15 febbraio 2000 0:00

INTERNET: HACKERS COME IL MILLENNIUM BUG

ALLARMISMO ECCESSIVO E SCANDALISTICO: BASTANO POCHE ACCORTEZZE COME QUANDO SI APRE UN NEGOZIO

Ormai e' allarme hackers, il terrorista del 2000 che tutto puo' ... almeno cosi' sembra nel leggere le vere e proprie cronache di guerra -a meta' tra disinformazione, fantascienza e sensazionalismo- che da piu' parti si trovano.
Sara' che noi siamo in rete da diversi anni e che, personalmente lo sono dal 1989, per cui la conoscenza dei fenomeni ci porta a centrare il cuore del problema e a non fermarci a gridare "al lupo al lupo" sull'onda di un generale allarmismo, ma sta di fatto che tutto quello che viene diffuso ci sembra eccessivo e, soprattutto, tendente a demonizzare sicurezza e serenita' del lavoro e della comunicazione in Internet.
Infatti perche' un gruppo di hackers -piu' o meno organizzati ... ma sono piu' che altro leggende metropolitane- riesca ad avere successo su un sito per attaccarlo, devono essere non solo bravi, ma avere qualcuno che, dall'interno del sito che intendono mettere in difficolta', gli faccia da "gola profonda".
Per capire meglio, e' come una banca con i suoi sistemi di sicurezza (per fare un esempio in cui si presuppone che la sicurezza sia una delle principali necessita'): se non sono attivi o se c'e' qualcuno che ne riferisce le caratteristiche ai malintenzionati, il gioco e' facile. Il resto e' come nella vita ordinaria: se un negozio e' senza serratura, e' chiaro che un ladro potra' piu' facilmente entrarci, e la faciloneria con cui molti hanno cominciato a fare E-commerce e' come se avessero aperto un negozio dimenticandosi di ordinare anche una saracinesca con serratura.
Le similitudini con quello che e' successo per il millennium bug, sono semplici: entrambi frutto di approssimazione e tecnici improvvisati.
(Vincenzo Donvito)

... MA LA SICUREZZA IN RETE E' UN'UTOPIA ..
Un amico ricercatore universitario mi ha sempre detto che un computer sicuro e' un computer spento, questo perche' la rete internet, cosi' come e' stata concepita trent'anni orsono, e' intrinsecamente insicura. Infatti quando Internet venne ideata gli utenti erano pochi ed interessati soprattutto alle sue possibilita' di interconnessione, adesso il panorama della rete e' molto diverso e vorremmo dare una mano a coloro che stanno pensando di creare un proprio sito (in quanto coloro che si connettono con un modem od una ISDN sono relativamente attaccabili proprio a causa della connessione ballerina).
Innanzitutto dobbiamo sapere che nessun sistema e' inarrestabile o perfettamente sicuro e non esistono software in grado di garantirvelo (lo stesso caso di Yahoo e Amazon lo fanno capire: un mega ping death, come viene chiamato in gergo, come quello e' difficile fermarlo, ma non impossibile) e per rendere la vita dura ai lamers necessita:
1. Immaginarsi come verranno portati gli attacchi al computer
2. Non dare la possibilita' ad altri di impadronirsi delle nostre Password
Per il primo punto bisogna controllare che il nostro sistema non stia utilizzando un programma buggato ovvero che non abbia pecche di fabbrica che lo rendano utilizzabile come piede di porco per entrare nel sistema informativo; per questo possiamo puntare i nostri browser a:
* Computer Emergency Response Team (CERT http://cert.org) della Carnegie Mellon University: un sito molto sobrio ed estremamente professionale, potete trovarci le documentazioni di tutti i bug di sicurezza di numerosissimi programmi e le patch (correzioni) per risolvere il problema
* s e c u r i t y f o c u s (http://www.securityfocus.com): sito molto ben fatto con un motore di ricerca molto semplice, nel quale, una volta inserito il nome del programma sospetto, potete trovare tutta la discussione fatta al riguardo sulle varie mailing list di sicurezza, gli exploit (ovvero programmi per verificare se il nostro sistema e' veramente affetto da un simile problema) una dettagliata documentazione tecnica, una patch e l'indirizzo dello scopritore del BUG
* Rootshell (http://www.rootshell.com) e' gia' un sito piu' cattivello rispetto ai precedenti e descrive i vari exploit per impossessarsi dei diritti di Amministratore su di un computer da attaccare, c'e' anche un simpatico programmino (se volete provare cliccate qui http://www.rootshell.com/smbcheck.cgi) che verifica se il vostro sistema Wintel esporta a tutta Internet il vostro disco fisso
* Se siete ancora in cerca di prove cattivelle per provare il vostro sistema andate a NewOrder (http://neworder.box.sk): qui trovate i ferri del mestiere dei vari lamer e crackers

* Se poi volete farvi testare il vostro computer (solo se siete permanentemente connessi visto che ci vogliono ore) puntate il vostro browser a: Webtrends (http://www.webtrends.com) dove potete usufruire gratuitamente di uno scanning da parte Security Analizer, un programma discendente da S.A.T.A.N. che loro stessi commercializzano; dopo alcuni giorni dallo scan riceverete una mail con le istruzioni per poter accedere ai risultati.
* Se siete in vena di filosofia della sicurezza e volete saperne di piu' sulle sigle e la cultura della sicurezza andata ad AntiOnline (http://www.antionline.com) molto interessante ed all'insegna del full disclosure ovvero sulla diffusione dell'informazione come difesa dai possibili attacchi.
Per il secondo punto bisogna dotarsi di un sistema crittografico per l'autenticazione sui server, onde evitare lo sniffing (ovvero ascoltare cosa passa sulla rete): quando controllate la posta, effettuate un telenet o effettuate una sessione ftp, gli username e le password che inserite vengono trasmesse cosi' come sono al server, e chiunque puo' leggerle e usarle indebitamente, ma cosi' non avviene quando usate il vostro navigatore per fare acquisti on-line su siti sicuri (avete mai visto comparire un lucchetto chiuso sul vostro browser? se si allora avete gia' potuto ususfruire di una connessione criptata).
Cosa fare per difendersi?
Come utenti casalinghi di Internet scegliere dei provider che diano la possibilita' di usare un protocollo sicuro per lo scambio della posta invece del POP3 (i protocolli sicuri sono: IMAP, Kerberos o POP3ssl), per utenti piu' professionali dotarsi di SSH (secure shell) (http://www.ssh.org) in sostituzione di telnet (potete trovare i client gratuiti per windows a http://www.replay.com http://www.doc.ic.ac.uk/~ci2/ssh) e cercare di evitare ftp.
Difendersi in questi casi vuol dire non lasciare la possibilita' ad altri di attaccarci!!
(Francesco Giovannini, solution manager di Toscana telematica srl, che cura il web dell'Aduc)