







Qualcuno sta diffondendo gli avvertimenti del CERT prima che siano pronti:

<<http://www.wired.com/news/infostructure/0,1377,58106,00.html>>

<<http://news.com.com/2100-1002-993375.html>>

Reali problemi con il voto anonimo telematico:

<<http://www.frogsonice.com/skateweb/articles/crash.shtml>>

Gli utenti non si fidano della sicurezza Microsoft, eppure si fidano ancora della sicurezza Microsoft:

<<http://news.com.com/2100-1002-994878.html>>

Uno studio interessante, "Strike and Counterstrike: The Law on Automated Intrusions and Striking Back". (attacco e contrattacco: la legge sulle intrusioni automatizzate e sulle risposte agli attacchi)

<<http://www.blackhat.com/presentations/win-usa-03/bh-win-03-karnow-notes.pdf>>

oppure <<http://tinyurl.com/9c43>>

Uno studio molto interessante, "The Myth of Security at Canada's Airports". (Il mito della sicurezza negli aeroporti canadesi)

<<http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05jan03-e.pdf>> oppure <<http://tinyurl.com/9c46>>

<<http://tinyurl.com/9c46>>

Le origini di quella finta notizia di cronaca riguardante una stampante infetta da un virus inviato di nascosto in Iraq durante la prima Guerra del Golfo.

<<http://www.securityfocus.com/columnists/147>>

Simpatizzanti dei terroristi sauditi studiano la sicurezza informatica nelle università americane. "Dopo aver studiato nel Texas e nell'Indiana, al-Hussayen ha iniziato il programma di dottorato dell'Università dell'Idaho in Informatica nel 1999, con una specializzazione in sicurezza informatica e tecniche di intrusione, secondo le accuse".

<<http://www.washingtonpost.com/wp-dyn/articles/A12758-2003Mar11.html>>

Qui vengono analizzati i bilanciamenti fra sicurezza ottenuta e libertà perdute:

<<http://www.nytimes.com/2003/03/11/politics/11SECU.html>>

<<http://www.plastic.com/article.html;sid=03/03/12/06265215;cmt=42>>

Interessante studio su come servirsi degli errori di memoria per attaccare un computer virtuale. L'attacco sfrutta il fatto che un controllo sul "tempo di compilazione" non è necessariamente valido durante il "tempo di impiego".

<<http://www.cs.princeton.edu/%7Esudhakar/papers/memerr.pdf>>

Vi sono parecchie reti di macchine compromesse, una di esse è composta da 140.000 computer. Le macchine hanno avuto dei programmi robot collegati ad esse; i robot instaurano un canale di comunicazione mediante server IRC (Internet Relay Chat) per ricevere comandi. Visto che occorrono centinaia di computer collegati in rete per buttar giù un grosso sito Internet con un attacco di tipo Denial-of-Service, queste reti potrebbero causare seri danni.

<<http://www.eweek.com/article2/0,3959,935790,00.asp>>

Un nuovo modo di rubare una password. Un cliente di carta di credito Discover riceve un'e-mail che lo informa che il suo conto è sospeso a causa di inattività, e che per riattivarlo egli dovrà effettuare il login in un certo sito web fasullo. I dati raccolti comprendono molte informazioni che permetterebbero un furto di identità: numero di Previdenza Sociale, cognome della madre da nubile, numero di conto e password. Simili frodi hanno colpito anche clienti PayPal ed eBay.

<<http://www.msnbc.com/news/884810.asp>>

<<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,79380,00.html>> oppure <<http://tinyurl.com/7mgh>>





Non solo si tratta di cattiva pratica sociale, ma è anche cattiva sicurezza. Un database con più errori è molto meno utile di un database che ha già molti errori, e un database di sicurezza pieno di errori ha molte più probabilità di prendere di mira gli innocenti che di lasciare i colpevoli a piede libero.

Per constatare questo, facciamo un esempio. Ammettiamo che vi sia un semplice database composto da nome e da un singolo codice che indica "innocente" o "colpevole". Quando un poliziotto ferma un individuo, controlla le generalità di costui nel database, e nel caso il database dica "colpevole", procede all'arresto.

Esempio 1: il database è corretto al 100%. Se questo è il caso, allora non ci saranno arresti sbagliati a causa di dati errati. Funziona perfettamente.

Esempio 2: il database ha un tasso di errore dello 0,0001%, cioè un errore su un milione di casi (diciamo errore nel caso una persona ha codice innocente quando è in effetti colpevole, o un codice colpevole quando invece è innocente). Inoltre, poniamo che una persona su 10.000 sia colpevole. In questo caso, per ogni 100 individui colpevoli correttamente identificati, il database identificherà erroneamente una persona innocente come colpevole (a causa di un errore). Il numero di persone colpevoli erroneamente indicate come innocenti sarà piccolo: una su un milione.

Esempio 3: il database ha un tasso di errore dell'1% (un errore su cento casi) e lo stesso tasso di un colpevole ogni 10.000 persone. I risultati sono molto diversi. Per ogni 100 persone colpevoli individuate correttamente, il database identificherà erroneamente 10.000 innocenti come colpevoli. Il numero di persone colpevoli erroneamente indicate come innocenti sarà più grande, ma sempre contenuto: una su cento.

Le differenze fra gli esempi 2 e 3 sono impressionanti. Nell'esempio 2 una persona viene erroneamente arrestata per ogni 100 persone arrestate giustamente. Nell'esempio 3, una persona viene arrestata correttamente per ogni 100 persone arrestate per sbaglio. Questo aumento del tasso di errore rende il database completamente inutile come sistema per stabilire chi arrestare. Questo accade a prescindere dal fatto che, in entrambi i casi, quasi nessun colpevole rimane a piede libero a causa di un errore del database.

La ragione di questo fenomeno è che il numero di persone colpevoli è una percentuale molto piccola della popolazione. Se vi fosse un colpevole ogni dieci innocenti, allora un tasso di errore dello 0,0001% porterebbe all'arresto erroneo di un innocente per ogni 100.000 colpevoli, e un tasso d'errore dell'1% porterebbe all'arresto di circa un innocente per ogni colpevole. Se il numero di colpevoli è ancora minore di uno su diecimila, allora il problema di arrestare delle persone innocenti aumenta con l'aumentare di errori nel database.

Ora, questo è un esempio semplice, e il database NCIC contiene dati molto più complessi e cerca di instaurare delle correlazioni molto più complesse. Io sto presumendo che il tasso di errore per i falsi positivi sia lo stesso del tasso di errore per i falsi negativi, e che non vi siano dipendenze di dati che possano complicare l'analisi. Ma anche con queste complicazioni, i problemi non cambiano. Dato che vi sono così pochi terroristi (per esempio) in mezzo alla popolazione globale, un database ricco di errori ha più probabilità di scambiare persone innocenti per terroristi che non di catturare veri terroristi.

Questo genere di cose sta già accadendo. Vi sono 13 milioni di persone sulla watch list dell'FBI riguardante i terroristi. Ciò è assurdo, è semplicemente inconcepibile che una quantità di persone pari al 4,5% della popolazione degli Stati Uniti sia composta da terroristi. Vi sono molti più innocenti su quell'elenco di quanti colpevoli non vi siano su quell'elenco. Queste persone innocenti vengono continuamente tormentate dalla polizia che cerca di fare il proprio lavoro. Ad ogni modo, una watch list contenente 13 milioni di persone è essenzialmente inutile. E poi, quante risorse ci si può permettere di spendere per controllare un ventesimo della popolazione?



Copyright (c) 2003 by Counterpane Internet Security, Inc.