

La ritorsione è un altro fatto di cui preoccuparsi. Il Brasile ora prende le impronte degli americani in visita nel paese, e altre nazioni ne seguiranno presto l'esempio. In tutto il mondo, i governi totalitari si serviranno del nostro regime di tracciamento delle impronte digitali per giustificarsi quando prenderanno le impronte ai cittadini americani che attraversano le loro frontiere. Ciò significa che le vostre impronte finiranno registrate insieme a quelle di ogni mediocre dittatorucolo, dalla Sierra Leone fino all'Uzbekistan. Tom Ridge ha già promesso di condividere queste informazioni di sicurezza con altre nazioni.

La sicurezza è un fatto di compensazioni. Quando si decide se implementare o meno una misura di sicurezza, è necessario fare un bilancio dei costi e dei benefici. Un sistema di presa di impronte digitali su vasta scala è qualcosa che non va ad aggiungere granché alla nostra sicurezza contro il terrorismo; in più costa un enorme quantità di denaro che potrebbe essere speso meglio in altri modi. Distribuire i fondi per compilare, condividere e rendere esecutiva una watch list dei terroristi sarebbe un investimento per la sicurezza di molto migliore. Come "utente" della sicurezza, mi sento raggirato.

La sicurezza dell'America deriva dalle nostre libertà e dai nostri privilegi. Per più di due secoli abbiamo mantenuto un delicato equilibrio fra libertà e possibilità di reato. Abbiamo coscientemente stabilito delle leggi che ostacolano le indagini di polizia, perché sappiamo di essere più tutelati grazie ad esse. Sappiamo che le leggi che regolamentano le intercettazioni, le perquisizioni, i sequestri, e gli interrogatori ci mantengono più sicuri, anche se rendono più difficile condannare i criminali.

Il sistema di governo statunitense possiede una regola basilare che non è scritta da nessuna parte: al governo occorre affidare soltanto un potere limitato, e per scopi ben precisi e definiti, poiché è certo che si abuserà di tale potere governativo. Abbiamo già visto affidati al governo i poteri del US-PATRIOT Act, originariamente pensati per combattere il terrorismo, e poi utilizzati contro reati comuni. Permettere ad un governo di creare l'infrastruttura per raccogliere le informazioni biometriche di più individui possibili non è un potere che dovremmo garantire così a cuor leggero. Si tratta di qualcosa che ci saremmo aspettati nella vecchia Germania Est, in Iraq o nell'Unione Sovietica. In tutti questi paesi un maggiore controllo nelle mani del governo ha sempre significato minor sicurezza per i cittadini, e le conseguenze negli Stati Uniti non sarebbero diverse. È pessima igiene civica costruire un'infrastruttura che può venire utilizzata per agevolare uno stato di polizia.

Una versione di questo intervento è comparsa originariamente su Newsday.

<<http://www.newsday.com/news/opinion/ny-vpsch143625202jan14,0,1880923.story>> oppure <<http://tinyurl.com/2yy7t>>

La pagina Web dell'Ufficio della Sicurezza Nazionale contenente il programma:

<http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0333.xml>

Articoli correlati:

<<http://www.washtimes.com/national/20031201-115121-4339r.htm>>

<<http://www.washtimes.com/national/20031027-112510-5818r.htm>>

<<http://www.nytimes.com/reuters/news/news-security-usa-visas.html>>

<http://gcn.com/vol1_no1/daily-updates/24536-1.html>

<<http://www.sunspot.net/news/custom/attack/bal-airport0106,0,42711.story>>

<<http://www.cnn.com/2004/US/01/04/visit.program/>>

<<http://www.nytimes.com/2004/01/05/national/05CND-SECU.html>>

<http://www.ilw.com/lawyers/immigdaily/doj_news/2004,0106-hutchinson.shtm>

<<http://www.theage.com.au/articles/2004/01/06/1073268031785.html>>

<<http://www.thestar.co.za/index.php?fSectionId=132&fArticleId=318749>>

<<http://www.ilw.com/lawyers/articles/2003,1231-krikorian.shtm>>

Opinioni:

<<http://news.mysanantonio.com/story.cfm?xla=saen&xlb=1020&xlc=1074396>>

Pare che tutti questi non siano stati altro che falsi allarmi. In alcuni casi si è trattato di uno scambio di identità. Per esempio, uno dei "terroristi" su un volo dell'Air France era solo un bambino il cui nome era identico a quello di un leader terrorista; in un altro caso si trattava di un agente assicurativo del Galles. In altre circostanze si è un po' esagerato nel presumere: il volo 223 della British Airways è stato fatto ritardare una volta e cancellato due volte in tre giorni consecutivi, presumibilmente perché quel numero di volo era saltato fuori in qualche comunicazione intercettata. Come risposta al pubblico imbarazzo derivato da tali falsi allarmi, il governo sta pian piano divulgando informazioni riguardo a una certa persona che non si è presentata sul suo volo, e due individui dai tratti non arabi che forse potevano essere in possesso di bombe. Ma questi sembrano essere più che altro dei tentativi per salvarsi la faccia, non certo la prova "molto credibile" promessa dal governo.

La sicurezza implica una compensazione: un bilancio dei costi e dei benefici. È evidente che cancellare ogni volo, ora e per sempre, eliminerebbe la minaccia e i pericoli del viaggiare in aereo. Ma nessuno mai suggerirebbe un provvedimento simile, perché il bilancio è troppo oneroso. Cancellare dei voli qua e là sembra un buon compromesso, perché le conseguenze del lasciarsi sfuggire una minaccia reale sono assai gravi. Ma continuare a lanciare falsi allarmi comporta anche dei seri problemi di sicurezza. I falsi allarmi costano molto -- in termini economici, di tempo, e della privacy dei passeggeri coinvolti -- e dimostrano che le "minacce credibili" non sono credibili affatto. Come il ragazzo che gridò "al lupo", tutti, dal personale di sicurezza degli aeroporti ai governi stranieri, cesseranno di prendere sul serio questi avvertimenti. Ci stiamo affidando ai nostri alleati per la sicurezza dei voli internazionali: dimostrare che non siamo capaci di distinguere fra terroristi e bambini non è certo il miglior modo per infondere sicurezza.

Raccogliere informazioni di intelligence è un problema difficile. Si inizia con una massa di dati grezzi: persone che frequentano scuole di volo, incontri segreti in paesi esteri, suggerimenti dai governi di altre nazioni, registri di immigrazione, contratti d'affitto, trascrizioni di telefonate, estratti conto di carte di credito. Analizzare questi dati e ricavarne le corrette conclusioni: questo è il lavoro di intelligence. Sembra semplice, visto col senno di poi, ma assai complesso prima dei fatti, poiché la maggior parte dei dati sono irrilevanti e parecchi indizi sono falsi. I dati più utili e cruciali sono tracce casuali in mezzo a migliaia di altre tracce casuali, delle quali la stragrande maggioranza si rivelano essere falsi, fuorvianti o irrilevanti.

Nei mesi e negli anni successivi all'11 settembre, il governo degli Stati Uniti ha cercato di affrontare il problema richiedendo (e in gran parte ottenendo) ancora più informazioni. Durante il weekend di Capodanno, ad esempio, gli agenti federali hanno raccolto i nomi di 260.000 persone che risiedevano negli alberghi di Las Vegas. Questa enorme raccolta di dati è costosa, e manca completamente il bersaglio. Il problema non risiede nell'ottenere informazioni, ma nel decidere quali dati val la pena di analizzare per poi interpretarli. Viene accumulata una tale quantità di informazioni che le organizzazioni di intelligence non potranno mai analizzare nella loro totalità. Stabilire che cosa osservare può rivelarsi un compito impossibile, ecco perché sostanziali quantità di dati finiscono col non venire lette né esaminate. La raccolta di informazioni è semplice; l'analisi è difficile.

Molti pensano che il problema dell'analisi possa essere risolto dandolo in pasto ad un maggior numero di computer, ma non è questo il caso. I computer sono stupidi. Possono trovare delle ricorrenze ovvie, ma non saranno in grado di scoprire il prossimo attacco terroristico. Al-Qaida è furbo, ed eccelle nel compiere le azioni più inattese. Osama Bin Laden e le sue truppe faranno sicuramente degli errori, ma per un computer, il loro comportamento "sospetto" non sarà molto diverso dal comportamento sospetto di milioni di altre oneste persone. Trovare il vero complotto in mezzo a un mare di falsi indizi richiede un'intelligenza umana.

Un numero ancora maggiore di dati può persino risultare controproducente. In presenza di più informazioni, si finisce con l'aver lo stesso numero di "aghi" ma un "pagliaio" sempre più grande in cui cercarli. Negli scorsi Anni Ottanta e ancor prima, la polizia della Germania Est raccolse una quantità immane di dati su 4 milioni di cittadini tedeschi dell'Est, circa un quarto dell'intera popolazione. Tuttavia non sono stati in grado di prevedere la pacifica deposizione del

Da: russfink@SAFe-mail.net

Oggetto: Blaster e il black-out del 14 agosto

Ho appena letto il suo articolo, ed avrei un'ulteriore questione da sollevare, che varrebbe la pena approfondire.

L'ipotesi alla base dell'articolo è che quell'imponente black-out sia stato indirettamente favorito dal non funzionamento dei sistemi d'allarme, causato da MS Blast, e che questi sistemi d'allarme non funzionanti abbiano permesso ad una serie di malfunzionamenti delle apparecchiature e di condizioni avverse di non essere rilevati dagli operatori della centrale. Dato che i tecnici non erano a conoscenza di tali avverse condizioni, si sono ritrovati con le mani legate e ne è risultato quell'enorme disastro dovuto a guasti in cascata.

La mia domanda è: in circostanze normali, assumendo che i sistemi di allarme siano operativi, quanto spesso di norma si verificano malfunzionamenti delle apparecchiature o condizioni avverse che vengono segnalate per tempo dai sistemi di allarme, in modo che i tecnici possano intervenire e quindi evitare disastri in cascata di grandi proporzioni?

Ho l'impressione che se i computer avessero funzionato quel giorno, i tecnici avrebbero saputo dello stato di allarme, e avrebbero potuto evitare la catastrofe. Mi interessa solo conoscere il livello di probabilità con cui si presentano queste condizioni di allarme nella quotidianità.

In altre parole, quanti incidenti accadono dei quali noi, l'opinione pubblica, non veniamo nemmeno a conoscenza?

Se conoscessimo quest'ordine di probabilità, potremmo trattare i relativi rischi di worm che portano a black-out di vasta scala come una funzione della probabilità di condizioni d'allarme e di interconnessione fra sistemi di allarme e Internet.

Non mi aspetto che qualcuno si faccia avanti per sostenere la sua ipotesi, dato che equivarrebbe ad un'ammissione di fallimento da parte dello staff responsabile della sicurezza, e possibile terreno per eventuali licenziamenti. Magari salterà fuori qualche voce isolata più avanti.

Da: Andrew Odlyzko <odlyzko@dtc.umn.edu>

Oggetto: Il voto computerizzato ed elettronico

La cabina elettorale offre sì un certo livello di protezione contro corruzione e costrizioni, ma solo se riusciamo a far in modo che al suo interno non vengano usati dei cellulari con fotocamera!

Da: Fred Heutte <phred@sunlightdata.com>

Oggetto: Il voto computerizzato ed elettronico

La ringrazio per le sue convincenti argomentazioni sulla sicurezza del procedimento di voto. Mi trovo in quasi totale accordo e sono stato uno dei primi firmatari della petizione di David Dill. Sono poi coinvolto professionalmente per quanto riguarda le informazioni degli elettori -- intendo dire, dal punto di vista della campagna elettorale, con i registri elettorali, non direttamente con le apparecchiature per il voto -- ma mi trovo abbastanza vicino al processo dei conteggi per vedere come funziona a tutti gli effetti.

Mi riservo di essere in leggero disaccordo su un punto. La pratica dello scrutinio a distanza è piuttosto sicura se si tiene conto dell'approccio complessivo e se si valutano i rischi in ogni fase del processo. Finché si adottano delle ragionevoli precauzioni quali il controllo della firma,

sarebbe complicato e costoso alterare in maniera significativa i risultati del voto per corrispondenza.

Per esempio, nell'Oregon, i voti vengono rispediti in una busta interna di sicurezza che viene sigillata dall'elettore. La busta esterna presenta sul retro una zona dove firmare. La firma dell'elettore viene confrontata con quella presente negli archivi del seggio elettorale. Le contee più estese effettuano un confronto digitalizzato, seguito da un confronto manuale con un campione casuale stratificato (per convalidare i risultati della macchina costantemente), e infine da una determinazione definitiva nel caso vi siano dei confronti incerti.

Certo, è possibile falsificare una firma. Tuttavia, questo procedimento di autenticazione farebbe aumentare di molto il costo di votazioni per corrispondenza truccate, con il silenzio-assenso del votante. D'altro canto, con lo scrutinio a distanza l'interferenza o la costrizione richiederebbero costi molto più elevati per i viaggi (almeno) che non il farlo in un contesto di seggio elettorale vero e proprio, se si vuole ottenere un qualche cambiamento nei risultati finali.

È vero che vi sono degli scrutatori nei vari distretti elettorali, cosa che non avviene con il voto a distanza. Ma consideriamo questo: i contenitori delle schede, che sono spesso consegnati da impiegati temporanei del seggio di zona all'ufficio elettorale, vengono rubati di tanto in tanto, ma le schede inviate per posta sono maneggiate insieme all'enorme flusso di tutta la corrispondenza da impiegati le cui buste paga e pensioni sono sempre in gioco. Il livello relativamente basso di frodi all'interno del sistema postale ne testimonia la relativa sicurezza, e i luoghi ove vengono accumulate le schede per essere poi consegnate all'ufficio elettorale sono in genere su suolo pubblico e possono essere controllati da osservatori esterni, se necessario.

In Oregon si sono tenute alcune elezioni con il 100% dei "voti per corrispondenza" sin dal 1996, e tutte le elezioni dal 1999. Finora non è emersa alcuna prova verificabile di una frode elettorale, malgrado i numerosi controlli ed alcune previsioni da parte di chi voleva politicamente tirare acqua al proprio mulino, secondo cui saremmo stati sommersi da un'ondata di rettifiche elettorali.

La realtà delle cose è che il sistema in uso in Oregon, basato su principi di sicurezza legati al buon senso, ha dimostrato di essere solido. L'inconveniente più duraturo è stata la necessità da parte di alcune contee di far utilizzare ai propri elettori delle schede perforate, a causa delle antiquate apparecchiature per i conteggi. Ma se questo è da un lato un problema di integrità di voto -- dato che le statistiche statali mostrano una netta diminuzione di voti e un maggior numero di voti nulli per quanto concerne le schede perforate, se comparato ai voti con sistema mark-sense -- non è certo un problema di sicurezza di per sé. Grazie ai fondi stanziati dal Help America Vote Act (HAVA) per modernizzare i sistemi di conteggio dei voti, le schede perforate in Oregon sono rimaste in una sola contea, e cadranno in disuso dopo il 2004.

I voti con il sistema mark-sense ("compilare le zone ovali") abbiamo lavorato bene, ed abbiamo tassi minimi di errore di conteggio dei voti, sia in eccesso che in difetto, malgrado la mancanza di un controllo automatizzato, che è possibile in quei seggi con un sistema di voto ben realizzato. Ciò lascia intendere che un progetto visuale coerente e l'approccio amichevole del voto domestico usando carta e matita/penna si rivela essere un metodo molto affidabile e sicuro. Se si aggiunge un'apparecchiatura per il conteggio automatico, abbiamo inoltre il vantaggio di conteggi iniziali assai velocizzati.

L'aumento della partecipazione degli elettori nell'Oregon dall'avvento del voto per corrispondenza -- dai 10 ai 30 punti percentuali sopra le medie nazionali, a seconda del tipo di elezioni -- porta all'unica altra problematica, ovvero i rallentati conteggi automatici la notte delle elezioni dopo la chiusura dei seggi, a causa dell'ultima ondata di schede recapitate nei punti di consegna sparsi per tutto lo stato. Infatti nell'Oregon non si usa tanto il "voto per corrispondenza", quanto il voto domestico, con una scheda cartacea che può essere spedita o

lasciata in un qualsiasi punto di consegna statale, fra cui gli uffici elettorali di contea, parecchie scuole e biblioteche, centri commerciali, piazze cittadine, ecc.

L'enorme vantaggio del sistema in uso nell'Oregon è che esso sfrutta il principio secondo cui se si fa appello alle migliori intenzioni del cittadino, la stragrande maggioranza "farà la propria parte" per assicurare l'integrità del processo democratico di voto; per assicurare che avvenga una disamina completa dei candidati e delle problematiche prima delle votazioni, controllando che tutte le schede siano trasferite e contate in modo sicuro; oppure favorendo quelle leggi e quelle politiche che garantiscono la possibilità di voto a tutti coloro in possesso dei requisiti necessari, e che questi voti siano contati, e che i candidati e i provvedimenti con il maggior numero di voti siano vincitori.

Tale sistema è anche più economico rispetto alle tradizionali procedure elettorali dei seggi. Che cos'ha che non va?

Da: Paul Rubin <phr-2003@nightsong.com>

Oggetto: macchine per il gioco d'azzardo contro macchine per il voto elettronico

Il documento all'indirizzo <<http://gaming.state.nv.us/forms/frm141.pdf>> mostra le procedure seguite per far certificare il progetto di una macchina per il gioco d'azzardo (per esempio un videopoker) nello stato del Nevada. Si noti che, secondo quanto riportato a pag. 4, tutto il codice sorgente delle parti della macchina inerenti al gioco deve essere sottoposto alla commissione per il gioco d'azzardo, unitamente ad una parte hardware sufficiente per poter essere verificata dalla commissione, e pare che il codice venga davvero esaminato riga per riga (per l'approvazione occorrono circa sei mesi). Vi sono anche delle specifiche riguardanti la sicurezza fisica delle macchine.

Dopo la messa in opera, il settore auditing effettua alcuni controlli casuali, andando nei casinò e smontando le macchine, verificando che le immagini EPROM in esse contenute siano effettivamente le stesse che furono approvate. Quattro o cinque altri stati svolgono simili verifiche per certificare l'apparecchiatura. Tutti gli altri stati seguono quanto viene deciso dai cinque o sei stati del gioco d'azzardo.

È assurdo che i produttori di macchine per il voto si mettano a piagnucolare così tanto perché il loro codice viene sottoposto ad auditing, visto che devono affrontare le stesse problematiche dei produttori di macchine da gioco (la revisione del codice serve in parte a garantire che la macchina non stia furtivamente prendendo qualche punto di guadagno extra), e che questi sembrano tollerare i requisiti richiesti.

Vi sono anche alcuni standard federali sulla certificazione del codice del firmware all'interno di impianti e protesi, o nell'avioelettronica. Sto cercando di raccogliere più informazioni su questo argomento. Il codice delle macchine per il voto non sembra avere standard alcuno.

Da: Arno Schäfer <arno_schaefer@gmx.de>

Oggetto: I dialer

Lei scrive: "Si tratta di una vecchia frode: un uomo si serve di un virus informatico per modificare i numeri di telefono di accesso a Internet e dirottare il collegamento verso numeri a tariffazione maggiorata, nel tentativo di guadagnare un sacco di soldi. Come costui abbia potuto pensare di farla franca, non lo capisco."

Quell'osservazione è interessante. In Germania, questi programmi chiamati "dialer" costituiscono un grandissimo problema, al punto che il Parlamento tedesco ha recentemente approvato una legge speciale in modo da arginare l'ondata di queste truffe. Oggi, far girare un tool "anti-dialer" è essenziale per gli utenti tedeschi di Internet, tanto quanto avere un

antivirus e un firewall installati. Apparentemente, per questi truffatori il pericolo di venire scoperti e perseguiti legalmente è lieve se confrontato con gli incentivi economici. Uno dei motivi di questo atteggiamento è che spesso è virtualmente impossibile scovare chi si cela dietro a questi numeri di connessione "a tariffa speciale". Esiste in Germania un'intera industria di venditori e rivenditori di questi numeri speciali, molti dei quali si trovano in altri paesi, lontano dalla giurisdizione tedesca. I costi di queste chiamate (fra cui le più spudorate arrivano ai 100 dollari al minuto, o fino a 1000 dollari a chiamata!) venivano raccolti insieme alla normale bolletta telefonica. Quando qualcuno scopriva di avere "contratto" accidentalmente un dialer, spesso era impossibile rintracciare i colpevoli, oppure era già troppo tardi ed erano spariti. In più occorreva provare di non avere attivato volontariamente il dialer, dato che questi venivano spacciati solitamente per "servizi" (ad esempio per accedere a contenuti vietati ai minori). Perciò riuscire a far processare davvero qualcuno per questo tipo di frode era l'eccezione, più che la regola. Per fortuna, la posizione legale delle vittime di questi imbrogli in Germania è migliorata decisamente, ormai.

Da: John Viega <viega@securesoftware.com>
Oggetto: Amit Yoran

Sono rimasto sorpreso, leggendo l'ultimo numero di Crypto-Gram, di aver visto Amit Yoran piazzato nel Canile per la seguente affermazione:

"Per esempio, dovremmo ritenere i produttori di software responsabili della sicurezza del loro codice o per quanto concerne eventuali falle nel loro codice? In teoria, ciò può avere un senso. Ma in pratica, sono essi in possesso delle capacità e degli strumenti per produrre un codice più sicuro?"

L'unico problema di questa affermazione è, a mio avviso, che è troppo decontestualizzata per riuscire a determinarne assolutamente gli intenti. Posso capire che lei l'abbia interpretata come se intendesse dire che "è impossibile produrre codice più sicuro di quel che produciamo oggi". Tuttavia, leggendo semplicemente tale dichiarazione, sembra più voler dire che costringere le aziende ad accettare determinate responsabilità non risolverà il problema, perché anche con un incentivo ad avere software perfettamente sicuro, le aziende non saranno in grado di distribuirlo, a causa delle complessità dello sviluppo del software e della mancanza di buoni strumenti e metodologie.

Se questo è ciò che il sig. Yoran vuole dire con quell'affermazione (e ne sono convinto, come dimostrerò fra poco), allora ha assolutamente ragione. Se da un lato vi sono chiaramente molte semplici cose che possono essere fatte per risolvere il problema (ad esempio utilizzare un qualsiasi altro linguaggio che non sia il C), il fine di costruire un sistema senza rischi è più o meno irrealizzabile in pratica. L'industria della sicurezza non ha mai fatto molto per facilitare la vita agli sviluppatori, per i quali la sicurezza non può più essere una preoccupazione secondaria.

Non solo noi, in quanto industria, non abbiamo fornito gli strumenti adeguati per supportare la progettazione, la realizzazione e il mantenimento di sistemi più sicuri, ma anche le soluzioni di sicurezza "pronte all'uso" che offriamo si prestano ad un cattivo uso. Per esempio, se da una parte Java viene talora indicato come linguaggio "sicuro", le posso dire che continuiamo a trovare un rischio di sicurezza di grave entità ogni mille righe di codice (o giù di lì) in programmi Java abilitati a Internet. Forse un esempio migliore è il SSL/TLS, dove le librerie che forniamo agli sviluppatori tendono ad incoraggiare un cattivo uso. Il modello mentale secondo cui gli sviluppatori devono usare tali librerie in un modo che protegga dai semplici attacchi dell'uomo della strada, è molto più complesso del modello che essi tendono ad avere in mente (ad esempio che SSL/TLS sia una semplice soluzione per rendere sicuro il traffico di rete). Di conseguenza, la stragrande maggioranza delle applicazioni che implementano SSL/TLS la prima volta sbagliano, e di grosso.

Certo, vi sono problemi di sicurezza del software che nessuno dovrebbe creare, in special modo il buffer overflow e i suoi simili. Ma sono sicuro che lei, più di altri, dovrebbe sapere quante cose possono andare storte in applicazioni connesse in rete (soprattutto quando sono coinvolti protocolli complessi) e quanto oscuri possano essere certi malfunzionamenti nei sistemi software. Per esempio è emerso un problema recente nel suo programma Password Safe, malgrado un'ideazione difensiva.

In più, sono sicuro che lei sia cosciente del fatto che le tecniche di progettazione e analisi della sicurezza del software sono ancora agli albori. Sto attualmente lavorando all'idea di riunire un consorzio per sviluppare delle metodologie di progettazione migliori, che si integrino più efficacemente con le attuali pratiche di ingegnerizzazione del software, perché non esiste ancora nulla di concreto in questo ambito. Mentre le tecnologie di analisi statica come il controllo di un modello sono vecchie di decenni, stiamo cominciando ad applicarle a problemi di sicurezza soltanto da alcuni anni. Tali tecnologie sono ancora piuttosto distanti dal punto in cui saranno sufficientemente complete e si integreranno adeguatamente con il flusso di lavoro degli sviluppatori più pignoli.

Anche in un mondo in cui vi fossero ottime tecnologie di progettazione e analisi, faremmo molta fatica ad istruire gli sviluppatori sulla miriade di rischi che li circondano fino a rendere gli attacchi di ingegneria sociale totalmente privi di senso pratico. Non è illogico affermare che ci troviamo molto distanti dal punto in cui avrebbe economicamente senso rendere i produttori di software responsabili degli errori di sicurezza.

Conosco personalmente Amit Yoran, e lo conosco abbastanza bene. È una persona estremamente intelligente e comprende il problema della sicurezza del software e i limiti dell'attuale tecnologia. Comprende questo problema così bene che, prima di accettare il compito di Capo della Cyber-Sicurezza, ha manifestato un attivo interesse negli affari inerenti al lancio della nostra impresa e alla nostra tecnologia di analisi. Quindi posso affermare con certezza che Amit non solo ha una comprensione del problema della sicurezza del software maggiore di molte altre persone, ma inoltre crede che sia importante per l'industria della sicurezza farsi pioniera di un nuovo corso verso la responsabilità, offrendo tecnologie e metodologie migliori.

Mi rendo conto di come lei abbia potuto fraintendere la posizione di Amit a causa dell'ambiguità di quella singola affermazione. Sono sorpreso, tuttavia, che lei sia giunto a formulare un giudizio così definitivo basandosi su quelle sole parole. Oltre al fatto che anche alcune sue affermazioni sono state mal riportate in almeno una circostanza, un minimo di approfondimento nei confronti di Amit avrebbe certamente rivelato il fatto che egli sia una persona assolutamente informata e competente in merito a questo argomento, e non appartiene allo stesso genere di ciarlatani che lei smaschera ogni mese.

Da: Mary Ann Davidson <mary.ann.davidson@oracle.com>
Oggetto: Amit Yoran

Rispondo a un commento che lei ha fatto nell'ultimo numero di Crypto-Gram in merito ad un'affermazione di Amit Yoran (non ho letto l'intervista originaria, per cui porti pazienza):

"Per esempio, dovremmo ritenere i produttori di software responsabili della sicurezza del loro codice o per quanto concerne eventuali falle nel loro codice?' si è chiesto Yoran durante un'intervista. 'In teoria, ciò può avere un senso. Ma in pratica, sono essi in possesso delle capacità e degli strumenti per produrre un codice più sicuro?'".

"Sono esterrefatto dalla totale idiozia di questo estratto. Ma pensa davvero che scrivere codice più sicuro è qualcosa di troppo difficile da gestire per quelle aziende? Pensa davvero che le compagnie stiano facendo assolutamente il meglio che possono?"

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>>.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2004 by Bruce Schneier.