

CRYPTO-GRAM  
15 novembre 2004

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

Edizione italiana curata da Communication Valley SpA

E-mail: [schneier@counterpane.com](mailto:schneier@counterpane.com)  
Web: <<http://www.schneier.com>> oppure <<http://www.counterpane.com>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Crypto- Gram in versione originale è anche consultabile in formato RSS:  
<<http://www.schneier.com/crypto-gram-rss.xml>>

Gli stessi articoli della newsletter sono disponibili sul blog di Bruce Schneier:  
<<http://www.schneier.com/blog>>.

\*\* \*\*

In questo numero:

Perché la tecnologia legata alle elezioni è difficile  
Le macchine per il voto elettronico  
Un attacco virale piuttosto scaltro  
Furto di una cassetta postale allo scopo di boicottare un voto  
La sicurezza informatica e la responsabilità  
Le ristampe di Crypto- Gram  
I playoff di baseball (World Series) e la sicurezza  
News  
Le News di Counterpane  
La sicurezza dei "controlli ed equilibri" (Checks and Balances)  
Il Canile: La Contea di Merced  
Security Information Management Systems (SIMS)  
Tecnologia e lotta al terrorismo  
Commenti dei lettori

\*\* \*\*

Perché la tecnologia legata alle elezioni è difficile

<[http://www.schneier.com/blog/archives/2004/10/getting\\_out\\_the.html](http://www.schneier.com/blog/archives/2004/10/getting_out_the.html)>

A quattro anni di distanza dal disastro avvenuto in Florida nel 2000 e due anni dopo che il Congresso ha passato lo Help America Vote Act, i problemi legati al voto sono di nuovo in primo piano: votazioni confuse, macchine per il voto non funzionanti correttamente, problemi riguardanti chi risulta registrato e chi non lo è. Tutto questo ci porta alla domanda di fondo: perché è così difficile gestire un'elezione?

Un requisito fondamentale per un'elezione democratica è il voto segreto, e questo è il primo motivo. I computer gestiscono solitamente transazioni finanziarie dell'ordine di milioni di dollari, ma molta della loro sicurezza deriva dalla capacità di tener traccia di tali transazioni dopo la loro esecuzione e

di correggere gli eventuali problemi ad esse legati. Molto di ciò che fanno può essere svolto il giorno successivo se il sistema non è attivo. Nessuna di queste soluzioni può essere messa in pratica nel caso delle elezioni.

Le elezioni americane si rivelano particolarmente difficili perché sono decisamente complicate. Un voto può avere 50 cose diverse su cui esprimere una preferenza, tutte (fuorché una) diverse per ogni stato, e molte diverse per ogni singolo distretto. È più semplice gestire le elezioni nazionali in India, dove ogni individuo esprime un unico voto, che non negli Stati Uniti. Inoltre, i sistemi delle elezioni americane devono poter essere in grado di gestire 100 milioni di votanti in un solo giorno: un'impresa immensa anche nelle migliori condizioni.

La velocità è un altro fattore. I cittadini americani vogliono i risultati delle elezioni prima di andare a dormire; non resisteremmo in un'attesa di due settimane prima di sapere chi ha vinto, come è accaduto quest'anno in India e in Afghanistan.

A peggiorare le cose va aggiunto il fatto che i sistemi di voto vengono usati raramente, al più qualche volta l'anno. I sistemi utilizzati quotidianamente migliorano perché le persone acquisiscono familiarità con essi, scoprono eventuali errori e cercano di trovare migliorie. Invece, sembra sempre che si debba rimparare come votare ogni volta che ci sono le elezioni.

Non dovrebbe sorprendere che vi siano problemi legati al votare. Ciò che sorprende è che i problemi non aumentano ogni volta. E quindi, come si può far funzionare meglio il sistema?

-- Semplicità: questa è la chiave per migliorare il sistema di voto. La registrazione dovrebbe essere il più semplice possibile. Il procedimento per votare dovrebbe essere il più semplice possibile. I progetti legati al sistema di voto dovrebbero essere semplici e sottoposti a test. L'industria informatica fa tesoro della scienza dell'interfaccia utente: tali conoscenze dovrebbero essere applicate alla progettazione del sistema di voto.

-- Uniformità: la semplicità porta all'uniformità. Gli Stati Uniti non hanno un unico insieme di regole per il voto, né un unico sistema di voto. Esistono 51 insiemi diversi di regole, uno per ogni stato e il District of Columbia, e un numero ancor superiore di sistemi di voto. Più si standardizzano i sistemi su tutto il territorio, più possiamo imparare dagli errori di ognuno.

-- Verificabilità: le macchine per il voto elettronico possono avere un'interfaccia utente molto semplice, ma la complessità sta dietro lo schermo e la tastiera. Per evitare ancor più problemi, queste macchine dovrebbero emettere un voto cartaceo verificabile dal votante. Non si tratta di una "ricevuta", niente che si possa portare a casa. Si tratta invece di una scheda cartacea che riporta quel che avete votato, un documento sul quale poter verificare la presenza di eventuali errori e, nel caso sia tutto a posto, poterlo infilare nell'urna. La macchina offre rapidi conteggi, ma la carta rimane la base per qualsiasi verifica dei voti.

-- Trasparenza: tutto il codice macchina utilizzato nelle macchine per il voto dovrebbe essere pubblico. Questo permetterebbe alle parti interessate di esaminarlo e di evidenziarne eventuali errori, e il risultato sarebbe una sicurezza sempre migliore. Qualsiasi azienda costruttrice di macchine per il voto elettronico che dichiarasse che il proprio codice deve rimanere segreto per motivi di sicurezza, sta dicendo bugie. La sicurezza nei sistemi informatici deriva dalla trasparenza (sistemi aperti che superano l'esame critico del pubblico) e non dalla segretezza.

Ma queste sono tutte soluzioni per il futuro. Se siete fra i votanti quest'anno, le vostre opzioni sono minori. Il consiglio che vi posso dare è votare con attenzione. Leggete attentamente le istruzioni, e fate domande se siete confusi. Seguite con attenzione le istruzioni, controllando ogni passo della procedura. Ricordate che potrebbe essere impossibile correggere un errore una volta terminato il procedimento per il voto. In molti stati, fra cui la California, potete richiedere una scheda cartacea se la macchina per il voto elettronico non vi convince.

Ma soprattutto, andate a votare. Quest'anno, migliaia di persone sono presenti ai seggi per aiutare i votanti a far sì che il loro voto sia valido.

Questo articolo è originariamente apparso sul San Francisco Chronicle:  
<<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/10/31/EDG229GREK1.DTL>>  
oppure <<http://makeashorterlink.com/?J353212C9>>

Si legga anche l'editoriale a riguardo, scritto da Avi Rubin:  
<<http://www.avirubin.com/vote/op-ed.html>>

\*\* \*\*

Le macchine per il voto elettronico

<[http://www.schneier.com/blog/archives/2004/11/the\\_problem\\_wit.html](http://www.schneier.com/blog/archives/2004/11/the_problem_wit.html)>

Nel dopo-elezioni presidenziali americane 2004, le macchine per il voto elettronico sono ancora una volta protagoniste delle news. Le macchine hanno perso dei voti, o ne hanno sottratti alcuni invece di aggiungerli, oppure li hanno raddoppiati. Poiché molte di queste macchine non hanno tracciamenti cartacei di verifica, un gran numero di voti non sarà mai conteggiato. E se da una parte è improbabile che vi sia stata una frode consapevole perpetrata attraverso le macchine per il voto elettronico allo scopo di cambiare i risultati delle elezioni presidenziali, dall'altra Internet pullula di voci e di accuse (non provate) di frode in un certo numero di giurisdizioni e corse elettorali. È ancora troppo presto per poter stabilire se alcuni fra questi problemi abbiano o meno influenzato le singole elezioni. Nelle prossime settimane vedremo se da tutte queste informazioni scaturirà qualcosa di rilevante.

Gli Stati Uniti ci sono già passati. Dopo il 2000, i problemi delle macchine per il voto elettronico sono stati in primo piano a livello internazionale. Il governo ha stanziato dei fondi per risolvere i problemi sull'intero territorio. Purtroppo, le macchine per il voto elettronico, pur essendo state introdotte come soluzione al problema, non hanno fatto altro che peggiorare la situazione. Ciò non vuol dire che tali macchine debbano essere abbandonate, ma che occorre progettarle per aumentare sia la loro precisione, sia la fiducia nella loro precisione da parte della gente. Un compito difficile, ma non impossibile.

Prima di entrare nel merito della questione, bisogna che spieghi perché votare è così difficile. Fondamentalmente, un sistema di voto presenta quattro requisiti imprescindibili:

1. Accuratezza. Lo scopo di un qualsiasi sistema di voto è manifestare l'intenzione di ogni singolo votante, e tradurre l'insieme di queste intenzioni in un riscontro finale. Se si arriva al punto che un sistema di voto non riesce ad ottenere quanto descritto, allora non abbiamo un sistema desiderabile. Questa caratteristica inoltre comprende la sicurezza: dovrebbe essere impossibile poter cambiare il voto o la scheda di qualcun altro, così come distruggere voti o influenzare in altri modi l'accuratezza del riscontro finale.
2. Anonimato. I voti a scrutinio segreto sono fondamentali per la democrazia, e i sistemi di voto dovrebbero essere ideati allo scopo di facilitare l'anonimato del votante.
3. Scalabilità. I sistemi di voto devono poter essere in grado di gestire elezioni di amplissima portata. In media, cento milioni di persone votano per le elezioni presidenziali negli Stati Uniti. Circa 372 milioni di persone hanno votato alle elezioni in India lo scorso giugno, e più di 115 milioni alle elezioni in Brasile tenute in ottobre. La complessità di un'elezione è un altro dei problemi. A differenza di molti paesi in cui le elezioni nazionali si riducono ad un unico voto per un singolo individuo o

partito, negli Stati Uniti un votante viene messo di fronte a decine di singole elezioni: nazionali, locali, e tutti i livelli intermedi.

4. Velocità. I sistemi di voto devono produrre risultati velocemente. Ciò è particolarmente importante negli Stati Uniti, dove la gente si aspetta di conoscere i risultati delle elezioni odierne prima di coricarsi. Questo è di minor importanza in altri paesi, dove la gente non ha problemi ad aspettare giorni (o settimane) prima di sapere chi ha vinto.

Attraverso i secoli, le varie tecnologie usate per il voto hanno fatto del proprio meglio. Il sistema di sassi e frammenti di coccio posti nei vasi, usato dagli antichi Greci ha portato alle schede cartacee imbucate in urne sigillate. Cabine elettorali meccaniche, schede perforate, e in seguito macchine a scansione ottica hanno sostituito i conteggi manuali. Le nuove macchine elettroniche per il voto promettono un'efficienza ancora maggiore, e il voto via Internet una comodità ancora maggiore.

Ma nella fretta di migliorare velocità e scalabilità, si è finito col sacrificare l'accuratezza. Ribadisco, per accuratezza non s'intende quanto bene vengano contate le schede ad esempio da un lettore di schede perforate. Né si intende come una macchina tabulatrice gestisca problemi quali frammenti punzonati ancora attaccati o non completamente rimossi, e cose del genere. Per accuratezza si intende con quanta efficacia il processo traduce le intenzioni del votante in voti propriamente contati.

Le tecnologie creano ostacoli all'accuratezza in forma di passi aggiunti. Ogni passo in più in un procedimento significa un maggior numero di potenziali errori, semplicemente perché nessuna tecnologia è perfetta. Prendiamo ad esempio un sistema di voto basato su scansione ottica. Il votante riempie i pallini su un pezzo di carta, che viene poi passato attraverso un lettore ottico. Il lettore rileva i pallini riempiti e conteggia i voti. Il sistema presenta diversi passi: votante - scheda - pallini - lettore ottico - tabulatore - totale centralizzato.

Ad ogni passo possono presentarsi degli errori. Se la scheda non è chiara, alcuni votanti riempiranno i pallini sbagliati. Se un votante non riempie bene un pallino, o se il lettore non funziona correttamente, allora il sensore non rileverà i pallini in modo appropriato. Anche gli errori a livello di tabulazioni (sia nella macchina, sia quando i totali parziali vengono raggruppati in totali più grandi) possono generare altri errori. Un sistema manuale, ovvero conteggiare le schede a mano e poi rifare il conteggio come controprova, è più accurato semplicemente perché presenta un minor numero di passi intermedi.

I tassi di errore nei sistemi moderni possono essere significativi. Alcune tecnologie per il voto presentano un tasso d'errore del 5%: ad una persona su venti che votano usando quel sistema non vengono conteggiati i voti in modo corretto. Tale sistema funziona lo stesso, perché il più delle volte gli errori non hanno rilevanza. Se si assume che gli errori siano distribuiti uniformemente (in altre parole, che vadano ad influenzare ciascun candidato con eguale probabilità), allora quegli errori non modificheranno il risultato finale, tranne in corse elettorali molto serrate. Quindi si vuole sacrificare l'accuratezza in favore di un sistema di voto che gestirà più rapidamente elezioni di ampia portata e complessità. Nelle corse elettorali più serrate, gli errori possono influenzare i risultati, ed è questa la ragione di un secondo conteggio. Tale verifica è un sistema alternativo di tabulare i voti: un sistema più lento (perché è manuale), più semplice (perché si concentra esclusivamente su una corsa), e quindi più accurato.

Si tenga presente che tutto questo è vero soltanto se tutti votano usando le stesse macchine. Se i quartieri di una città che tendono a supportare il candidato A usano un sistema di voto con un tasso d'errore maggiore rispetto al sistema di voto utilizzato in quelle parti della città che supportano il candidato B, allora i risultati saranno alterati a sfavore del candidato A. Questa è un'importante considerazione riguardante l'accuratezza del voto, anche se marginale rispetto al tema di questo articolo.

Tenendo in conto questo background, ecco che il problema delle macchine per il voto elettronico risulta chiaro. In effetti, l'espressione "macchine per il voto elettronico", o anche "macchine elettroniche per il voto", è una pessima scelta di termini. Molte delle attuali tecnologie di voto coinvolgono i computer. Computer ("calcolatori") sono sia le macchine a scheda perforata, sia quelle a

scansione ottica. Il dibattito attuale si concentra su quei sistemi di voto interamente computerizzati, in primis i sistemi touch-screen, chiamati macchine DRE (Direct Record Electronic). (Il sistema di voto usato nelle più recenti elezioni in India -- un computer con una serie di pulsanti -- è soggetto alle medesime problematiche). In questi sistemi al votante viene presentato un elenco di scelte su uno schermo, magari su più schermi se vi sono molteplici elezioni, ed egli indicherà la sua scelta toccando lo schermo. Queste macchine sono facili da usare, producono riscontri immediatamente dopo la chiusura dei seggi, e possono gestire elezioni molto complicate. Inoltre possono mostrare istruzioni in lingue diverse e permettono ai non vedenti e in genere ai disabili di votare senza bisogno di assistenza.

Sono anche maggiormente inclini all'errore. Lo stesso software che rende i sistemi di voto touch-screen così amichevoli, li rende allo stesso tempo imprecisi. Ancora peggio, sono inaccurati esattamente nella maniera peggiore.

I bug nei software sono cosa comune, come ben sa qualsiasi utilizzatore di computer. I programmi presentano regolarmente dei malfunzionamenti, a volte in modi sorprendenti e sottili. Ciò è vero per qualsiasi software, compreso quello presente nelle macchine per il voto elettronico. Alcuni esempi:

Nella Contea di Fairfax (Virginia), nel 2003, un errore di programmazione nelle macchine per il voto ha fatto sì che sottraessero misteriosamente 100 voti dai totali di un certo candidato.

Nella Contea di San Bernardino (California), nel 2001, un errore di programmazione ha fatto in modo che il computer cercasse i voti nella parte sbagliata della scheda in 33 elezioni locali, e questo ha portato alla mancata registrazione dei voti sulle schede relative a quella elezione. Un secondo conteggio è stato poi svolto a mano.

Nella Contea di Volusia (Florida), nel 2000, una macchina per il voto elettronico ha dato ad Al Gore un conteggio finale di 16.022 voti negativi.

Alle elezioni del 2003 nella Contea di Boone (Iowa), il sistema elettronico di conteggio voti ha generato un totale di più di 140.000 voti al termine delle elezioni municipali del 4 novembre. La contea ha solo 50.000 residenti, e meno della metà di essi aveva i requisiti per votare in quell'elezione.

Ci sono letteralmente centinaia di storie come queste.

Quel che è importante notare in questi problemi non è tanto che i risultati hanno mostrato riscontri poco accurati, ma che gli errori non erano uniformemente distribuiti, e hanno danneggiato un candidato più di un altro. Ciò significa che non si può assumere che gli errori si annulleranno l'un l'altro e non influiranno sull'andamento delle elezioni. Occorre presumere che qualsiasi errore andrà ad alterare i risultati in modo sensibile.

Un altro problema sta nel fatto che il software può essere craccato. Ovvero, qualcuno può introdurre volontariamente un errore che modifichi il risultato in favore del suo candidato preferito. Che le macchine per il voto siano o meno collegate a Internet il giorno delle elezioni non fa alcuna differenza. La minaccia risiede nel fatto che il codice macchina possa essere modificato durante le fasi di sviluppo e test, sia da uno dei programmatori o da un hacker maligno che riesca ad infiltrarsi nella rete aziendale della compagnia che produce le macchine per il voto. È più facile modificare di nascosto un sistema software che non un sistema hardware, ed è più facile rendere irrintracciabili tali modifiche.

Una terza problematica è che questi problemi possono avere effetti ad ampio raggio nel software. Un problema con una macchina manuale riguarda solo quella macchina. Un problema software, che sia accidentale o causato intenzionalmente, può ripercuotersi su molte migliaia di macchine, ed alterare i risultati di un'intera elezione.

Alcuni si sono espressi in favore delle macchine touch-screen per il voto, riferendosi ai milioni di dollari che vengono gestiti giornalmente dai Bancomat e da altri sistemi finanziari elettronici. Questa posizione ignora un'altra caratteristica fondamentale dei sistemi per il voto: l'anonimato. I sistemi

finanziari elettronici basano gran parte della loro sicurezza sulle verifiche (audit). Se si sospetta un problema, chi si occupa delle verifiche può andare a ritroso attraverso i passi registrati dal sistema e capire quel che è accaduto. E se il problema è davvero tale, è possibile verificare e riparare la singola transazione. Dato che le elezioni sono anonime, quel tipo di sicurezza semplicemente non è applicabile.

Con questo non intendo affermare che occorra abbandonare il voto con sistemi touch-screen; i benefici apportati dalle macchine DRE sono troppo grandi per poter essere accantonati. Tuttavia dobbiamo riconoscerne i limiti, e progettare sistemi che possano essere precisi malgrado quei limiti.

Gli esperti di sicurezza informatica sono unanimi su ciò che bisogna fare. (Alcuni esperti di sistemi di voto non sono d'accordo, ma credo che faremmo tutti meglio ad ascoltare gli esperti di sicurezza informatica. Qui i problemi risiedono nei computer, e non nel fatto che il computer venga impiegato nel sistema di voto). Due sono le indicazioni degli esperti di sicurezza:

1. Le macchine DRE devono avere un riscontro cartaceo verificabile dal votante (chiamato a volte scheda cartacea). Si tratta di una copia cartacea del voto che viene stampata dalla macchina, che il votante è autorizzato ad esaminare e a verificare. Non se la porta a casa: o la osserva sulla macchina, dietro a uno schermo di vetro, oppure prende il pezzo di carta e lo imbuca in un'apposita urna. Lo scopo è duplice. Primo, permette al votante di confermare che il suo voto è stato registrato secondo il suo volere. Secondo, mette a disposizione un buon sistema per effettuare eventuali secondi conteggi nel caso vi siano problemi con la macchina.

2. Il software usato sulle macchine DRE deve essere aperto al pubblico esame. Anche questo ha due funzioni: anzitutto permette a qualsiasi parte interessata di esaminare il software e di scoprire bug che possono in seguito essere corretti. Tale analisi pubblica migliora la sicurezza. In secondo luogo, aumenta la fiducia della gente verso il procedimento di voto. Se il software è pubblico, nessuno può insinuare che il sistema di voto è intrinsecamente parziale. (Le aziende che producono queste macchine dichiarano regolarmente che è necessario mantener segreto il loro software per ragioni di sicurezza. Non credeteci. In queste circostanze, la segretezza non ha nulla a che vedere con la sicurezza).

I sistemi computerizzati che presentano queste caratteristiche non saranno perfetti (nessun software lo è), ma saranno molto migliori di quelli che abbiamo oggi. Dobbiamo iniziare a trattare il software per il voto proprio come trattiamo qualsiasi altro sistema ad alta affidabilità. L'auditing che viene condotto sul software delle slot machine negli Stati Uniti è significativamente più meticoloso di quanto viene fatto con il software per il voto. Il processo di sviluppo del software mission-critical aeronautico fa sembrare il software per il voto come qualcosa fatto a casaccio. Se teniamo all'integrità delle nostre elezioni, tutto questo deve cambiare.

I sostenitori delle macchine DRE spesso indicano i risultati positivi delle elezioni come "prova" che il sistema funziona. Ciò è completamente fuori luogo. La paura è che gli errori nel software (sia accidentali, sia introdotti volontariamente) possano alterare in maniera invisibile i riscontri finali. Un'elezione senza problemi rilevati non è una prova dell'affidabilità e della sicurezza del sistema, così come il fatto che nessuno si sia introdotto nottetempo in casa vostra non è una prova che le vostre serrature funzionano bene. Magari è perché nessuno ci ha mai provato, o forse qualcuno ci ha provato e ci è riuscito... a vostra insaputa.

Anche se riusciremo a perfezionare la tecnologia, non avremo ancora finito. Se lo scopo di un sistema di voto è quello di tradurre accuratamente le intenzioni dei votanti in un riscontro finale, la macchina per il voto è solo un anello della catena. Nelle elezioni presidenziali americane del 2004, i problemi legati alla registrazione dei votanti, a impiegati non addestrati nei seggi, alla progettazione delle schede elettorali, e alle procedure per la gestione dei problemi hanno prodotto più un mancato conteggio di molti voti che non inconvenienti connessi alla tecnologia. Ma se occorre investire denaro in nuove tecnologie per il voto, ha senso spenderlo su tecnologie che rendano il problema più semplice, e non più difficile da risolvere.

Una versione di questo articolo è apparsa originariamente su openDemocracy.com:  
<[http://www.opendemocracy.com/debates/article- 8- 120- 2213.jsp](http://www.opendemocracy.com/debates/article-8-120-2213.jsp)>

Le esperienze di Avi Rubin in qualità di giudice elettorale:  
<<http://avirubin.com/judge2.html>>

Siti sul voto elettronico:  
<<http://www.blackboxvoting.org/>>  
<<http://www.verifiedvoting.org/>>  
<<http://www.votingintegrity.org/>>

Problemi con le Elezioni Presidenziali 2004:  
<[http://www.eff.org/deeplinks/archives/cat\\_evoting.php](http://www.eff.org/deeplinks/archives/cat_evoting.php)>  
<[http://votingintegrity.org/archive/news/e- voting.html](http://votingintegrity.org/archive/news/e-voting.html)>  
<<http://www.dailykos.com/story/2004/11/3/04741/7055>>  
<<http://www.alternet.org/election04/20416/>>  
<<http://www.newstarget.com/002076.html>>  
<[http://ustogether.org/Florida\\_Election.htm](http://ustogether.org/Florida_Election.htm)>  
<<http://www.washingtondispatch.com/spectrum/archives/000715.html>>  
<<http://www.michigancityin.com/articles/2004/11/04/news/news02.txt>>  
<<http://edition.cnn.com/2004/ALLPOLITICS/11/05/voting.problems.ap/index.html>>  
oppure <<http://makeashorterlink.com/?B283122C9>>  
<[http://www.palmbeachpost.com/politics/content/news/epaper/2004/11/05/a29a\\_BROWVOTE\\_1105.html](http://www.palmbeachpost.com/politics/content/news/epaper/2004/11/05/a29a_BROWVOTE_1105.html)> oppure <<http://makeashorterlink.com/?X3A323CB9>>  
<<http://www.ansiblegroup.org/furtherleft/index.php?option=content&task=view&id=51>>  
oppure <<http://makeashorterlink.com/?C593122C9>>  
<[http://www.truthout.org/docs\\_04/110504V.shtml](http://www.truthout.org/docs_04/110504V.shtml)>  
<[http://www.truthout.org/docs\\_04/110604Z.shtml](http://www.truthout.org/docs_04/110604Z.shtml)>  
<[http://www.commondreams.org/views04/1106- 30.htm](http://www.commondreams.org/views04/1106-30.htm)>  
<[http://www.truthout.org/docs\\_04/110804A.shtml](http://www.truthout.org/docs_04/110804A.shtml)>

Un progetto open source per sviluppare una macchina per il voto elettronico:  
<[http://open- vote.org/](http://open-vote.org/)>

Articoli sull'e- voting:  
<<http://www.pcmag.com/article2/0,1759,1677194,00.asp>>  
<<http://www.wired.com/news/evote/0,2645,65031,00.html>>

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

Un attacco virale piuttosto scaltro

<[http://www.schneier.com/blog/archives/2004/11/clever\\_virus\\_at.html](http://www.schneier.com/blog/archives/2004/11/clever_virus_at.html)>

Ho ricevuto questo messaggio e-mail, con un allegato chiamato "schneier@counterpane.com". Il file è davvero un file .COM eseguibile, presumibilmente veicolo di un virus. Uno scaltro attacco di ingegneria sociale, uno che non avevo ancora visto.

Da: ((un qualche indirizzo fittizio))  
A: schneier@counterpane.com  
Oggetto: Non è stato possibile recapitare il messaggio

Caro utente schneier@counterpane.com,

Il suo account email è stato utilizzato per inviare un gran numero di messaggi spam durante la scorsa settimana. È ovvio che il suo computer è stato attaccato e che ora fa girare un proxy server Trojan.

La preghiamo di seguire le istruzioni nel file allegato per poter mantenere sicuro il suo computer.

Virtualmente vostro,  
Team di supporto utenti counterpane.com

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

Furto di una cassetta postale allo scopo di boicottare un voto

<[http://www.schneier.com/blog/archives/2004/10/mailin\\_ballot\\_a.html](http://www.schneier.com/blog/archives/2004/10/mailin_ballot_a.html)>

Ampersand vive nell'Oregon, dove il sistema di voto è interamente via posta ordinaria. Lunedì (il giorno in cui a molti votanti dell'Oregon vengono fatte pervenire le schede), qualcuno ha abbattuto il cartello "No on 36" [No al 36] di Ampersand e ha rubato la sua cassetta postale, presumibilmente sperando di rubargli la scheda e impedirgli di votare "no" all'Emendamento 36. Fortunatamente aveva ricevuto la sua scheda il sabato precedente, altrimenti quel furto avrebbe facilmente funzionato.

Da "Alas A Blog": "Lunedì qualcuno si è introdotto nella nostra proprietà, ha abbattuto il nostro cartello "No on 36", e ha rubato la nostra cassetta postale (con dentro la posta di lunedì).

"Dubito che si sia trattato di un atto casuale di vandalismo; lo stato dell'Oregon ci ha inviato le schede la settimana scorsa (in Oregon si vota esclusivamente per posta), e moltissimi cittadini dell'Oregon hanno ricevuto la propria scheda lunedì. Per cui penso che qualcuno abbia rubato la nostra cassetta postale sperando di impadronirsi delle nostre schede e di impedirci di votare contro l'Emendamento 36".

Dubito che questo episodio sia stato parte di un'azione su vasta scala. Di certo, chiunque l'avesse fatto su larga scala, si sarebbe presto stancato di rubare cassette postali, e avrebbe soltanto preso la posta al loro interno. È anche difficile evitare di essere colti sul fatto, dato che occorre rubare la posta di giorno, dopo che è stata recapitata ma prima che i residenti tornino a casa e la prendano.

Ad ogni modo, è interessante come la spedizione di schede, con tempi prevedibili, e la prevalenza di cartelli di stampo politico in evidenza in giardino, faccia scattare un attacco con un bersaglio così ristretto.

<<http://amptoons.poliblog.com/blog/001231.html>>

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

La sicurezza informatica e la responsabilità

<[http://www.schneier.com/blog/archives/2004/11/computer\\_securi.html](http://www.schneier.com/blog/archives/2004/11/computer_securi.html)>

L'information INsecurity ci sta costando miliardi di dollari. La paghiamo in furti: furti di informazioni, furti finanziari. La paghiamo in termini di perdita di produttività, sia quando le reti smettono di funzionare, sia nelle decine di inconvenienti di sicurezza minori che dobbiamo sopportare un po' tutti. La paghiamo quando dobbiamo comprare prodotti e servizi di sicurezza che riducano le due precedenti perdite. Paghiamo per la sicurezza, anno dopo anno.

Il guaio è che tutti i soldi che spendiamo non stanno risolvendo il problema. Stiamo pagando, eppure finiamo sempre col trovarci in mezzo a insicurezze di ogni tipo.

Il problema risiede nel software insicuro. Cattiva progettazione, funzionalità male implementate, test inadeguati e vulnerabilità di sicurezza derivanti da bug software. Il denaro che spendiamo in sicurezza serve a gestire gli effetti del software insicuro.

Ed è questo il problema: non stiamo pagando per migliorare la sicurezza del software che sta sotto, ma stiamo pagando per venire a patti con il problema invece di risolverlo.

Il solo modo per risolvere il problema è che i produttori sistemino il proprio software, e non lo faranno finché non sarà nei loro migliori interessi finanziari.

Oggi, i costi del software insicuro non sono sostenuti dai produttori di quel software. In economia questo fenomeno si chiama esternalità, cioè il costo di una decisione viene sostenuto da persone diverse da quelle che hanno deciso.

Non vi sono vere e proprie conseguenze dannose per i produttori di software di bassa qualità e scarsa sicurezza. Ancora peggio, spesso il mercato premia la bassa qualità. Più precisamente, premia le funzionalità aggiuntive e il tempismo delle date di rilascio, anche se tutto questo va a scapito della qualità.

Se ci aspettiamo che i produttori di software diminuiscano le funzionalità, prolunghino i cicli di sviluppo e investano in processi di sviluppo software sicuri, tutte queste cose devono far parte dei loro migliori interessi finanziari. Stesso discorso se ci si aspetta che le grandi imprese investano in risorse significative per la sicurezza della propria rete aziendale (soprattutto per la sicurezza dei loro clienti).

La legge della responsabilità è un modo per entrare nei migliori interessi di quelle aziende. Aumentando i rischi connessi alla responsabilità, si aumentano i costi derivanti dall'agire in modo scorretto e quindi aumenterà la quantità di denaro che un CEO vorrà investire per agire in maniera corretta. La sicurezza è gestione dei rischi; la responsabilità va ad influenzare l'equazione dei rischi.

Fondamentalmente, dobbiamo aggiustare l'equazione dei rischi in modo che il CEO di turno abbia interesse nel risolvere effettivamente il problema, e attuando pressioni sul suo bilancio di esercizio è il sistema migliore per farlo.

Chiaramente, non si tratta di una situazione "tutto o niente". Vi sono molte parti coinvolte in un tipico attacco software. C'è anzitutto la compagnia che ha venduto il software contenente la vulnerabilità. C'è la persona che ha scritto il tool di attacco. C'è l'aggressore stesso, che ha sfruttato il tool per penetrare in una rete. C'è il proprietario della rete, a cui è stato affidato il compito di difenderla. Il cento per cento della responsabilità non deve ricadere sulle spalle del produttore del software, così come il 100% della responsabilità non deve ricadere sull'aggressore o sul proprietario della rete. Ma oggi il 100% del costo va a pesare direttamente sul proprietario della rete, e questa cosa deve finire.

Pagheremo sempre la sicurezza. Se i produttori di software si trovano ad avere costi di responsabilità, li passeranno su di noi. Potrebbe non costarci meno di quanto paghiamo oggi, ma visto che dobbiamo pagare, almeno pagheremo la risoluzione del problema. Obbligare il produttore di software a pagare per sistemare il problema e in seguito girare a noi i costi relativi significa che è molto probabile che il problema sarà risolto davvero.

La responsabilità cambia tutto. Al momento, non c'è ragione perché un'azienda di software non offra funzionalità su funzionalità su funzionalità. La responsabilità obbliga le compagnie a fare analisi ponderate prima di cambiare qualcosa. La responsabilità le obbliga a proteggere i dati che è loro compito proteggere. La responsabilità significa che chi si trova nella migliore posizione per sistemare un problema, sarà effettivamente responsabile del problema.

L'information security non è un problema tecnologico, ma economico. E il modo di migliorare l'information technology è di risolvere il problema economico. Fatto ciò, tutto il resto verrà da sé.

Questo articolo è originariamente apparso su Computerworld:

<<http://www.computerworld.com/securitytopics/security/story/0,,96948,00.html>>

oppure

<<http://makeashorterlink.com/?X3A3252C9>>

\*\* \*\*

Le ristampe di Crypto- Gram

Crypto- Gram è attualmente al suo settimo anno di pubblicazione. I numeri precedenti coprono tutta una serie di argomenti legati alla sicurezza e si possono trovare tutti a questo indirizzo: <<http://www.schneier.com/crypto-gram.html>>. Quella che segue è una selezione di articoli apparsi in questo mese gli anni scorsi.

Gli hacker degli aerei:

<<http://www.schneier.com/crypto-gram-0311.html#1>> (originale)

<<http://www.cryptogram.it/novembre03.htm#a1>> (traduzione)

La difesa del Trojan:

<<http://www.schneier.com/crypto-gram-0311.html#8>> (originale)

<<http://www.cryptogram.it/novembre03.htm#a8>> (traduzione)

Esposizione totale:

<<http://www.schneier.com/crypto-gram-0111.html#1>> (originale)

<<http://www.cryptogram.it/novembre01.htm#a1>> (traduzione)

Perché le Firme Digitali non sono delle Firme

<<http://www.schneier.com/crypto-gram-0011.html#1>>

Programmare il computer di Satana, ovvero: perché i computer non sono sicuri:

<<http://www.schneier.com/crypto-gram-9911.html#WhyComputersareInsecure>>

La crittografia a chiave pubblica basata sulla matematica delle curve ellittiche (Elliptic Curve Cryptography):

<<http://www.schneier.com/crypto-gram-9911.html#EllipticCurvePublic-KeyCryptography>>

oppure

<<http://makeashorterlink.com/?T2C3422C9>>

Il futuro della frode: tre motivi che spiegano perché il commercio elettronico è diverso.

<<http://www.schneier.com/crypto-gram-9811.html#commerce>>

La protezione anti- copia del software e perché non funziona:

<<http://www.schneier.com/crypto-gram-9811.html#copy>>

\*\* \*\*

I playoff di baseball (World Series) e la sicurezza

<[http://www.schneier.com/blog/archives/2004/10/world\\_series\\_se.html](http://www.schneier.com/blog/archives/2004/10/world_series_se.html)>

I playoff di baseball non sono estranei alla sicurezza. I tifosi cercano di intrufolarsi nello stadio senza biglietti o con biglietti fasulli. Spesso cibo e alcool non possono essere portati all'interno dello stadio, per appoggiare il monopolio delle concessioni a prezzi maggiorati. La violenza è sempre un rischio: sia piccole baruffe, sia scontri più gravi, come risultato dell'eccessiva vicinanza dei tifosi di entrambe le squadre -- come quell'incidente che è quasi accaduto durante la sesta partita dell'American League.

Oggi il nuovo rischio è il terrorismo. La sicurezza alle Olimpiadi è costata 1,5 miliardi di dollari. Alle convention Democratiche e Repubblicane sono stati spesi 50 milioni di dollari da ciascuna delle parti. Non c'è ancora stata una pubblica dichiarazione di quanto è costata la sicurezza per i playoff di baseball (World Series), ma è ragionevole supporre che sarà impressionante.

Nella smania di difenderci, è importante spendere saggiamente il nostro denaro. Molto di quel che la gente ritiene essere sicurezza contro il terrorismo, in effetti non ci rende affatto più protetti. Anche in un mondo di sicurezza ad alta tecnologia, la soluzione più efficace è il tizio che sta in guardia e impedisce che vengano gettate bottiglie di birra sul campo di gioco.

In genere, le misure di sicurezza atte a difendere bersagli specifici sono un inutile spreco, perché è possibile aggirarle semplicemente cambiando bersaglio. Se difendiamo i playoff di baseball da qualsiasi attacco possibile, e i terroristi fanno saltare una bomba in un affollato centro commerciale, non abbiamo ottenuto niente.

In ogni caso, alcuni siti di importanza rilevante, come monumenti nazionali ed edifici simbolici, e certi eventi di grande rilievo, come incontri politici e manifestazioni sportive giustificano un più imponente dispiegamento di forze di sicurezza. Quali misure aggiuntive hanno senso?

I controlli dei documenti d'identità non hanno senso. Chiunque ha un documento del genere. Lo avevano anche i terroristi dell'11 settembre. Ciò che vogliamo è in qualche modo un controllo sulle intenzioni: quella tal persona sta forse per compiere qualcosa di pericoloso? Ma non possiamo saperlo, e allora controlliamo i documenti. È un totale spreco di denaro e di energie, e non fa assolutamente nulla per renderci più sicuri.

I sistemi automatici di riconoscimento facciale non funzionano. Computer che automaticamente estrapolano i terroristi all'interno di una folla sono una bella idea per un film, ma non funzionano nel mondo reale. Non siamo in possesso di un database fotografico esaustivo dei terroristi conosciuti. Ancora peggio, la tecnologia di riconoscimento facciale è così imprecisa che spesso non riesce a far combaciare i profili anche quando abbiamo delle buone fotografie. L'abbiamo provata al Super Bowl del 2001: è stato un disastro.

Installare dei checkpoint come negli aeroporti non funziona. I terroristi che hanno occupato quella scuola in Russia avevano introdotto le armi molto prima di sferrare l'attacco. E controllare i tifosi è solo una piccola parte della soluzione. Semplicemente, c'è troppa gente, troppi veicoli e rifornimenti che si muovono dentro e fuori lo stadio con regolarità. Questo tipo di sicurezza ha fallito alle Olimpiadi. I reporter hanno infatti dimostrato ripetutamente come potevano introdurre ogni genere di cose all'interno degli stadi senza venire scoperti.

Ciò che funziona sono le persone: ufficiali di sicurezza in gamba che osservano il pubblico. Viene chiamata "behaviour recognition" (lett. identificazione del comportamento), e richiede personale addestrato a caccia di comportamenti sospetti. Qualcuno sembra fuori posto? È nervoso e non sta guardando la partita? Non sta esultando, fischiando, e gesticolando come farebbe un qualsiasi tifoso?

Questo è ciò che fanno in ogni momento i buoni poliziotti. È quel che fa la sicurezza dell'aeroporto israeliano. Funziona perché invece di affidarsi a checkpoint che possono essere aggirati, si appoggia alla capacità umana di notare qualcosa che non quadra. È intuito, ed è molto più efficace di qualsiasi soluzione di sicurezza "elettronica".

Tutto questo porterà a una sicurezza perfetta? Sicuramente no. Nessuna misura di sicurezza è una garanzia. Tutto ciò che possiamo fare è ridurre le circostanze avverse. E il modo migliore per farlo è di



\*\* \*\*

## Le News di Counterpane

Bruce Schneier sta tenendo una serie di tavole rotonde, trattando di problematiche di sicurezza insieme a vari CIO e CISO. Se intendete ricevere un invito per uno di questi eventi, inviate un messaggio email a [info@counterpane.com](mailto:info@counterpane.com). Fra le città che Schneier visiterà da qui alla fine dell'anno ci sono San Francisco, Sacramento e Chicago.

\*\* \*\*

## La sicurezza dei "Checks and Balances" (controlli ed equilibri)

<[http://www.schneier.com/blog/archives/2004/10/the\\_security\\_of.html](http://www.schneier.com/blog/archives/2004/10/the_security_of.html)>

Molta della retorica politica intorno alle elezioni presidenziali americane è incentrata sulle relative posizioni in merito alla sicurezza del presidente George W. Bush e del senatore John Kerry, dove ciascuna delle parti proclama a gran voce che il suo oppositore procurerà danni irreversibili alla sicurezza nazionale.

Il terrorismo è un grave problema che affligge gli Stati Uniti agli inizi del XXI secolo, e i punti di vista contrastanti di questi due candidati sono importanti. Ma questo dibattito oscura un altro rischio di sicurezza, uno ancora più vitale per gli Stati Uniti: la crescente centralizzazione del potere politico americano nelle mani dell'esecutivo del governo.

Più di 200 anni fa, gli artefici della Costituzione degli Stati Uniti crearono un meccanismo di sicurezza ingegnoso per evitare governi tirannici: divisero il potere governativo in tre entità distinte. Un sistema di checks and balances attentamente ponderato nei poteri esecutivo, legislativo e giudiziario assicurava che nessuna di quelle tre branche diventasse troppo potente. Dopo aver assistito alla nascita e alla caduta delle tirannie in Europa, questo sembrò un modo assai prudente di formare un governo.

Dall'11 settembre 2001, gli Stati Uniti hanno visto finire una larga fetta di potere nelle mani dell'esecutivo. Dal negare ai sospettati il diritto di processo (a volte persino il diritto di avere un avvocato), alla zona senza legge stabilita a Guantanamo; dal decidere quali trattati ratificati ignorare, a leggi-burla pensate per favorire l'open government, l'amministrazione Bush si è mossa costantemente per aumentare i propri poteri a scapito del resto del governo. I cosiddetti "Torture Memos", preparati su richiesta del presidente, sostengono che il presidente possa vantare potere illimitato se si resta nell'ambito della lotta al terrorismo.

Il potere presidenziale come problematica di sicurezza non avrà un ruolo nelle imminenti elezioni presidenziali americane. Bush ha dimostrato attraverso le sue azioni nei primi quattro anni di mandato che egli è a favore dell'aumento dei poteri della branca esecutiva del governo, ai danni del potere legislativo e giudiziario. Le parole di Kerry mostrano come lui sia sostanzialmente d'accordo con il presidente su questo aspetto. E in larga misura, la branca legislativa e quella giudiziaria si stanno facendo calpestare.

In tempi di crisi, la reazione umana più naturale è quella di cercare sicurezza in un unico leader forte. Questo spiega perché la retorica di Bush basata sulla forza è stata così ben accolta dai cittadini americani, e perché anche la campagna di Kerry è basata sulla forza. Purtroppo, consolidare il potere in un'unica persona è pericoloso. La storia mostra di continuo come il potere sia un cattivo influsso che porta alla corruzione, e più potere significa più corruzione. La perdita del sistema americano di checks and balances, controlli ed equilibri rappresenta un pericolo per la sicurezza molto maggiore del terrorismo.

L'antico senato romano aveva un sistema simile per affrontare crisi molto gravi. Se c'era una seria minaccia militare contro la sicurezza e l'incolumità della Repubblica, i lunghi dibattiti e la legislazione di compromesso che accompagnavano il procedimento democratico sembravano un inutile lusso. Il senato avrebbe designato un singolo individuo, chiamato "dittatore" (lat. "dictator", cioè "colui che ordina"), che avrebbe avuto potere assoluto su Roma in modo da gestire più efficacemente la crisi. Il periodo di designazione era di sei mesi oppure per tutta la durata dell'emergenza, qualunque fosse il periodo più breve. A volte questo funzionava, ma spesso le ingiustizie derivanti dall'aver un dittatore in carica si rivelavano peggiori della stessa crisi originale.

Oggi, i principi della democrazia gelosamente conservati nella Costituzione degli Stati Uniti sono più importanti che mai. Per vincere sul terrorismo a livello globale e contemporaneamente preservare i valori che hanno fatto grande l'America, il sistema costituzionale dei checks and balances è cruciale.

Non è una questione partigiana: non credo che John Kerry, se fosse eletto, deciderebbe di sua volontà di diminuire i propri poteri né più né meno di quanto farebbe un Bush in altri quattro anni di mandato. Ciò che serve agli Stati Uniti è un Congresso forte e un altrettanto robusto sistema giudiziario per controbilanciare la presidenza, e non delle entità deboli pronte a cedere ancor più potere al presidente.

Pubblicato originariamente sul Sydney Morning Herald.  
<<http://www.smh.com.au/articles/2004/10/26/1098667726433.html>>

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

Il Canile: la contea di Merced

<[http://www.schneier.com/blog/archives/2004/10/doghouse\\_merced\\_1.html](http://www.schneier.com/blog/archives/2004/10/doghouse_merced_1.html)>

La contea di Merced si trova in California, ed ha spiegato perché sono state scelte le macchine per il voto elettronico della Election System & Software (ES&S). Vi sono un mucchio di criteri di selezione piuttosto vaghi, ma questo è davvero esplicito: "Perché si serve di crittografia a 1064 bit e non di quella a 128 bit, che è meno sicura".

Questo è il sito Web, anche se quella frase è stata cancellata a seguito della citazione sul mio blog:  
<<http://web.co.merced.ca.us/elections/touchvote.html>>

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

Security Information Management Systems (SIMS)

<[http://www.schneier.com/blog/archives/2004/10/security\\_inform.html](http://www.schneier.com/blog/archives/2004/10/security_inform.html)>

L'industria della sicurezza informatica è colpevole di fare troppo sensazionalismo e di non mantenere le promesse fatte. Continua ripetutamente a dire ai clienti che è necessario comprare un certo prodotto per essere sicuri. Ripetutamente questi comprano il prodotto -- e continuano a non essere al sicuro.

I firewall non hanno tenuto gli aggressori alla larga -- infatti, il concetto di "perimetro" è decisamente erroneo. I sistemi anti-intrusione (IDS) non hanno mantenuto al sicuro le reti, e worm e virus continuano a procurare seri danni malgrado la grande diffusione di prodotti antivirus. È in questo contesto che voglio esaminare i SIMS, Security Information Management Systems (lett. "Sistemi di

Gestione delle Informazioni di Sicurezza”), che promettono di risolvere un grave problema delle reti: l'analisi dei log.

I file di log sono una miniera d'oro di informazioni di sicurezza, che contengono non soltanto gli allarmi IDS, ma messaggi provenienti dai firewall, dai server, dalle applicazioni e da altri dispositivi di rete. La vostra rete produce megabyte di questi log ogni giorno, e nascoste al loro interno si trovano le impronte di un attacco. Il trucco è scoprirle e reagire in maniera sufficientemente rapida.

Analizzare i messaggi di log può mostrare in che modo l'aggressore è riuscito a penetrare, a che cosa ha avuto accesso, se ha aggiunto delle backdoor o meno, e così via. L'idea alla base dell'analisi dei log è che se si riesce a leggere i messaggi di log in tempo reale, è possibile stabilire che cosa sta facendo l'aggressore. Se si è in grado di rispondere abbastanza velocemente, si può sbatterlo fuori prima che riesca a far danni. È il sistema di rilevamento e risposta della sicurezza. L'analisi dei log funziona, che si usino o no i SIMS.

Ancora meglio, essa funziona contro una vasta e variegata serie di rischi. A differenza delle “point solution”, il monitoraggio di sicurezza è generale. L'analisi dei log può rilevare aggressori a prescindere dalle loro tattiche.

Ma i SIMS non mantengono le aspettative generate dalla pubblicità, poiché sono privi di quell'ingrediente essenziale che manca a molti altri prodotti di sicurezza informatica: l'intelligenza umana. I firewall spesso falliscono perché sono configurati e gestiti in maniera impropria. Gli IDS sono spesso inutili perché non c'è nessuno che risponda ai loro segnali d'allarme, oppure perché non c'è nessuno che sia in grado di distinguere fra attacchi veri e falsi allarmi. I SIMS hanno lo stesso problema: a meno che non sia presente un essere umano esperto addetto al loro monitoraggio, non stanno difendendo proprio nulla. Gli strumenti sono efficaci solo quanto lo sono le persone che li utilizzano.

I SIMS richiedono vigilanza: gli attacchi possono avvenire a qualsiasi ora del giorno e in qualsiasi giorno dell'anno. Di conseguenza, il personale deve essere composto da cinque impiegati full-time; o in numero ancora maggiore, se si contano i supervisori e personale di rinforzo con capacità specialistiche. Anche se un'organizzazione potesse permettersi di pagare tutte queste persone, sarebbe difficile assumerle nel panorama lavorativo e professionale attuale. Attacchi contro una singola organizzazione non accadono con sufficiente frequenza per mantenere attivo e interessato uno staff di questo calibro.

Nel 1999 ho fondato Counterpane Internet Security; vendiamo un servizio in outsourcing chiamato Managed Security Monitory, in cui analisti di sicurezza addestrati effettuano un monitoraggio costante degli allarmi IDS e dei messaggi di log. Grazie alle informazioni che i nostri analisti hanno ricevuto dalla rete -- in tempo reale -- unitamente al loro addestramento e alla loro esperienza, essi sono riusciti a rilevare attacchi in diretta e hanno offerto ai clienti un livello di sicurezza che non avrebbero mai raggiunto altrimenti.

Quando abbiamo realizzato il servizio di monitoraggio Counterpane nel 1999, abbiamo esaminato dispositivi di log-monitoring di aziende quali Intellitactics e e-Security. A quei tempi non erano strumenti sufficientemente buoni per noi, così abbiamo sviluppato un nostro sistema proprietario. Oggi, grazie al calibro degli analisti che usano il sistema Counterpane, esso è migliore di qualsiasi prodotto SIMS commerciale. Siamo stati in grado di progettarlo pensando ai nostri analisti esperti in rilevamento e risposta, e non al mercato del generico amministratore di rete.

La chiave per la sicurezza di rete sono le persone, non i prodotti. Accumulare altri prodotti di sicurezza, come i SIMS, sulla nostra rete non potrà funzionare. È per questo che credo che la sicurezza di rete finirà con l'essere gestita in outsourcing. Non esiste un altro sistema economicamente conveniente per ottenere in modo affidabile gli esperti di cui si ha bisogno, e quindi nessun altro modo economicamente conveniente per ottenere una sicurezza affidabile.



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

## Commenti dei lettori

Da: "Dosco Jones" <doscojones@earthlink.net>

Oggetto: Delle scritte in arabo bastano ad interrompere un volo

Malgrado le scritte siano state descritte come "arabe", dopo un attento esame è stato stabilito che la lingua è il Farsi (la lingua ufficiale dell'Iran e di almeno altri due paesi -- <[http://en.wikipedia.org/wiki/Persian\\_language](http://en.wikipedia.org/wiki/Persian_language)>). La scritta altro non era che una semplice preghiera meditativa. Malgrado il Farsi scritto utilizzi una forma modificata dell'alfabeto arabo, non appartiene alla famiglia delle lingue arabe. Dubito che molti americani nativi siano a conoscenza di questo.

Da: "Michael Lambrellis" <mikelambrellis@hotmail.com>

Oggetto: Delle scritte in arabo bastano ad interrompere un volo

Lasciare una scritta sospetta su un aereo è un attacco denial-of-service molto efficace e a basso costo. Nel clima di terrore attuale, frammenti di carta con scritte in arabo sono di sicuro considerati sufficientemente sospetti da interrompere un volo. Il colpevole (se trovato) potrebbe anche negare plausibilmente qualsiasi intento malevolo, assicurando che il frammento altro non è che un messaggio alla sua amata, una ricetta per il falafel, o l'indirizzo dell'Hotel Hilton a Riyadh.

Un pezzo di carta non può causare morti, ma giova indubbiamente al terrorismo. Si tratta di un classico attacco asimmetrico che non costa praticamente nulla a chi lo crea, ma provoca gravi costi per chi viene attaccato. Immaginiamo la pubblicizzazione di simili note lasciate sugli aerei per un periodo di un mese o due: essa verrebbe a decadere a mano a mano che le persone diventano assuefatte alla minaccia. L'immediata conseguenza a tutto questo sarebbe una progressiva indifferenza a simili scritte o a qualsiasi altra cosa altrettanto sospetta. Il costo è grande. Mancati guadagni per le compagnie aeree, per i loro clienti, ritardi nell'invio di merci, per non parlare di una riduzione della clientela. Come potrebbero rispondere le compagnie aeree? Istruendo tutti i piloti in arabo? Un numero sufficiente di falsi allarmi e alla fine ai membri dell'equipaggio sarà ordinato di ignorare scritte del genere.

Purtroppo, proprio come accade nella rete, dove gli attacchi DOS sono molto più numerosi di vere e proprie infiltrazioni nel sistema, nel mondo reale mi aspetto che la facilità di creare certi attacchi stile DOS finirà con il prevalere sul numero di attacchi terroristici veri e propri. Il risultato? Una caduta generale del livello di attenzione nella comunità, e le imprese affronteranno i costi finanziari allo stesso modo con cui hanno gestito la frode delle carte di credito, cioè li metteranno in conto come un altro valore assicurabile.

Da: Tracy R Reed <treed@copilotconsulting.com>

Oggetto: Re: CRYPTO-GRAM 15 ottobre 2004

Lei ha segnalato:

"Un client di e-mail con crittografia per il Treo:

<<http://discussion.treocentral.com/showthread.php?t=57658>>"

Possedendo un Treo, ho letto questo articolo con grande interesse. Purtroppo, pare che utilizzino un algoritmo crittografico proprietario, a "21.000" bit e quindi 200 volte più sicuro della crittografia SSL a 1024 bit. Tutto questo non suona molto incoraggiante. Come lei ha fatto notare in molte occasioni, gli algoritmi proprietari hanno una grande probabilità di rivelarsi insicuri, e il fatto che questi confrontino



CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

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](mailto:crypto-gram@communicationvalley.it).

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.