Cyber security and ubiquity. An approach human-centric.

ABSTRACT

Antonio Colella
Ph.D. in Informatics and Information Engineering XV N.S.
Tutor: *Alfredo De Santis*

Le recenti violazioni della sicurezza hanno dimostrato che ogni attacco inizia con il coinvolgimento degli utenti e continua con lo sfruttamento di bug tecnologici.

In quasi tutti i casi, senza la collaborazione umana, cosciente e inconsapevole, sarebbe davvero difficile raggiungere l'obiettivo criminale. Il nostro approccio ha principalmente tre caratteristiche:

• centralità del fattore umano;

• la capacità flessibilità allo scenario da proteggere;

• adattamento dinamico alle minacce esterne e interne.

Il primo passo consiste nell'individuazione di un insieme di attributi da utilizzare per la costruzione di un sistema di sicurezza conforme a un determinato contesto, superando la strategia dei paradigmi preesistenti (CIA e simili). Più precisamente, in questa tesi ci concentriamo sull'idea che i membri della società devono acquisire conoscenze e esperienze sufficienti per evitare le conseguenze delle limitazioni delle soluzioni tecniche. Ciò ci ha portato verso un modello integrato basato su un approccio culturale in cui la fiducia e la compartecizione all'implementazione del sistema di sicurezza sono il punto focale. Questo modello implica che le soluzioni tecnologiche separate dall'ambiente circostante sono completamente inadeguate. I fattori sociali, organizzativi e psicologici devono essere considerati ad ugual maniera di quelli tecnici quando si implementa la sicurezza all'interno di un'organizzazione. Le combinazioni tra fattori sociali, fattori tecnologici, fiducia, cooperazione, cultura, motivazione e modelli organizzativi vanno armonizzati in un unico sistema. Abbiamo analizzato la fiducia in un ambiente di sicurezza e come questa alimenta la componente razionale, utilizzando informazioni basate sull'esperienza considerando, anche, gli elementi irrazionale, il cosiddetto "salto di fede" fatto di puro istinto, ovvero, senza alcuna logica. Abbiamo scoperto che la fiducia e il rischio sono due concetti inscindibili il cui legame è sostenuto sia da caratteri razionali che irrazionali. Quindi, ci siamo concentrati su un approccio alla gestione del rischio che, considerando il carattere olistico del problema, al tempo stesso tiene conto dei rapporti di lavoro interni e delle relazioni tra le organizzazioni. Inoltre, abbiamo chiarito perché le soluzioni tecnologiche da sole sono completamente inadeguate per garantire la sicurezza e perché i fattori sociali, organizzativi e psicologici devono essere considerati durante l'implementazione della sicurezza all'interno di un'organizzazione (security by design). Infatti, dobbiamo considerare come

la gente costruisce le comunità e deve tener conto di come le modalità di comunicazione influenzino le interazioni. Le considerazioni di cui sopra ci hanno guidato verso un modello che comprende l'approccio culturale in cui sia la fiducia che la compartecipazione al sistema di sicurezza hanno un ruolo molto importante. I comportamenti della sicurezza promossi dalle organizzazioni devono essere conseguiti perseguendo la motivazione e il desiderio come fattori culturali. Il modello considera gli elementi sociali come la parte più importante del sistema di sicurezza. La fiducia e la cooperazione aiutano a creare una cultura di sicurezza forte che funge da collante per il sistema di sicurezza delle informazioni. Alla fine della tesi, verrà applicata la fiducia e la cooperazione per introdurre un modello predittivo di valutazione del rischio di sicurezza informatica basato su reti bayesiane e metodologia ibrida (come definito da Francois-Xavier Aguessy). Le motivazioni che stanno alla base di questa tesi sono basate principalmente su due osservazioni. La prima osservazione è che la fiducia e la *co-partnership* implicano un pieno coinvolgimento di tutto lo stile di gestione. Per ottenere la cooperazione, il fattore umano deve essere il fulcro del modello di sicurezza.

La seconda osservazione è che un modello ibrido di valutazione del rischio può contribuire a fornire una solida base per la modellazione della sicurezza dinamica. L'esattezza di tale modello sarebbe correlata al numero di scenari disponibili e all'uso della capacità delle reti bayesiane di apprendere parametri dai dati.

La tesi è organizzata come di seguente:

• *Capitolo 2*: in questo capitolo abbiamo proposto un approccio al di là del paradigma CIA che ha principalmente tre caratteristiche: la centralità del fattore umano; la capacità di adattarsi allo scenario da proteggere; un adattamento dinamico alle minacce esterne e interne.

• *Capitolo 3*: in questo capitolo analizziamo l'ipotesi di un modello adattabile basato sulla consumerizzazione. L'idea fondamentale che i membri di un'organizzazione devono acquisire conoscenze ed esperienze sufficienti per evitare le conseguenze delle limitazioni delle soluzioni tecniche. Questa idea ci ha portati verso un modello integrato basato su un approccio culturale in cui la fiducia e la cooperazione con il sistema di sicurezza sono i punti principali. Il nostro modello implica che le soluzioni tecnologiche separate dall'ambiente circostante siano completamente inadeguate.

• *Capitolo 4*: in questo capitolo si affronta la cultura sociale integrata alla cyber security.

• *Capitolo 5*: in questo ultimo capitolo proponiamo di migliorare la sicurezza informatica attraverso l'integrazione del sistema umano e proponiamo una valutazione dei rischi utilizzando le metodologie ibride.