Autore: Raoul Chiesa - *Ottobre 1999*

Aziende, Y2K e consulenti esterni: dove va la sicurezza?

In un recentissimo articolo apparso sul Dow Jones Newswire, il gruppo hacker dei L0PHT accusa le aziende informatiche che subappaltano consulenti informatici: cerchiamo di capire quali sono i problemi ed i possibili pericoli.

14 ottobre 1999, Down Jones Newswire: intervista via e-mail a The Mudge, membro dei L0PHT (si pronuncia loft), storico gruppo hacker americano nato nel 1992. Oggi i L0PHT hanno una propria divisione security dedicata alle aziende, la L0PHT Heavy Industries (http://www.l0pht.com, 500.000 accessi al giorno). I membri sono conosciuti pubblicamente solo attraverso i propri nickname (soprannomi di rete) e si presentano con nome e cognome esclusivamente con i loro clienti. Clienti che sono nell'elenco Top 500 di Fortune USA, potenti multinazionali che operano in diversi settori. Grazie ai loro advisory la Microsoft chiuse immediatamente un security hole molto compromettente ed oggi i L0PHT sono un punto di riferimento serio per le grandi aziende americane.

I L0PHT hanno fatto negli USA quello che io con MediaService (http://www.mediaservice.net/) sto facendo in Italia da alcuni anni: proporsi come ***migliore soluzione antihacking*** , in quanto hacker per più di un decennio.

Mudge ha annunciato che entro i primi di novembre renderà pubblico un suo report, dove analizzerà ed elencherà 30 sistemi informatici insicuri, i quali hanno il compito di gestire la fornitura della corrente elettrica negli Stati Uniti. L'hacker-consulente spiega che questi sistemi sono facilmente "shuttable", vale a dire che si possono spegnere da remoto senza grandi problemi. Sino a qua nulla di nuovo, sentiamo parlare in continuo dell'insicurezza dei sistemi informatici, di attacchi da parte di hacker agli stessi e della poca cultura nei confronti dell'Information Security.

"Lo faccio per gli utenti, gli utilizzatori finali: il sistema è insicuro e il fornitore del servizio ***deve provvedere*** in tal senso", spiega Mudge. Normalmente gli elenchi di aziende insicure e di trucchi per aggirare le barriere informatiche (bug, exploit, script, etc..) vengono immediatamente pubblicati sul sito del L0PHT; in questo caso specifico il gruppo di consulenti di alto livello ha comunicato che attenderà, sperando che le aziende implicate provvedano a "tappare i buchi" prima della pubblicazione on-line.

Questa volta, però, non si punta il dito contro questi problemi, ma si cerca di rendere pubblico un nuovo, pericoloso problema: il boom del "Millenium Bug" (Y2K) ha avuto come naturale conseguenza la "corsa" alla standardizzazione e l'impiego a tamburo battente di consulenti informatici e programmatori: tutte persone prese in outsourcing.

E' ovvio che per modificare programmi che girano su sistemi informatici, serve avere accesso a tali sistemi; l'accesso serve privilegiato (ogni sistema operativo ha più livelli di accesso e di privilegi utente), e una volta ottenuto un accesso privilegiato creare un utente fantasma o una "backdoor" (porta di servizio per accedere ugualmente al sistema aggirando le barriere e le richieste di password) è molto facile.

Mudge ha "esplorato" i 30 principali sistemi di gestione per l'erogazione ed il controllo dell'elettricità negli USA: "tutti hanno un buco comune, e questa è stata la cosa che mi ha fatto pensare". Buco comune che sembra opera di una stessa persona, o che ha comunque delle caratteristiche comuni. L'FBI accusa i consulenti, dicendo che "le utility ed i sottoprogrammi sono così vulnerabili -- permettendo dunque attacchi ed intrusioni esterne non autorizzate -- perché sono stati "affittati" così tanti consulenti esterni per risolvere in fretta e furia la problematica Anno 2000, con il conseguente annullamento di ogni policy base di sicurezza, ove queste esistevano, lasciando di fatto degli esterni a mettere le mani su procedure e sistemi sensibili". Mudge replica che "ad oggi sono più pericolosi i consulenti Y2K che gli hacker stessi" e raccoglie i consensi di Scott Bradner, Senior Technical Consultant alla Harvard University e vice presidente per gli standard della Internet Society. Bradner conferma di essere a conoscenza di almeno 3 "Y2K Incidents", causati da consulenti esterni per il Millenium Bug "affittati" da aziende di consulenza, i quali avevano introdotto backdoor in sistemi di importanza nazionale.

Il problema reale sta diventando comunque la "forma mentis" adottata di default dalle aziende, come spiega Robert Rubin, analista alla Bear Stearns & Co, a New York City: "lavoriamo e creiamo reti sotto la convinzione che la gente non tenti di violare una rete aziendale e tantomeno i server di gestione erogazione servizi elettrici: quando si verifica un problema, siamo obbligati a contattare l'appropriata Agenzia Governativa, la quale indaga e si occupa del caso." L'FBI ha però comunicato allo U.S. Senate che il loro team di esperti informatici è sovraccarico di lavoro, e che il numero di richieste d'intervento per computer hacking e network intrusions è raddoppiato ogni anno, da due anni a questa parte. Il solo media italiano "tradizionale" (cartaceo) ad aver parlato -- seriamente e con competenza -- del problema è sinora stato Il Sole24Ore (http://www.ilsole24ore.it), tramite gli articoli e gli approfondimento di Rosanna Santonocito.

Negli USA il timore di atti "cyber-terroristici" è molto alto e l'informazione viaggia ***sempre di più on-line*** : nel nostro Paese stiamo iniziando -- grazie alle spinte di AIPA e RUPA - ad intravedere un'informatizzazione totale, un

collegamento ed uno scambio di dati aggiornati tra le varie realtà statali ed i servizi per il cittadino. Cosa accadrà quando anche in Italia l'informazione ***sensibile*** viaggerà on-line e di colpo ci renderemo conto di aver trascurato per anni un problema importante chiamato **Sicurezza Informatica?**