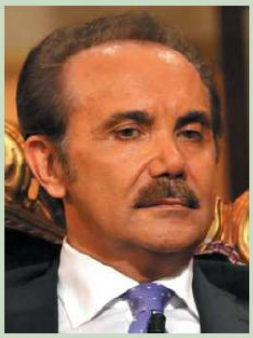
ItaliaOggi
diffusione:9304
tiratura:22827

IL PUNTO DI MAURO MASI*

Hacker, la cyber-war è già realtà

Qualche tempo fa la Honda subì un attacco informatico alla sua rete aziendale che compromise gravemente le operazioni della società in tutto il mondo; alcuni stabilimenti furono chiusi e il servizio assistenza clienti si è dovuto fermare per molti giorni. Secondo la casa di Tokyo, il problema aveva riguardato i suoi server, i sistemi di posta elettronica e altri programmi interni che erano stati infettati da un virus informatico introdotto da un attacco da parte di più hacker. A suo tempo invece fece scalpore (e lo fa tuttora) il fatto che l'Fbi fosse riuscita ad «aprire» lo smartphone del terrorista autore della strage di San Bernardino (in California) contro la volontà di Apple (che intendeva così dare un segno di come tutelasse la privacy dei propri clienti) grazie a un'azienda che utilizzava alcuni dei più abili (e temuti) hacker del mondo. Sono due esempi di natura opposta che indicano come il fenomeno hacker possa avere declinazioni sicuramente negative ma anche positive. Il termine hacker indica qualcuno che riesce a inserirsi in un sistema o in una rete senza la volontà dei gestori. Alcuni hacker hanno (spesso involontariamente) contribuito a rendere più sofisticati ed efficaci i sistemi di sicurezza di rete, così come importante è stato, ed è, il loro rapporto con il movimento open source. Recentemente **Elon Musk** ha assunto, per «migliorare Twitter», quello che passa per essere il «più quotato» hacker mondiale, **George Hotz**. Sui media poi ha raccolto particolare attenzione il gruppo Anonymous, che ha rivendicato nel tempo una serie di spettacolari azioni di disturbo in rete anche a siti istituzionali italiani (nonché qualche anno fa la chiusura per molte ore del sito web ufficiale del Vaticano). Ma l'attività degli hacker può andare molto al di là di queste azioni. Secondo uno studio di Security defense agenda – Sda (il principale think tank specializzato nel settore), il 57% degli esperti mondiali di sicurezza informatica ritiene che sia in atto una corsa agli «armamenti» informatici in vista di una possibile «cyber-war». Una guerra i cui prodromi potrebbero già esistere (e ben prima dei conflitti russo-ucraino e Usa-Iran che pare tocchino, e moltissimo, l'universo cyber): secondo i media Usa, la Nato avrebbe segnalato che il numero di attacchi ai siti del Congresso e delle agenzie governative Usa, in patria e nel mondo, è cresciuto in maniera esponenziale, si parla addirittura di 1,6 milioni di attacchi al mese. Il tema riguarda anche la guerra cibernetica tra privati, capitolo molto rilevante tra le grandi corporation mondiali che, tra l'altro, da tempo investono miliardi di dollari all'anno per difendersi da attacchi informatici (anche assumendo hacker proprio come ha fatto Elon Musk). C'è da chiedersi quanto i riflessi di questa guerra, silente ma non per questo meno cruenta, influenzino l'atteggiamento di alcune grandi lobby economiche mondiali (quella delle industrie dell'high-tech o quella delle telecomunicazioni) nei confronti della rete e di una sua eventuale regolamentazione a livello internazionale.



Mauro Masi

*delegato italiano alla Proprietà intellettuale
Contatti: mauro.masi@bancafucino.it