PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4130 di Lunedì 27 novembre 2017

Come si è evoluto il mondo degli hackers?

Una breve carrellata, a partire dagli anni 90, con spunti sulle evoluzioni previste, possa essere utile per tutti i lettori coinvolti nel settore: in fondo, la storia è maestra di vita!

Chi scrive ha vissuto nel mondo dell'informatica sin da quando i computer lavoravano utilizzando schede perforate, come strumento di programmazione ed introduzione di dati. La costante evoluzione degli strumenti informatici e la crescita esponenziale dei tecnici, in grado di neutralizzare tali strumenti informatici, portavano, come naturale conseguenza, all'apparizione di soggetti ambigui, che all'inizio forse non era corretto chiamare criminali, ma che certamente avevano una visione distorta del mondo dell'informatica.

Il fatto che in paesi avanzati, come ad esempio la California, negli anni 80 non fosse obbligatorio segnalare alle forze dell'ordine reati di natura informatica fece sì che la percezione del problema non fosse sufficientemente accurata. La situazione però cambiò drammaticamente quando la California, primo paese al mondo, varò una legge che obbligava tutti i responsabili informatici a segnalare alle forze dell'ordine ogni attività di hackeraggio e violazione di sistemi informatici, in quanto reati.

Nei primi anni 90, il servizio segreto degli Stati Uniti lanciò una campagna mirata a identificare ed arrestare tutti i soggetti coinvolti in un crimine informatico, grazie una serie di raid presso abitazioni private, chiamata operazione Sundevil. L'operazione fu sviluppata in collaborazione con le polizie locali e esperti di telecomunicazioni ed informatica. I bersagli dell'operazione furono i famosi Bulletin board che venivano utilizzati per attività criminose, legate allo scambio di dati di carte di credito e di codici che permettevano di violare i sistemi telefonici.

Questa operazione di polizia richiamò l'attenzione degli organi di stampa e della popolazione, in generale, e mise in evidenza come i soggetti coinvolti erano perlopiù dei teenager della media borghesia, che operavano dalle loro abitazioni.

Questi giovani avevano sufficienti disponibilità economiche per acquistare strumenti informatici e avevano accesso ai modem, che a quei tempi erano lo strumento principale di connessione fra l'apparato informatico domestico e il resto del mondo. Il modem consentiva infatti il collegamento ad Internet e nascevano i primi gruppi coordinati di scambio di informazioni, non tutte di tipo legale.

Il clamore destinato da questa operazione di polizia portò a presentare, nel 1995, il film Hackers. Il protagonista era un teenager che era stato individuato dagli agenti federali, mentre operava nella sua camera da letto, in una abitazione di periferia, dove uno dei suoi floppy disk, utilizzato per attività illegali, era nascosto. Il film rappresentò anche altri aspetti della cultura degli hacker, ad esempio l'attività volta a violare le reti telefonici, per poter fare telefonate gratuite, nonché l'abitudine diffusa degli hacker di scambiarsi informazioni tecniche che venivano estratte dai sistemi informativi di grande azienda.

In questo film per la prima volta veniva mostrato un libro, contenente queste notizie, chiamato Crayola.

Oggi molti degli hackers degli anni 90 sono diventati esperti di sicurezza delle informazioni e sono pagati profumatamente da varie aziende per proteggere i propri sistemi informativi. Uno dei più celebri personaggi è certamente Kevin Mitnick, che ho scritto un libro che raccomando a tutti i lettori di leggere.

Nel frattempo la esplosione esponenziale del mondo delle comunicazioni e la disponibilità di strumenti informatici sempre più potenti, sempre più economici è sempre più compatti creava un nuovo scenario operativo, che modificava lo stereotipo dell'hacker, trasformandolo in un soggetto con una cultura, età e profilo sociale completamente diverso.

L'attività degli hacker è stata resa anche più difficile dalla introduzione graduale di sistemi di protezione molto più efficaci, rispetto a quelli disponibili negli anni 80.

Ecco la ragione per la quale oggi il mondo degli hacker è cambiato in maniera significativa, raggiungendo un livello di professionalità, per così dire, molto più elevato. A parte i gruppi di hackers che sono motivati da ragioni sociopolitiche, sono nate delle associazioni di hacker di elevato livello, che utilizzano personale informatico di altrettanto alto livello.

L'ormai famoso ransomware WannaCry, che ha colpito innumerevoli sistemi informatici a partire dal maggio 2017, è stato sviluppato da specialisti utilizzando strumenti informatici, che erano stati messi a punto dalla national security agency al fine di proteggere la sicurezza nazionale, ma che erano stati ri-configurati per utilizzi illeciti.

Un altro aspetto che si è evidenziato negli ultimi tempi è legato ad attività criminose che hanno origine completamente diversa, rispetto al ritorno economico.

Ad esempio, uno studente ha attaccato il sistema informativo dell'università in cui lavorava, perché riteneva che l'università non lo avesse valutato correttamente. In un altro caso, un dipendente che era stato allontanato da un'azienda attaccò il sistema informatico della sua azienda, come vendetta per il suo licenziamento.

In questo caso è evidente che l'attacco non nasce da un gruppo di criminali specializzati, ma da persone con livello di conoscenze informatiche medie, motivate da ragioni personali.

Che ormai l'attività degli hacker abbia raggiunto un livello quasi di pubblica accettazione è confermato dal fatto che ogni anno, a Las Vegas, si tiene la ormai famosissima Black hat convention, nella quale esperti informatici mettono in evidenza le debolezze di molti sistemi informatici. Appare del tutto evidente che alcune debolezze vengono pubblicamente illustrate, mentre altre debolezze vengono tenute nascoste e potrebbero essere utilizzate in modo illecito.

La pubblica dimostrazione nella quale un hacker, non animato da intenti criminosi, ma da intenti dimostrativi, dimostrò come poteva prendere il controllo di una autovettura ad elevata componente informatica, neutralizzando i comandi del guidatore e pilotando la vettura dall'esterno, è stato un esempio per il quale ancora oggi una grande casa automobilistica trema nel ricordo!

Dall'altro canto, i responsabili della sicurezza informatica hanno cominciato a valutare con estrema serietà questi scenari operativi e hanno oggi a disposizione strumenti tecnici ed economici, sicuramente assai più avanzati rispetto a quelli disponibili qualche tempo fa.

Chi scrive ha recentemente partecipato ad una conferenza, nella quale sono stati illustrati i sistemi di controllo puntuale dell'intera architettura informatica aziendale, in grado di mettere in evidenza in tempo reale tutt'una serie di parametri, che potrebbero essere ricondotti a situazioni se non illecite, perlomeno di rischio.

L'eccessivo utilizzo di alcuni strumenti informatici, l'eccessiva frequenza degli accessi alla rete, la ripetizione di tentativi di accesso non autorizzato e simili sono indicatori che devono far suonare subito i campanelli di allarme dei responsabili della sicurezza informatica.

Ciò non toglie che spesso, nella corsa fra la guardia e ladro, il ladro sia avanti e la guardia faccia una certa fatica nel cercare di raggiungerlo. D'altro canto, ogni volta che si ha notizia di un attacco, perpetrato o tentato, i responsabili della sicurezza informatica acquisiscono una migliore conoscenza dei punti deboli dei sistemi informativi e possono meglio identificare le aree, dove esistono vulnerabilità che possono essere messe sotto controllo.

Anche lo sviluppo di normative di livello europeo e mondiale, come le norme EN ed ISO, hanno aiutato nello stabilire dei parametri di riferimento oggettivi, afferenti alla sicurezza dei sistemi informativi, che possono essere valutati da entità terze, dotate delle appropriate competenze.

Adalberto Biasiotti
