AFFARI TECNICI

Social Engineering, la nuova frontiera del Cybercrime

APPROFONDIMENTI Francesco Viafora 23/11/2021 Stampa Email

Nell'immaginario collettivo l'hacker si trova in una stanza buia, tra videogiochi e gadget da nerd, mentre naviga nel dark web cercando di sferrare un nuovo attacco informatico capace di salvare il mondo. Anche se serie e film come Matrix hanno attribuito, dagli anni 90 in poi, agli hacker un alone quasi mistico, assegnandogli un ruolo di redenzione collettiva, nella realtà quotidiana gli attacchi informatici sono diventati una vera e propria emergenza e, come è naturale che sia, non c'è crimine senza vittime.

I numeri del cybercrime sono a dir poco impressionanti: sono infatti quantificabili a 6 trilioni di dollari le perdite collettive mondiali del 2021 dovute a forme di crimini informatici, gli attacchi, inoltre, si moltiplicano ovunque, nella sola Europa sono diventati il 25% del totale, e valgono circa il 6% del Pil mondiale e 3 volte il Pil italiano di un anno.

Il crimine informatico rappresenta un business che rende molto più del traffico di cocaina il cui valore è quantificabile attorno agli 820 milioni di dollari annui, e fa entrare nelle casse delle organizzazioni criminali, oltre che denaro, tecnologie e dati sensibili capaci di modificare, spesso, alcuni assetti sociali e politici. Gli obiettivi sono, infatti, sempre più differenziati e, se il cyber spionaggio è in netto calo, crescono altri tipi di attacchi: da gennaio a giugno 2021 il cyber crime ha investito trasporti e stoccaggio +108,7%, servizi professionali, scientifici e tecnici, +85,2% e informazione e multimedia +65,2%, seguite da commercio all'ingrosso e dettaglio+61,3% e produzione manifatturiera, +46,9%. Aumentano anche, seppur in maniera minore, gli attacchi verso le categorie energia e servizi pubblici +46,2%, settore pubblico +39,2%, arti e intrattenimento +36,8% e sanità +18,8%.

La percezione che si ha dei rischi legati agli attacchi cyber è ancora molto blanda, rendendo ancora più facile penetrare nelle tante falle che si aprono nei computer e nelle persone. Il rischio reale è molto più forte del rischio percepito, e spesso alcune distrazioni possono essere fatali per la perdita di migliaia di dati sensibili e password.

Se fino a qualche anno fa la maggior parte degli attacchi era sferrata contro le macchine e gli hardware, nella evoluzione delle tattiche di hacking legata alla difficoltà di penetrare codici,

INTERVISTE

Margiotta: "L'osmosi di risorse tra Fondazione e Centro Studi uno dei punti di forza del nostro sistema"
di Antonio Felici

Zambrano: "Dai professionisti tecnici un contributo reale per il rilancio del Paese"
di Antonio Felici

DIAMO I NUMERI

algoritmi e sistemi di sicurezza informatica sempre più complessi, la nuova frontiera del cyber crime prende il nome di Social Engineering e ha come obiettivo, non tanto la macchina, quanto l'essere umano e la sua psicologia.

La psicologia umana è infatti molto più vulnerabile di qualsiasi macchina e presenta molte più componenti emotive su cui è possibile intervenire: distrazione, paura, avidità, urgenza sono alcune delle reazioni emotive su cui il social engineering basa la sua fortuna. Esso infatti non è solamente una forma di manipolazione psicologica, ma è una vera e propria forma di capitale sociale codificato in sapere scientifico che accumula informazioni e know how per hackerare psicologicamente l' essere umano e rubare i dati dal suo computer o dalla sua rete.

La cyber sicurezza e altre iniziative sono state recentemente oggetto di una serie di webinar organizzati dalla Fondazione del Consiglio Nazionale ingegneri sulla cyber security, webinar nati con l'obiettivo di sensibilizzare il mondo dei professionisti verso i temi della sicurezza informatica.

Le nuove frontiere del cyber crimine non risparmiano nessuno, e bisogna essere sempre informati e preparati a fronteggiare gli attacchi. L'ingegneria sociale ha infatti anche scalzato le forme di hacking classiche; secondo le recenti statistiche oltre il 55% degli attacchi informatici avvenuti nel 2021 si è basato su tecniche di ingegneria sociale che sta diventando, anno dopo anno, una vera propria emergenza per aziende e istituzioni che si vedono chiedere riscatti esorbitanti, molto spesso pagati, per non vedere diffusi o distrutti i propri dati.

EDITORIALI

Il senso del Paese per i Superbonus 110%
di Francesco Estrafallaces

INPGI: cronaca di una morte annunciata
di Antonio Felici

TEMI

superbonus
congresso 65
Pnrr
equocompenso
assicurazioneprofessionale

BREVI

"Ing4Future green", incontro divulgativo a libera partecipazione

Modalità per l'istituzione degli elenchi dei professionisti per il Pnrr