MASTER UNIVERSITARIO di II Livello

in

HOMELAND SECURITY

Università Campus Bio-Medico – Roma

Consorzio NITEL

Anno accademico 2015/2016

Divulgazione Coordinata e Responsabile delle Vulnerabilità Informatiche

Tutor aziendale: Ing. Elena Agresti

Candidato: Dott. Michele Gallante

ABSTRACT

Nel corso degli ultimi anni c'è stato uno sviluppo vertiginoso della tecnologia che ha portato la società a diventare sempre più interconnessa e dipendente dai nuovi strumenti digitali. La velocità con cui si scambiano le informazioni, dovuta principalmente al crescente utilizzo di internet, che permette di raggiungere ogni parte del globo in una frazione di secondo, non è ancora supportata da un'adeguata sicurezza dei dispositivi che interagiscono con questo mondo virtuale. Quindi, nell'era dell'IoT (*Internet of Things*) dove ogni oggetto è connesso alla rete, è difficile anche per le organizzazioni più scrupolose, che attuano politiche di sicurezza all'avanguardia, azzerare il rischio di essere attaccati da criminali informatici con l'intento di trovare una debolezza nel sistema analizzato. Per queste ragioni, e data l'influenza che il mondo cyber sta avendo sempre più sulla vita reale, si auspica una collaborazione internazionale tra governi sovrani, organizzazioni private e portatori di interessi pubblici per arginare il fenomeno del cyber-crime.

L'elaborato tratta un metodo particolare di divulgazione delle vulnerabilità informatiche, le quali se sfruttate da un cyber criminale possono mettere a repentaglio la sicurezza di un'organizzazione e i diritti del privato cittadino. Dopo un'analisi sul contesto globale di riferimento, che evidenzia le problematiche del momento storico che stiamo vivendo, si passa in esame l'iniziativa Olandese sulla divulgazione coordinata e responsabile delle vulnerabilità informatiche. Il progetto denominato "Manifesto", attuato con un' insolita partnership Pubblico-Privato, si prefigge lo scopo di rendere più sicuri i sistemi informatici delle infrastrutture aderenti, attraverso una Policy comune che permette agli "*Ethical Hackers*" che trovano delle debolezze in un sistema informatico, di avere un contatto diretto con l'organizzazione interessata, garantendogli inoltre di non essere perseguiti per legge e addirittura di essere ricompensati (in modo discrezionale anche solamente simbolico).

Verrà, inoltre, fatto un excursus sul sistema giuridico italiano, principalmente sulle leggi in materia di crimini informatici e sulle convenzioni di carattere internazionale che disciplinano l'ampia materia in questione. Il fine è quello di comprendere come una politica di divulgazione responsabile possa insinuarsi all'interno del nostro sistema legale, poiché una policy (come quella olandese) rimane sempre una "comunità d'intenti" e non potrà mai sovrastare la legislazione nazionale con tutte le sue prerogative. Proprio in quest'ottica sarà analizzato il testo dell''articolo 615-ter del Codice Penale, riguardante "Accesso abusivo ad un sistema informatico" e i vari articoli che disciplinano il danneggiamento informatico (artt. 635-bis-ter-quater-quinquies c.p.).

In conclusione, viene presentata la proposta di una tavola rotonda tra organizzazioni private ed enti pubblici per esportare questa iniziativa anche nel nostro Paese. Le continue minacce alle quali siamo esposti

potranno essere mitigate unicamente con un'intensa cooperazione e coesione tra le parti interessate e con una condivisione di informazioni che dal lato difesa sembra essere non ancora adeguata.