Cyber Security e Human Factor: il vero tallone d'Achille della sicurezza informatica (di Marco Strano-2022)

Relazione al Congresso nazionale dell'A.I.C.A. Reggio Calabria, 27 ottobre 2022.

Mi chiamo Marco Strano e sono un Dirigente Psicologo della Polizia di Stato in quiescenza dal 2020 e attualmente senior consultant di un Dipartimento di Polizia nel sud della California. Mi sono occupato di cyber criminologia e cyber security a tempo pieno dal 1995 fino al 2005 e, in particolare, dal 2001 al 2005 ho diretto l'UACI (l'unità di analisi sui crimini informatici) della polizia postale e delle comunicazioni. In seguito ho continuato a occuparmi di Cyber Crime nell'ambito della consulenza aziendale sia in Italia che all'estero e ho continuato a fare ricerca soprattutto nell'ambito delle aziende.

Attualmente, nonostante l'attività di sicurezza informatica si sia molto evoluta sia in termini qualitativi ma anche in termini quantitativi questo per certi versi non ha contribuito a limitare i rischi. Il motivo è abbastanza banale: negli ultimi anni sono aumentati in maniera esponenziale le attività aziendali, di gestione della cosa pubblica e in generale della vita degli individui affidate a sistemi informatici.

L'accesso a internet l'utilizzo di smartphone e di computers e in generale le procedure affidate alle tecnologie digitali negli ultimi 20 anni sono aumentate a dismisura ed quindi chiaro che statisticamente sono aumentati anche i rischi di crimini informatici.

Anche il passaggio dall'identità fisica e documentale all'identità digitale per lo svolgimento di attività fondamentali nella vita dell'individuo e nelle procedure delle organizzazioni si sta progressivamente realizzando e questo offre ovviamente il fianco a un aumento degli illeciti informatici.

Non abbiamo a disposizione dei dati statistici attendibili sul numero reale degli attacchi informatici a singoli e a organizzazioni pubbliche e private. Solo una percentuale di tali illeciti viene infatti denunciata (perché le organizzazioni non vogliono quasi mai rendere pubbliche le loro vulnerabilità) e sovente le vittime degli attacchi non si rendono conto di averli subiti.

L'ambito del cybercrime dove abbiamo la possibilità di avere a disposizione dei dati più attendibili è quello delle truffe e delle frodi dove il volume totale sembra essere notevolmente aumentato negli ultimi anni.

È mia opinione che il fattore umano rappresenti ancora l'elemento cardine della sicurezza informatica e il suo studio deve quindi necessariamente affiancarsi allo sviluppo delle tecnologie e delle procedure di sicurezza.

L'elemento primario nel fattore umano legato alla Cyber-sicurezza, è ovviamente quello che viene chiamato tecnicamente "percezione del rischio". Maggiore o minore percezione del rischio fa sì che l'utente di tecnologie informatiche adotti un meno di comportamenti sicuri, sia nell'ambito delle organizzazioni che a livello del singolo utente.

La percezione del rischio di attacco informatico è un elemento che degli psicologi appositamente addestrati sono in grado di misurare con degli strumenti analitici tipici della loro professione (tests, interviste, osservazione, ecc.). In altri contesti di rischio, e mi riferisco

per esempio alle problematiche di sicurezza del lavoro nei cantieri, abitualmente vengono condotte ricerche o attività di prevenzione legati proprio alla percezione del rischio.

Mentre, per quanto riguarda i rischi nella sicurezza informatica, dove i rischi sono ovviamente legati alla possibilità di subire un danno per un illecito, le valutazioni sulla percezione del rischio negli utenti e nelle organizzazioni sono purtroppo ancora un'attività residuale nei percorsi di messa in sicurezza.

Quello che sembra essere (storicamente) più avanti rispetto ad altri ambiti è probabilmente il settore bancario che ha nella sua cultura organizzativa e nella sua cultura d'impresa il fattore sicurezza molto radicato.

Un altro settore che è storicamente più avanzato degli altri è quello militare dove il concetto di compartimentazione interna delle informazioni (per evitare gli attacchi insiders) ottenuto adottando una specifica formazione ed efficaci procedure di sicurezza anche nel flusso interno di informazioni tra componenti dell'organizzazione è un qualcosa che è da sempre fortemente radicato nella sua cultura.

Ma altri comparti aziendali sembrano invece ancora essere un po' indietro rispetto al concetto del fattore umano nella cyber-security.

Le organizzazioni che vogliono adottare contromisure efficaci per evitare illeciti nei contesti digitali non devono quindi implementare solo le contromisure che vengono dette tecnicamente "difese perimetrali" vale a dire tecnologie per evitare che qualcuno dall'esterno di un'organizzazione riesca ad introdursi nel loro sistema telematico (quello che noi tutti conosciamo come attività di hacking) ma devono contemporaneamente migliorare la cultura della sicurezza (security awareness) delle persone che operano all'interno dell'organizzazione e naturalmente le procedure di sicurezza, prendendo esempio da quei comparti pubblici e privati che sono più avanti degli altri (comparto militare e comparto bancario).

CYBERCRIME E INVESTIGAZIONI

Sul versante investigativo la specializzazione di reparti investigativi o di magistrati diventerà sempre più anacronistica. Entro una certa un certo numero di anni probabilmente non esisterà più la polizia postale e delle comunicazioni o la sezione reati telematici dell'arma dei Carabinieri e della Guardia di Finanza perché in ogni forma di crimine sarà presente qualcosa di digitale, di informatico per cui tutte le forze di polizia, compresa la Stazione Carabinieri più remota o il Commissariato di Polizia più "periferico", dovranno necessariamente essere in grado di mettere il naso in qualche illecito che a che fare con le tecnologie digitali perché il mondo diventerà così digitale nei prossimi anni che sarà impossibile ragionare delimitando mondi reali e mondi virtuali. Ci troveremo di fronte a un unico mondo con componenti reali e componenti virtuali fortemente interconnessi.

CRIMINAL PROFILING E CYBERCRIME

Nel profilo criminale tipico di coloro che fanno degli attacchi informatici c'è stata una modifica negli ultimi anni. Conoscere il profilo di chi fa gli attacchi è fondamentale a mio avviso per organizzare delle contromisure efficaci. Solamente conoscendo il comportamento e il profilo di chi ti può attaccare possiamo organizzare delle difese realmente efficaci.

Nell'ambito della cyber-criminologia gli attaccanti normalmente rientrano in due macro categorie: gli outsider e gli insider, vale a dire chi attacca una organizzazione o un singolo individuo dall'esterno (i famosi hackers) o chi invece l'attacco lo fa dall'interno perché è un membro dell'organizzazione oppure una persona che vive vicino al singolo individuo che viene attaccato.

Nel profiling una importante tipologia/classificazione riguarda poi il livello di competenza criminale di colui che attacca e qui e normalmente ci sono due macro categorie: i professionisti (gli esperti) e i dilettanti che hanno scarse competenze ma che comunque possono riuscire comunque a provocare dei danni.

Quindi il profilo che è possibile realizzare rispetto a un cybercriminale è primariamente un profilo che considera il ruolo nell'organizzazione (interno/esterno) e il livello di competenza tecno-criminale. All'interno delle macro categorie poi ci sono infinite sfumature naturalmente.

Riguardo il profilo di personalità dell'attaccante, abbiamo attualmente in corso una ricerca sul campo (in città universitarie statunitensi) che utilizzando interviste semistrutturate a giovani hackers, sta cercando di delineare il profilo di questi giovani criminali.

PROFILO DI VULNERABILITA' DELLA VITTIMA

Un'altra tipologia di profilo che è possibile fare nell'ambito della cybersecurity riguarda le possibilità che un singolo individuo o un'organizzazione venga attaccata quindi una valutazione del rischio potenziale. Questo genere di profili considera normalmente le due variabili classiche che sono la vulnerabilità del target e l'appetibilità del target ma una valutazione basata su questi due elementi ovviamente potrebbe apparire banale e quindi vengono utilizzati degli altri fattori di analisi che servono per delineare l'andamento nel tempo del rischio.

La mia equipe di ricerca negli anni ha sviluppato dei modelli analitici predittivi in grado di valutare quali sono livelli di rischio di vittimizzazione da cybercrime per un'organizzazione e per un singolo individuo.

Per verificare la sicurezza di un'organizzazione da molti anni le società specializzate effettuano un vulnerability assessment che serve per individuare situazioni di rischio. Normalmente in queste verifiche intervengono diverse società specializzate in diverse aree di rischio che però sovente non comunicano tra loro. L'approccio progettato dallo scrivente inizialmente durante il periodo di servizio alla Polizia Postale e delle Comunicazioni e implementato poi in ambito civile attraverso un gruppo di ricerca, suggerisce invece un approccio integrato dove un unico gruppo di consulenti (coordinato) analizza contemporaneamente tutte le aree critiche di un'organizzazione. Un vulnerability assessment integrato è in grado di valutare quindi contemporaneamente gli elementi di rischio di intrusione fisica, informatica e psicologica all'interno dell'organizzazione da parte di soggetti esterni ostili o di insiders.

Il protocollo di ricerca da noi adottato per la messa a punto del nostro I.V.R.A (Integrated Vulnerability Risk Assessment) parte da un campione di aziende/organizzazioni e di singoli individui analizzando le situazioni in cui gli attacchi hanno avuto o meno successo e le caratteristiche organizzative, tecnologiche e psicologiche della vittima. Da questo genere di analisi emergono evidentemente gli elementi di appetibilità e vulnerabilità compatibili con il successo dell'azione illegale.

Il nostro I.V.R.A. è stato presentato per la prima volta (in versione beta) all'edizione 2014 di BAKUTEL, la prestigiosa convention sull'information technology che si svolge ogni anno in Azerbaijan ed è composto da diversi strumenti operativi per la valutazione e la prevenzione del rischio di attacchi informatici nelle organizzazioni pubbliche e private e nei singoli individui. Dopo più di 8 anni di sperimentazioni e di esperienze sul campo, questo metodo di analisi (I.V.R.A.) si è sviluppato ed è ora a disposizione di organizzazioni pubbliche e private. I costi dello strumento sono inoltre molto contenuti e i tempi di somministrazione sono molto rapidi (circa cinque giorni ogni 100 persone). Il protocollo di intervento prevede

una fase iniziale di misurazione/valutazione e una fase successiva di correzione delle vulnerabilità.

Il C.S.L.S.G., il centro studi che presiedo, è uno dei più antichi d'Italia, fondato nel 1999 che continua a svolgere delle ricerche sulla sicurezza informatica, soprattutto quella legata al mondo aziendale ed è a disposizione per qualsiasi tipo di approfondimento nell'ambito del fattore umano della sicurezza informatica delle organizzazioni di singoli individui.