurl.com/28r7kc>>

Il Progetto Honey Pot intenta una causa legale di più di un miliardo di dollari contro gli spammer.
<http://www.projecthoneypot.org/5days_thursday.php>

Tutti sappiamo che i monitor CRT emettono moltissime radiazioni, e che qualcuno con l'attrezzatura adatta può leggerli a distanza. Marcus Kuhn dimostra come fare la stessa cosa con i monitor LCD.
<<http://www.newscientist.com/blog/technology/2007/04/seeing-through-walls.html>>
oppure <<http://tinyurl.com/ys28t8>>
Una ricerca simile, ma più datata:
<http://unix.be.eu.org/docs-free/tempest/optical_tempest.pdf>

La polizia britannica ha fatto saltare un rilevatore di pipistrelli credendo fosse una bomba. Per chi non lo sapesse, la A23 è la strada principale che unisce Londra e Brighton sulla costa meridionale.
<<http://www.theargus.co.uk/misc/print.php?artid=1372149>>
<http://www.theregister.co.uk/2007/05/04/bat_defences_pierced_by_bomb_panic/>
oppure <<http://tinyurl.com/ynoqq>>
<<http://news.bbc.co.uk/1/hi/england/sussex/6618737.stm>>
Adoro questo commento: "Stiamo lavorando su metodi per migliorare l'identificazione della nostra proprietà, così da evitare il ripetersi di un simile incidente". Potrei suggerire un cartello, tipo "Questa non è una bomba".

Un'altra striscia di xkcd sulla crittografia:
<<http://xkcd.com/c257.html>>

Un nuovo Trojan imita l'interfaccia di attivazione di Windows.
<<http://www.pcmag.com/article2/0,1895,2126214,00.asp>>
<http://www.symantec.com/security_response/writeup.jsp?docid=2007-042705-0108-99&tabid=2>
oppure <<http://tinyurl.com/yp2nlk>>

Divergenze fra USA e Canada sulle procedure di frontiera.

<http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20070427/border_plan_070427/20070427>

oppure <<http://tinyurl.com/24t48d>>

Due teenager hanno detonato una fialetta puzzolente su un treno di pendolari a Sydney e hanno scatenato una risposta antiterrorismo. La citazione migliore: " 'Avrebbe potuto essere terrificante. Vi trovate su un treno, d'un tratto sentite un forte botto, e la logica conclusione che ha tratto la gente era che si trattasse probabilmente di un attacco terroristico', ha dichiarato Owens ai giornalisti". Sono d'accordo sul fatto che sarebbe stata la conclusione a cui avrebbe pensato la gente, ma non che si tratti di una _logica_ conclusione.

<<http://www.stuff.co.nz/4047150a12.html>>

Un hacking bizzarro ai danni della lotteria:

<<http://www.smh.com.au/articles/2007/05/02/1177788228072.html>>

Consigli dell'Università della California su cosa fare in presenza di un tiratore nel campus:

<<http://www.ucpd.ucla.edu/ucpd/zippdf/2007/Active%20Shooter%20Safety%20Tips.pdf>>

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

"The Myth of the Superuser" [Il Mito del Superutente], uno studio di giurisprudenza molto interessante di Paul Ohm:

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372>

Ecco un riassunto in tre parti di Ohm sull'argomento:

<http://www.volokh.com/archives/archive_2007_04_08-2007_04_14.shtml#1176127892>

oppure <<http://tinyurl.com/ys9pwt>>

<http://volokh.com/archives/archive_2007_04_08-2007_04_14.shtml#1176212420>

oppure <<http://tinyurl.com/ys9pwt>>

<http://volokh.com/archives/archive_2007_04_08-2007_04_14.shtml#1176311368>

oppure <<http://tinyurl.com/29xyks>>

Chiarificazione di Ohm al post sul blog:

<http://www.schneier.com/blog/archives/2007/05/the_myth_of_the.html#c168413>

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

Il ricercatore afferma che questa è "la prima vulnerabilità di sicurezza SCADA che è possibile sfruttare da remoto", e credo che abbia ragione. In generale, ritengo che la minaccia di attacchi di tipo SCADA sia attualmente piuttosto gonfiata, esagerata. Ma diventerà molto più seria negli anni a venire.

<<http://www.physorg.com/news94025004.html>>

Le Flying Tigers, piccola squadra aerea dei guerriglieri Tamil a bassa tecnologia, battono la più numerosa e tecnologicamente sofisticata Air Force dello Sri Lanka.

<<http://www.theaustralian.news.com.au/story/0,20867,21672616-2703,00.html>>

oppure <<http://tinyurl.com/2oqm6c>>

<http://www.gulf-times.com/site/topics/article.asp?cu_no=2&item_no=146822&version=1&template_id=44&parent_id=24>

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

Ricordate la strana storia delle radio-trasmittenti nascoste nelle monete canadesi per spiare i cittadini americani? Un mucchio di scemenze.

<http://www.schneier.com/blog/archives/2007/05/poppy_coins_are.html>

A volte quello zaino dall'aspetto un po' strano _è davvero_ una bomba. Non molto spesso, ma dopo molto tempo è accaduto veramente. In ogni caso ritengo che non sia possibile risolvere la questione assumendo preventivamente che tutti gli oggetti strani siano dei potenziali ordigni. Esistono troppi oggetti strani a questo mondo.

<<http://www.cnn.com/2007/US/05/07/backpack.explodes.ap/index.html>>

Il post nel mio blog:

<http://www.schneier.com/blog/archives/2007/05/sometimes_it_is.html>

Singapore sta allestendo un centro di ricerca da 98 milioni di dollari per lo studio del calcolo quantico. Eccellente novità, ma che cosa diavolo significa questa dichiarazione? "Il genere di crittografia quantica che sviluppiamo qui è probabilmente la più sofisticata non presente in altri paesi, pertanto abbiamo in mente alcune soluzioni per renderla così sicura che non sarà più necessario fidarsi dei dispositivi acquistabili presso un produttore".

<<http://www.channelnewsasia.com/stories/singaporelocalnews/view/273831/1/.html>>

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

Il parcheggio più sicuro del mondo?

<http://en.wikipedia.org/wiki/Bold_Lane>

Rischi di sicurezza dei gadget sessuali: a me suonano come un sacco di idiozie, oppure si tratta di marketing molto furbo.

<<http://observer.guardian.co.uk/world/story/0,,2073474,00.html>>

"Il vostro PC è libero da virus? Infettatelo qui!": una campagna Google Adwords realmente esistente.

<<http://didierstevens.wordpress.com/2007/05/07/is-your-pc-virus-free-get-it-infected-here/>>

oppure <<http://tinyurl.com/25klcw>>

Il Beerbelly [lett. "pancia di birra"] si aggancia all'addome e sembra il classico "pancione da alcolista", dando la possibilità di introdurre birra e bevande alcoliche dove è proibito, ingannando la sorveglianza e anche quelle guardie che effettuano sommarie perquisizioni corporali.

<<http://thebeerbelly.com/>>

** *** *****

Saper individuare ciò che non quadra e i cittadini informatori

Per quanto riguarda il tema delle persone che notano e segnalano attività sospette, ho abbracciato due linee di pensiero che alcuni trovano contraddittorie. Da una parte sostengo che saremmo tutti più al sicuro se la polizia, le guardie, gli addetti alla sicurezza e altre figure analoghe ignorassero il profiling tradizionale e prestassero invece maggiore attenzione a persone che agiscono in maniera strana o sospetta. Dall'altra ho più volte sostenuto che se incoraggiassimo la gente a contattare le autorità

ogni volta che qualcuno nota qualcosa di strano, finiremmo col perdere un sacco di tempo a seguire falsi allarmi: stranieri i cui usi e costumi sono diversi dai nostri, persone non gradite ad altri, e così via.

La differenza fondamentale è l'esperienza. Le persone addestrate a notare ciò che non quadra svolgeranno un lavoro migliore di qualsiasi profiler, ma l'operato di persone che non hanno alcuna idea su che cosa cercare non sarà migliore dell'agire completamente a caso.

Ecco una storia che dimostra molto bene questo punto. La settimana scorsa uno studente al Rochester Institute of Technology è stato arrestato per possesso di due armi d'assalto illegali e 320 cartucce di munizioni nella sua stanza d'alloggio e nella sua auto:

"Le armi sono state scoperte per puro caso. Un impiegato del centro conferenze che ha prestato servizio militare stava camminando nei pressi della stanza d'alloggio di Hackenburg. La porta era chiusa a chiave, ma l'impiegato ha udito il suono fin troppo familiare di un'arma che veniva maneggiata, ha dichiarato il direttore del centro Bill Gunther".

Si noti come l'esperienza abbia giocato un ruolo fondamentale. L'"impiegato del centro conferenze" era in possesso delle nozioni necessarie per riconoscere il suono dell'arma e per capire che si trattava di un dettaglio che non quadrava nell'ambiente in cui era stato avvertito. Nessuno lo aveva istruito per individuare persone o cose sospette: la sua attenzione, acuita dall'addestramento militare, si è attivata automaticamente. Ha individuato un particolare che non quadrava e ha agito di conseguenza. Una persona qualunque non potrà agire allo stesso modo, perché non sarà in grado di individuare l'elemento sospetto quando si presenterà ai suoi sensi. Potrà segnalare degli imam perché stanno pregando, o un vicino che lo infastidisce, o altre persone a caso. Vedrà un professore di inglese mentre sta gettando della carta nei contenitori di raccolta differenziata e segnalerà che un uomo dall'aspetto mediorientale ha lasciato uno scatolone sul marciapiede.

Tutti abbiamo vissuto analoghe situazioni. Ognuno di noi possiede un certo grado di esperienza nelle materie più diverse, e di tanto in tanto ci capiterà di individuare qualcosa fuori posto anche se non sappiamo esattamente spiegare che cosa o perché. Un architetto potrebbe notarlo in una particolare struttura; un artista in un certo dipinto. Io potrei esaminare un sistema crittografico e sapere intuitivamente che presenta qualcosa di sbagliato, molto prima di individuare esattamente cosa e dove. Sono tutti esempi del riconoscere a livello subliminale che qualcosa non quadra, nei vari ambiti in cui abbiamo esperienza.

Buoni esperti di sicurezza possiedono la conoscenza, l'abilità e l'esperienza per agire in modo analogo in situazioni legate alla sicurezza. Questa è la differenza fra un buon esperto di sicurezza e un amatore.

Ecco perché il profiling basato sulla valutazione comportamentale è una buona idea, mentre il TIPS (Terrorist Information and Prevention System) non lo è. Ecco perché addestrare i camionisti affinché possano individuare situazioni sospette sulle autostrade è una buona idea, mentre un vago elenco di cose a cui prestare attenzione non lo è. Ecco perché un automobilista israeliano ha potuto riconoscere che un autostoppista era

in realtà un bombarolo suicida, mentre un automobilista americano probabilmente non se ne sarebbe neanche reso conto.

Non è per niente facile effettuare un addestramento per questo genere di cose (si è scritto molto a riguardo, però; si veda "Blink" di Malcolm Gladwell, che tratta la questione in dettaglio). Non si può imparare guardando un filmato di sette minuti. Ma più ci orientiamo su tutto ciò, e prima smetteremo di sprecare risorse di sicurezza aeroportuale in screener che confiscano pietre e globi di neve; meglio investire tali risorse in screener ben addestrati che si aggirano per l'aeroporto a caccia di persone e situazioni che non quadrano. Saremo tutti molto più al sicuro.

Ciò che "non quadra":

<<http://www.schneier.com/blog/archives/2005/07/profiling.html>>

L'episodio del RIT:

<<http://www.nj.com/news/ledger/morris/index.ssf?/base/news-2/1177047289122820.xml&coll=1>>

oppure <<http://tinyurl.com/228zm8>>

La sicurezza dei casinò e il principio JLDR ("Just Doesn't Look Right" - ossia "Non sembra proprio a posto"):

<<http://www.casinosurveillancenews.com/jldr.htm>>

Commenti:

<<http://www.cato-at-liberty.org/2007/04/26/id-be-ok-with-hinky-given-post-hoc-articulation/>>

oppure <<http://tinyurl.com/2b3bfz>>

Il post sul mio blog contiene molti più link ai vari dettagli trattati nell'articolo:

<http://www.schneier.com/blog/archives/2007/04/recognizing_hin_1.html>

*** **

Ancora sul REAL ID

Lo scorso marzo il Dipartimento per la Sicurezza Nazionale ha rilasciato il tanto atteso documento direttivo riguardante l'implementazione a livello nazionale del programma Real ID, come parte delle iniziative di sicurezza nazionale post-11 settembre. È forse assai indicativo che, malgrado l'opposizione bipartitica, Real ID fu sepolto in un disegno di legge "da approvare a tutti i costi" per lo stanziamento di fondi militari, poi approvato e reso legge senza alcun dibattito pubblico né udienze congressuali.

Il Dipartimento per la Sicurezza Nazionale sostiene che il concetto di Real ID non è un database di identificazione nazionale. Se è vero che il sistema non è un solo database in sé e per sé, è altrettanto vero che si tratta di uno stratagemma semantico: secondo il documento del Dipartimento per la Sicurezza Nazionale, Real ID sarà un ambiente di scambio dati collaborativo costituito da una serie di sistemi interconnessi gestiti e amministrati dai vari stati. In altre parole, per il Dipartimento di Sicurezza Nazionale non si tratta di un singolo database perché non è un solo sistema. Ma la funzionalità di

un singolo database rimane intatta sotto l'apparenza di un ambiente di scambio dati confederato.

Il documento del Dipartimento fa notare che "il beneficio principale di Real ID è quello di migliorare la sicurezza e ridurre la vulnerabilità di edifici federali, infrastrutture nucleari e aeree in caso di attacchi terroristici". Sappiamo adesso che i portelli di accesso alla cabina di pilotaggio erano la principale falla di sicurezza che ha contribuito alla tragedia dell'11 settembre, e che rinforzarli è stata una misura di sicurezza che era necessario istituire già da tempo per prevenire dirottamenti. Ma tutto questo solleva comunque un quesito interessante: vi sono davvero così tanti membri del pubblico americano che si trovano per caso a passare davanti a una centrale nucleare e a visitarla, al punto da farla diventare la ragione principale per creare un sistema di identificazione nazionale? E un tal numero di visitatori viene poi fatto entrare davvero in una centrale?

Il Dipartimento per la Sicurezza Nazionale propone una serie di linee guida in modo che il singolo individuo possa provare la propria identità e residenza quando fa domanda per una tessera Real ID. Ma se da un lato il Dipartimento riconosce che sia un compito monumentale quello di provare il domicilio o la residenza di un cittadino, dall'altro lascia ai singoli stati stabilire quali documenti siano da considerare come prova adeguata di residenza, e suggerisce persino che anche una bolletta o una dichiarazione bancaria possono venire considerati documenti appropriati. In tal caso, una persona potrebbe facilmente generare tutta una serie di documenti come prova di residenza. Basare Real ID su una documentazione così semplice da falsificare elimina una grossa parte di ciò che dovrebbe essere lo scopo stesso di Real ID.

Infine, e cosa forse più importante per gli americani, l'ultima sezione del documento su Real ID lungo 160 pagine merita una particolare attenzione. Con un cenno ai sostenitori dei diritti statali, il Dipartimento per la Sicurezza Nazionale dichiara che i vari stati, se vogliono, sono liberi di non partecipare al sistema Real ID, ma ogni documento di identificazione da loro emesso che non soddisferà i requisiti di Real ID dovrà essere contrassegnato come tale e in modo evidente, per esempio utilizzando "caratteri in grassetto" o un "design particolare", analogamente alle patenti di guida che molti stati emettono ai minori di 21 anni.

Insomma, nel suo stesso documento direttivo il Dipartimento per la Sicurezza Nazionale ha proposto di contrassegnare i cittadini sprovvisti di una tessera Real ID in maniera tale che faccia sapere a chiunque esamini il loro documento d'identità (ufficialmente emesso dallo stato a cui appartengono) che sono cittadini "diversi", magari potenzialmente pericolosi, secondo gli standard stabiliti dal governo federale. Questi cittadini verranno bollati, marchiati, ostracizzati, separati. Tutto questo in nome della protezione del suolo nazionale; non c'è da stupirsi se questo provvedimento si trova proprio alla fine del documento direttivo.

Un probabile risultato di questa separazione sociale proposta dal Dipartimento per la Sicurezza Nazionale è che le persone che presenteranno documenti di identità che non sono Real ID verranno automaticamente considerate sospette e magari soggette a ulteriori controlli o sorveglianza per confermare la propria innocenza in un bar, in un palazzo di uffici, all'aeroporto o durante un controllo stradale. Una situazione del genere creerebbe una nuova forma di scissione sociale, un tentativo di separare "noi" da "loro" nell'era dell'antiterrorismo e del nuovo normale, in cui un individuo viene presunto sospetto fino a quando non viene provato... ancor più sospetto.

Vengono alla mente altre due questioni legate al disegno globale di Real ID. Anzitutto, osservando il concetto generale di un database di identificazione nazionale, e considerando i controlli di sicurezza dei dati già esistenti in grandi sistemi distribuiti, viene da chiedersi quanto vulnerabile questo sistema-di-sistemi sarà alla perdita di dati o al furto di identità dovuti a impiegati senza scrupoli, tecnologie difettose, compromessi esterni o semplicemente all'errore umano, anche nelle migliori condizioni di sicurezza. E in secondo luogo, non esiste alcuna chiara direttiva in merito ai limiti di utilizzo del database Real ID. Altre iniziative di sicurezza nazionale, come il Patriot Act, sono state sfruttate e fatte valere (alcuni direbbero abusate) per scopi ben lontani da qualsiasi cosa che abbia a che vedere con la sicurezza nazionale. Quali garanzie abbiamo che non accadrà lo stesso con il programma Real ID?

Real ID, per come è stato attualmente proposto, fallirà per svariate ragioni. Da un punto di vista tecnico e di implementazione vi sono seri dubbi sulle capacità operative del programma sia per quanto riguarda la protezione delle informazioni personali dei cittadini, sia per quanto concerne la sua resistenza a eventuali raggiri da parte di aggressori. Da un punto di vista finanziario, il costo iniziale di 11 miliardi di dollari imposto dal governo federale ai vari stati è semplicemente eccessivo. E da un punto di vista sociologico, Real ID farà aumentare le possibilità di una più estesa sorveglianza personale e getterà le basi di una nuova forma di separazione sociale in nome della protezione del suolo nazionale.

È tempo di rivedere alcune delle decisioni in materia di sicurezza prese durante il forte impatto emotivo a seguito dell'11 settembre e stabilire se siano ancora delle buone idee per la sicurezza nazionale e per l'America. Dopotutto, se Real ID fosse un programma così ben congegnato, il Maine e 22 altri stati non si opporrebbero ad esso nelle loro legislature né rifiuterebbero il concetto di Real ID per tutta una serie di motivazioni. Invece è quel che stanno facendo.

E anche noi, come cittadini, dovremmo farlo. Che il dibattito abbia inizio.

La mia posizione su REAL-ID:

<<http://www.schneier.com/essay-160.html>>

Il documento direttivo del Dipartimento per la Sicurezza Nazionale:

<http://news.com.com/National+ID+card+a+disaster+in+the+making//Homeland+Security+offers+details+on+Real+ID/2100-1028_3-6163509.html>

oppure <<http://tinyurl.com/yroz6g>>

L'8 maggio ho deposto di fronte alla commissione giudiziaria del Senato in merito al REAL ID. La deposizione scritta e il filmato sono disponibili sul sito web.

<<http://judiciary.senate.gov/hearing.cfm?id=2746>>

<<http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050801899.html>>

oppure <<http://tinyurl.com/2y3d54>>

Questo articolo è stato scritto insieme a Richard Forno, ed è apparso su News.com:

<http://news.com.com/National+ID+card+a+disaster+in+the+making/2010-7348_3-6180835.html>

oppure <<http://tinyurl.com/2zk7b2>>

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

Schneier interverrà al Web Security Summit a Johannesburg, Sudafrica, il 23 maggio:
<<http://www.itweb.co.za/events/securitysummit/2007/default.asp>>

Schneier interverrà al Cisco Security 2007 a Oslo, Norvegia, il 31 maggio:
<<http://www.cisco.no/security2007>>

Schneier interverrà al Gartner IT Security Summit a Washington DC il 4 giugno:
<http://www.gartner.com/2_events/conferences/sec13.jsp>

Schneier interverrà alla ACLU Biennial Conference a Seattle il 14 giugno:
<http://action.aclu.org/site/Calendar/397839578?JServSessionIdr007=abyt2prxa2.app27a&view=Detail&id=102121&whence=http%3A%2F%2Faction.aclu.org%2Fsite%2FPageServer%3Fpagename%3Dspeakingengagements_ns>
oppure <<http://tinyurl.com/293mwo>>

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

Un campanello anti-spam del 1933

Ecco una bella descrizione di un campanello anti-spam del 1933. Per far suonare il campanello della porta, l'ospite doveva inserire una moneta da un decimo di dollaro in una fessura. Se il padrone di casa apprezzava la visita, restituiva il decimo, altrimenti la moneta sarebbe diventata il costo per aver disturbato il padrone di casa.

Questo tipo di soluzione è stata proposta anche per l'email: il mittente paga il destinatario (o un'altra entità del sistema) una piccolissima somma di denaro per ogni email inviata. Il denaro viene restituito se il messaggio è posta gradita (non spam), oppure trattenuto in caso di spam. L'effetto vuole essere di aumentare il costo di invio dello spam a un punto in cui diventa antieconomico.

Penso che sia il caso di confrontare i due sistemi (il campanello e la posta elettronica) per dimostrare perché non può funzionare nel caso dello spam.

Il sistema del campanello fallisce per tre motivi: la percentuale di visitatori importuni è talmente ridotta da rendere il sistema sostanzialmente inutile; un visitatore solitamente non ha sempre con sé degli spiccioli (rimediabile se il sistema viene adottato su vasta scala); è facilissimo aggirare il sistema bussando alla porta (non vale per i condomini).

Il sistema anti-spam non viene intaccato dai primi due problemi: lo spam rappresenta una grandissima percentuale del totale dei messaggi di posta elettronica, e un sistema di contabilità automatizzata facilita di gran lunga i meccanismi finanziari in gioco. Ma il sistema anti-spam è purtroppo molto facile da aggirare e da sabotare. E una volta impostato un sistema in cui circola del denaro, questo è praticamente un invito alla truffa.

Il sistema anti-spam non può funzionare perché gli spammer non inviano le email direttamente: possono appropriarsi di computer innocenti e inviarla da loro. Pertanto sono i proprietari dei computer innocenti, vittime a loro volta, che finiranno col

sostenere i costi dello spam. Si può mitigare tale rischio permettendo alle persone di stabilire un tetto massimo sui loro conti, ma il problema rimane ed è serio.

E i criminali possono sfruttare il sistema nella direzione opposta, introducendosi in computer innocenti e usandoli per inviare "spam" ai propri indirizzi email, riuscendo così a raccogliere denaro.

Cercare di imporre una qualche sanzione economica sulla posta indesiderata è una buona idea, ma non potrà funzionare fino a quando gli endpoint non saranno fidati. E attualmente siamo ben lungi da una cosa del genere.

<<http://blog.modernmechanix.com/2007/05/05/dime-put-in-slot-rings-doorbell/>>
oppure <<http://tinyurl.com/2723pl>>

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

La segretezza contribuisce a proteggere le informazioni personali?

La protezione delle informazioni personali è un problema di tipo economico, non di sicurezza. E il problema può essere facilmente spiegato: le organizzazioni a cui ci rimettiamo per proteggere le nostre informazioni personali non pagano le conseguenze nel caso tali informazioni vengano divulgate. Dall'altra parte, le persone danneggiate dall'esposizione delle loro informazioni non hanno le possibilità materiali per proteggerle.

In realtà qui i problemi sono due: le informazioni personali sono facili da rubare, e sono merce di valore una volta rubate. Non è possibile risolvere uno dei due problemi senza risolvere l'altro. Le soluzioni non sono semplici, e sono piuttosto sgradevoli.

Primo - sistemare il problema economico. Le compagnie di carte di credito guadagnano molti più soldi concedendo prestiti e semplificando l'utilizzo delle proprie carte da parte dei clienti, rispetto a quanti ne perdono a causa delle truffe. Non faranno nulla per migliorare la propria sicurezza fino a quando sarete voi (e non loro) a pagare le conseguenze dei furti di identità. Stesso discorso per banche e mediatori: finché siete voi a soffrire le conseguenze delle truffe ai vostri danni, essi non sono incentivati a risolvere il problema. E data broker come ChoicePoint sono ancora peggio: non subiscono alcun danno nel caso rivelino i vostri dati personali. Non avete alcuna relazione d'affari con loro, non potete nemmeno passare alla concorrenza in segno di disgusto.

La sicurezza delle carte di credito funziona così bene perché la Truth in Lending Law [Legge federale sulle dichiarazioni veritiere in materia di mutui e prestiti] del 1968 limita la responsabilità del consumatore a 50 dollari in caso di frode. Se le compagnie di carte di credito potessero scaricare sui clienti le perdite causate dalle frodi, investirebbero molto meno denaro per fermare tali perdite. Ma da quando il Congresso le ha obbligate a sostenere i costi delle frodi, le compagnie si sono inventate ogni genere di misure di sicurezza per prevenirle: verifica della transazione in tempo reale, sistemi esperti di controllo sul database delle transazioni, e così via. La lezione è chiara: occorre scaricare la responsabilità del rischio sulla parte, fra quelle coinvolte,

che più è in grado di attenuare tale rischio. L'effetto sarà quello di mettere in moto il motore dell'innovazione capitalistica. Una volta che il proteggerci dal furto di identità rientra nell'interesse economico delle istituzioni finanziarie, queste ci proteggeranno.

Secondo - occorre smettere di utilizzare informazioni personali per autenticare le persone. Si osservi come funzionano le carte di credito. Notare come il commesso di un negozio guardi a malapena la vostra firma, o come sia possibile utilizzare le carte di credito in Internet o da remoto, e non vi è nessuno dall'altra parte che possa controllare la vostra firma. L'industria delle carte di credito ha compreso da decenni che l'autenticazione delle persone ha un valore molto ridotto. Invece i loro sforzi si concentrano sull'autenticazione della transazione, e per questo sono molto più sicure.

Ciò non risolverà il problema del mettere al sicuro le nostre informazioni personali, ma ridurrà la minaccia in maniera consistente. Una volta che l'informazione stessa non ha più valore, la vostra unica preoccupazione sarà quella di proteggere i dati sensibili da eventuali curiosi invece che dai truffatori, più frequenti e molto più incentivati economicamente.

Terzo - sistemare l'altro problema economico: le organizzazioni che espongono le nostre informazioni personali non risentono delle conseguenze di tale scorrettezza. È necessaria un'estesa legge sulla privacy che garantisca agli individui il possesso delle loro proprie informazioni e permetta loro di agire per vie legali contro le organizzazioni che non si curano di proteggerli adeguatamente.

"Password" come numeri di carta di credito e il cognome da nubile della propria madre erano solite funzionare, ma ormai abbiamo abbandonato per sempre quel mondo in cui la nostra privacy viene salvaguardata dalla segretezza dei nostri dati personali e dalla difficoltà di accedere a essi da parte di terzi. Occorre lasciarci alle spalle i sistemi di sicurezza basati sulla segretezza e sulla difficoltà, e costruire una rete di protezioni legali che agiscano là dove il progresso tecnologico ha fallito, lasciandoci esposti.

Questo articolo è originariamente apparso sul numero di gennaio di "Information Security", come seconda parte di un 'botta e risposta' con Marcus Ranum.

<http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1238789,00.html>

oppure <<http://tinyurl.com/2h5y5u>>

L'intervento di Marcus:

<http://www.ranum.com/security/computer_security/editorials/point-counterpoint/personal_info.html>

oppure <<http://tinyurl.com/27e2gj>>

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

Vale la pena effettuare dei test di penetrazione?

Vi sono esperti di sicurezza che insistono nell'affermare che i test di penetrazione sono fondamentali per la sicurezza di rete, e che non ci sono speranze di essere al sicuro a meno che tali test non vengano effettuati con regolarità. Poi vi sono altri esperti di

sicurezza di parere opposto che vi dicono che i test di penetrazione sono soltanto uno spreco di tempo e risorse e che tanto vale buttare direttamente i soldi dalla finestra. Entrambe queste scuole di pensiero sbagliano. La realtà dei test di penetrazione è molto più complicata e sfumata.

‘Test di penetrazione’ è un’espressione molto ampia. Può voler dire penetrare in una rete per dimostrare che è possibile farlo. Può voler dire tentare di penetrare in una rete per documentarne le vulnerabilità. Può comportare un attacco remoto, la penetrazione fisica in un centro dati o attacchi di ingegneria sociale. Può servirsi di strumenti (commerciali o proprietari) di rilevazione delle vulnerabilità, o affidarsi ad abili hacker ‘white-hat’. Può limitarsi a verificare i numeri di versione del software e i livelli di patch installate, ed effettuare inferenze sulle vulnerabilità.

In ogni caso il test è costoso, e il risultato sarà un lungo, esteso rapporto una volta che il test sarà ultimato.

E questo è il vero problema. In realtà non volete un lungo, esteso rapporto che documenta tutte le ragioni del perché la vostra rete è insicura. Non avete un budget sufficiente per sistemare tutte le falle, e quindi quel corposo documento rimarrà lì finché non verrà usato per mettere in cattiva luce qualcuno. O, ancora peggio, verrà scoperto nel corso di una causa legale. Volete davvero che l’avvocato dell’accusa vi chieda di spiegare perché avete pagato per documentare le falle di sicurezza della vostra rete e poi non le avete sistemate? Probabilmente la cosa più sicura da fare con quel rapporto, dopo averlo letto, è distruggerlo.

Con una quantità sufficiente di tempo e denaro, un test di penetrazione troverà qualche vulnerabilità; non serve a nulla darne prova documentata. E se non potete o non avete intenzione di sistemare tutte le vulnerabilità che sono venute alla luce, non serve a nulla scovarle. Ma esiste un modo utile di effettuare un test di penetrazione. Per anni ho sostenuto che la sicurezza consiste in protezione, rilevamento e risposta, e vi occorrono tutti e tre i componenti per avere una buona sicurezza. Prima di fare un buon lavoro con uno qualsiasi di tali componenti, è necessario valutare la vostra sicurezza. E, se ben fatto, il test di penetrazione è un elemento chiave di una verifica di sicurezza.

Preferisco restringere il test di penetrazione alle vulnerabilità critiche che sono più frequentemente oggetto di exploit, come quelle riportate dal SANS nella classifica delle Top 20. Se il vostro sistema presenta una di queste vulnerabilità, è proprio il caso di porvi rimedio.

A ben pensarci, il test di penetrazione è una faccenda un po’ strana. Vi sono delle procedure analoghe in altri ambiti di sicurezza? Certo, i militari effettuano continuamente prove di questo genere, ma in ambito economico? Paghiamo degli scassinatori affinché cerchino di penetrare nei nostri magazzini? Cerchiamo di commettere frodi ai nostri stessi danni? Certamente no.

Il test di penetrazione è diventato un grosso business perché i vari sistemi sono molto complicati e poco conosciuti. Sappiamo molto di scassinatori, rapimenti, frodi, ma non sappiamo un granché in materia di criminali cibernetici. Non sappiamo esattamente che cosa è pericoloso oggi e che cosa può esserlo domani. Pertanto assumiamo degli esperti in test di penetrazione credendo che possano spiegarcelo.

Vi sono due motivi che possono indurvi a condurre un test di penetrazione. Uno - volete sapere se una certa vulnerabilità è davvero presente perché siete intenzionati a ripararla nel caso lo sia. Due - vi serve un rapporto lungo e corposo che possa convincere il vostro capo a investire più soldi. Se la vostra situazione è diversa da queste, vi farò risparmiare molto denaro offrendovi questo test di penetrazione gratuito: siete vulnerabili.

Ora usate questa informazione per fare qualcosa di utile.

Questo articolo è originariamente apparso sul numero di marzo di "Information Security", come seconda parte di un 'botta e risposta' con Marcus Ranum.

<http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1245619,00.html>

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

L'intervento di Marcus:

<http://www.ranum.com/security/computer_security/editorials/point-counterpoint/pentesting.html>

oppure <<http://tinyurl.com/23epfv>>

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

Abbiamo veramente bisogno di un'industria della sicurezza?

La settimana scorsa ho partecipato alla conferenza Infosecurity Europe a Londra. Come è accaduto alla RSA Conference a febbraio, l'area delle esposizioni era strapiena di aziende che si occupano di reti, di informatica e di information security. Come faccio spesso, mi sono fermato a riflettere su che cosa significa per l'industria IT che esistano migliaia di prodotti di sicurezza dedicati sul mercato: alcuni di buona qualità, molti scadenti, molti altri persino difficili da descrivere. Perché i prodotti e i servizi IT non sono sicuri per natura, e cosa significherebbe per l'industria se lo fossero?

Ho accennato alla questione in un'intervista con Silicon.com, e l'articolo che è stato pubblicato in seguito pare abbia causato una certa animazione. Piuttosto che lasciare tutti quanti nel dubbio in merito a che cosa intendessi dire veramente, ho pensato di fornire una spiegazione più chiara.

La ragione principale dell'esistenza dell'industria IT della sicurezza è che i prodotti e i servizi IT non sono intrinsecamente e naturalmente sicuri. Se i computer fossero già protetti contro i virus, non vi sarebbe il bisogno di prodotti antivirus. Se non si potesse sfruttare del traffico di rete malevolo per attaccare i computer, nessuno si preoccuperebbe di acquistare un firewall. Se non vi fossero più i buffer overflow, nessuno sarebbe costretto a comprare i prodotti necessari a proteggersi contro i loro effetti. Se i prodotti IT che acquistiamo fossero sicuri fin dal principio, non dovremmo spendere miliardi di dollari ogni anno per renderli sicuri.

La sicurezza 'aftermarket' è in realtà un sistema molto inefficiente di spendere il nostro denaro per la sicurezza. Certo, può compensare la presenza di prodotti IT non sicuri, ma non aiuta a migliorarne la sicurezza. In più, finché la sicurezza IT rimane

un'industria distinta, vi saranno aziende che faranno soldi sfruttando l'insicurezza, ovvero compagnie che perderanno denaro nel caso Internet diventasse più sicura.

Se si integra la sicurezza nei prodotti sottostanti, le compagnie che commercializzano tali prodotti saranno incentivate a investire da subito nella sicurezza, così da non spendere altro denaro per evitare i problemi in un secondo momento. I loro profitti aumenterebbero di pari passo al livello generale di sicurezza in Internet. Inizialmente continueremmo a spendere ogni anno in sicurezza una quantità di denaro paragonabile (in pratiche di sviluppo sicuro, nella sicurezza incorporata, e così via), ma parte di quel denaro verrebbe destinata al miglioramento della qualità dei prodotti IT che stiamo comprando, e ridurrebbe le spese per la sicurezza negli anni a venire.

So bene che si tratta di una visione utopica che probabilmente non vedrò mai in vita mia, ma il mercato dei servizi IT ci sta spingendo in questa direzione. Con il progressivo trasformarsi dell'IT in una utilità pubblica, gli utenti finiranno con l'acquistare molti più servizi che non prodotti. E, per natura, i servizi si concentrano più sui risultati che sulle tecnologie. Chi usufruisce di un servizio, che sia un privato o una multinazionale, è sempre meno interessato alle specifiche delle tecnologie di sicurezza impiegate, e si aspetta sempre più che il proprio IT sia integralmente sicuro.

Otto anni fa ho fondato Counterpane Internet Security sul principio che gli utenti finali (grosse entità aziendali, in questo caso) non vogliono affatto dover avere a che fare con la sicurezza di rete. Vogliono far volare aerei, produrre farmaci o realizzare qualsiasi cosa sia il loro core business. Non vogliono pagare degli esperti per controllare la propria sicurezza di rete, ma saranno ben lieti di darla in appalto a una compagnia che può svolgere il lavoro per loro. Noi di Counterpane abbiamo fornito una serie di servizi che hanno sollevato il cliente dall'onere della sicurezza giornaliera: monitoraggio di sicurezza, security-device management, incident response. La sicurezza era qualcosa che i nostri clienti acquistavano, ma ciò che compravano erano risultati, non dettagli tecnici.

L'anno scorso, BT ha acquisito Counterpane, incorporando ancor più i servizi di sicurezza di rete nell'infrastruttura IT. I clienti di BT non vogliono occuparsi per niente di gestione della rete, vogliono che questa, semplicemente, funzioni. Vogliono che Internet sia come la rete telefonica, o elettrica, o idrica; vogliono che sia un'utilità. Per questi clienti, la sicurezza non è nemmeno qualcosa che acquistano: è una piccola parte di un ben più vasto accordo di servizi IT. È la stessa ragione per cui IBM ha acquisito ISS: per essere in grado di avere una soluzione più integrata da fornire alla propria clientela.

Questa è la direzione intrapresa dall'industria IT, e quando arriverà in fondo, conferenze come Infosec e RSA non avranno ragion d'essere. Non scompariranno, ma diventeranno conferenze di industria, non di utenti. Se volete misurare il progresso, osservate il campione demografico presente a queste conferenze. Uno spostamento verso un tipo di partecipanti orientati all'infrastruttura è una misura di successo.

Ovviamente i prodotti di sicurezza non scompariranno, o meglio, non farò in tempo a vederli scomparire. Continueranno a esserci firewall, antivirus e tutto quanto. Continueranno a esserci nuove aziende che svilupperanno tecnologie di sicurezza brillanti e innovative. Ma l'utente finale non sarà interessato ad esse. Saranno incorporate all'interno di servizi venduti da grandi compagnie IT in outsourcing come

BT, EDS e IBM, o da Internet Provider come Earthlink e Comcast. O saranno una voce da spuntare da qualche parte nel core switch.

La sicurezza IT sta diventando sempre più difficile (la causa principale è la complessità sempre maggiore) e il bisogno di prodotti di sicurezza aftermarket non svanirà tanto presto. Ma non si capisce assolutamente perché gli utenti dovrebbero sapere che cosa sia un sistema anti-intrusione con analisi di protocollo stateful, né perché sia utile al rilevamento di attacchi SQL injection. L'intera industria IT della sicurezza è un accidente, un prodotto di come si è sviluppata l'industria informatica. Con lo sfumare dell'IT sempre più verso lo sfondo e con la sua trasformazione in un servizio di utilità come tanti altri, gli utenti si aspetteranno semplicemente che funzioni e basta, e i dettagli sul suo funzionamento non avranno importanza.

<<http://software.silicon.com/security/0,39024655,39166892,00.htm>>
<<http://www.techworld.com/security/blogs/index.cfm?blogid=1&entryid=467>>
<http://techdigest.tv/2007/04/security_guru_q.html>
<<http://www.itbusinessedge.com/blogs/top/?p=114>>

Complessità e sicurezza:

<<http://www.schneier.com/crypto-gram-0003.html#8>>

Commenti all'articolo:

<<http://www.networkworld.com/community/?q=node/14813>>
<<http://it.slashdot.org/it/07/05/03/1936237.shtml>>
<<http://matt-that.com/?p=5>>

Questo articolo è originariamente apparso su Wired.

<http://www.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0503>

oppure <<http://tinyurl.com/23b3av>>

** ** ** * * * * *

Commenti dei lettori

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

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

** ** ** * * * * *

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia. I numeri arretrati sono disponibili all'indirizzo

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

Per iscriversi, cancellare l'iscrizione o cambiare il proprio indirizzo a cui recapitare la newsletter, visitate sempre <<http://www.schneier.com/crypto-gram.html>>

La versione italiana è curata da Communication Valley SpA

<<http://www.communicationvalley.it/>>

Per iscriversi o cancellarsi andare all'indirizzo <<http://www.cryptogram.it/>>

I numeri arretrati sono disponibili all'indirizzo <<http://www.cryptogram.it/>>

Per informazioni <crypto-gram@communicationvalley.it>

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

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

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla 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) 2007 - Bruce Schneier.