Telematic Journal of Clinical Criminology
www.criminologia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

Articolo pubblicato su ICT Security - Febbraio 2004

L'importanza del fattore umano nelle policy di sicurezza informatica

Di Roberta Bruzzone[1]

Introduzione

Dietro ad ogni tecnologia di sicurezza c'è una persona che deve utilizzarla. Ogni sofisticato sistema di sicurezza fisico e logico può essere quindi vanificato da utilizzatori non addestrati o poco convinti della sua necessità. Alcuni comportamenti criminali commessi da dipendenti (insiders) sono inoltre legati ad una ridotta percezione del crimine dovuta in special modo alla "tecnomediazione" operata dal computer. Le ricerche psicologiche più avanzate sul computer crime hanno infatti evidenziato delle modifiche percettive indotte dalla tecnologia digitale, soprattutto quando tale tecnologia media una relazione tra l'autore di un crimine e la sua vittima: operare un illecito senza spostarsi dalla propria "familiare e rassicurante" postazione di lavoro e soprattutto senza guardare negli occhi la propria vittima rappresenta uno scenario meno ansiogeno per l'individuo. La Psicologia umana è quindi un fattore che deve essere considerato da chi progetta e gestisce la sicurezza informatica e, nei moderni "*vulnerability assessment*", dovrebbe trovare posto anche un settore di analisi dedicato al fattore umano.

Psicologia e sicurezza

Nei contesti lavorativi più moderni e sviluppati la Psicologia ha già da diversi anni a che fare con le procedure di sicurezza. Specie negli USA e in Gran Bretagna *l'human factor* viene ad esempio particolarmente curato nel settore della sicurezza fisica delle persone sul luogo di lavoro. La funzione dello psicologo in tali ambiti è quella di convincere le persone, al di là delle prescrizioni, ad attuare un comportamento sicuro, facendo leva anche sulla loro sfera motivazionale. Gli operai di alcuni cantieri di avanguardia vengono ad esempio sottoposti ad interventi psicologici (corsi di formazione, focus-groups, colloqui individuali) per instillare in loro l'abitudine all'uso di strumenti di protezione individuale e collettiva per ridurre gli infortuni; lavoratori che svolgono mansioni pericolose vengono addestrati al rispetto di regole di sicurezza sotto la supervisione di uno psicologo.
Sul versante della sicurezza informatica e della prevenzione del crimine le esperienze di ricerca e di intervento psicologico appaiono invece alquanto pionieristiche e sono riconducibili in Europa alle esperienze del Prof. Marco Strano e della sua equipe (in cui opera la scrivente) e in USA all'attività di un'equipe in stretto contatto scientifico con la prima e diretta dal Prof. Marc Rogers della Purdue University. In tale ambito i fattori maggiormente indagati sono la *percezione del crimine* (per la valutazione del rischio insiders) e la *percezione del rischio* di attacco (per la valutazione delle vulnerabilità dei sistemi di sicurezza legate al fattore umano).

Gli insiders e la percezione del crimine

Il computer crime, così come documentato dalla moderna letteratura specialistica (M. Strano 2000) risulta essere frutto di dinamiche complesse, strettamente legate ai processi di interazione dell'autore con le norme penali e sociali, con l'ambiente esterno, con la vittima e, in definitiva con il proprio Sé. Gli uomini, ovvero, intraprendono azioni illegali in base a una serie di informazioni che provengono dalla loro esperienza e dall'ambiente esterno (Rogers M., 2003), soprattutto dall'interazione con gli altri individui e con le norme (giuridiche e sociali) attinenti a tali azioni e tali informazioni vengono poi "processate" dalla loro mente che genera un processo decisionale in direzione (o meno) dell'illegalità. In tale ottica analizzare come le persone percepiscono e producono significato intorno ad un

[1] Psicologa e Criminologa, Vicepresidente International Crime Analysis Association (I.C.A.A.)

determinato comportamento criminale è assai importante poiché tale processo influenza in ultima analisi la progettazione e l'esecuzione del crimine. Alcuni dei fattori rilevanti nel "*criminal decision making*" sono solitamente i seguenti (M. Strano, 2003):

1. Percezione della gravità del comportamento
2. Stima dei rischi di essere scoperto
3. Stima dei rischi di essere denunciato
4. Percezione del danno procurato alla vittima
5. Paura della sanzione sociale
6. Paura della sanzione legale

I suddetti fattori possono essere misurati con appositi strumenti di indagine criminologica (M. Strano, 2001).

La percezione del rischio di attacco informatico

Il rispetto di una procedura di sicurezza da parte delle persone si basa su una serie di schemi cognitivi ed atteggiamenti che costituiscono la percezione di rischio:

1. atteggiamenti diffusi rispetto all'utilità della procedura
2. conoscenza dei rischi reali di attacco
3. conoscenza e timore delle sanzioni derivanti dal non rispetto della procedura
4. stima dei danni provocabili dall'attacco informatico
5. consapevolezza di poter costituire un target per l'attaccante

Oltre a tali fattori occorre ovviamente considerare anche le condizioni di ergonomia della procedura e l'entità del rallentamento del processo lavorativo (alcune misure di sicurezza molto lunghe e complesse possono rappresentare un fastidio eccessivo per l'operatore)

Una ricerca sul rischio insiders e outsider basato sul fattore umano.

E' interessante citare un progetto di ricerca scientifica sulla percezione del crimine informatico e sulla cultura della sicurezza informatica condotto dall'I.C.A.A.[2] in collaborazione con la S.I.P.TECH[3], con il Servizio Polizia Postale e delle Comunicazioni[4], con la Purdue University (USA)[5] e con alcune Società di consulenza nel settore della sicurezza informatica[6]. L'obbiettivo della ricerca è la misurazione dei livelli di consapevolezza del crimine e della percezione del rischio di attacco informatico in campioni di lavoratori di aziende private e della Pubblica Amministrazione, di vario livello gerarchico. Lo studio utilizza un assessment sul computer crime nelle organizzazioni centrato sul fattore umano P.R.A. (Psychological Risk Assessment) che comprende due questionari strutturati anonimi (WC.P.Q. e C.R.P.Q.) realizzati dall'ICAA e una griglia per la rilevazione dei casi (W.C.A.G.). L'assessment è in corso di somministrazione in Italia e in USA e può essere richiesto direttamente all'associazione ICAA.

Gli strumenti dell'assessment P.R.A

W.C.P.Q. (**W**orkplace **C**omputer crime **P**sychology **Q**uestionnaire). Il questionario (32 items) è centrato sul fenomeno "insiders" ed analizza la consapevolezza dei lavoratori intervistati rispetto a comportamenti illegali effettuati nell'ambito dell'informatica. Lo strumento indaga ad esempio il modo in cui le persone interpretano e valutano diverse attività illegali connesse all'uso del computer in azienda. Viene misurata la minore o maggiore consapevolezza della gravità dell'atto, le aspettative di reazione sociale, il timore della sanzione, la stima delle possibilità di essere scoperto e denunciato, il livello di conoscenza delle leggi sullo specifico argomento ed altri atteggiamenti e

[2] International Crime Analysis Association, un'associazione no-profit dedicata alla divulgazione della ricerca scientifica,
[3] Società Italiana di Psicotecnologie e Clinica dei Nuovi Media
[4] UACI (Unità di Analisi sui Crimini Informatici)
[5] Prof. Marc Rogers
[6] Symantec

schemi cognitivi che entrano abitualmente in gioco quando un individuo materializza l'idea di agire in maniera illegale. I risultati del questionario WCPQ dell'ICAA suggeriscono direttamente, le variabili su cui è possibile intervenire per tentare di ridurre l'incidenza del fenomeno attraverso percorsi di formazione e sensibilizzazione mirati alla cultura della legalità.

C.R.P.Q. (**C**omputer crime **R**isk **P**erception **Q**uestionnaire). Il questionario valuta il livello di percezione del rischio di attacco informatico (interno ed esterno) e la diffusione di atteggiamenti e comportamenti potenzialmente facilitanti gli attacchi. La somministrazione di questo strumento è preceduta da una fase di osservazione dell'organizzazione al fine di individuare alcune esigenze specifiche. I ricercatori effettuano, prima dell'intervento, un breve colloquio con la dirigenza aziendale e con i responsabili della sicurezza per rilevare alcuni possibili "punti deboli" da misurare. Il questionario CRPQ contiene infatti un'area generale adatta a tutte le organizzazioni analizzate (18 domande) e un'area specifica (4-5 domande) che vengono tarate sulle caratteristiche produttive ed organizzative dell'azienda. Lo strumento consente di evidenziare aree di rischio per quanto riguarda il fattore umano nell'ambito del processo di sicurezza informatica delle organizzazioni pubbliche e private.

Il tempo di somministrazione dei due strumenti è estremamente breve (circa 20 minuti) e l'analisi dei dati ottenuti consente la realizzazione di un *report* sullo stato della sicurezza della specifica organizzazione legato al "fattore umano" e di progettare un intervento correttivo basato su elementi di rischio realmente presenti nello specifico contesto di intervento.

W.C.A.G. (**W**orkplace **C**omputer crime **A**nalysis **G**rid). La griglia per la rilevazione dei casi acquisisce infine informazioni standardizzate (anonime) sul modus operandi di *outsiders* e *insiders* ed è destinata alla creazione di un data-base (on-line) di libera consultazione da parte degli addetti alla sicurezza in corso di realizzazione dall'ICAA.

La prevenzione psicologica del crimine: un intervento da professionisti

La produzione e la somministrazione di strumenti psicologici destinati alla misurazione della percezione del crimine e del rischio è un'attività estremamente complessa e delicata che deve necessariamente essere condotta da uno psicologo con una vasta esperienza nell'ambito della psicologia criminale. Operare in ambito aziendale su tali tematiche in maniera goffa o poco professionale può infatti ingenerare nei lavoratori una spiacevole sensazione di controllo e criminalizzazione (a ragione). L'argomento "illegalità" attiva inoltre notevoli resistenze e timori negli individui che, anche in un contesto di assoluta anonimità, tendono spesso a celare eventuali atteggiamenti non conformi alle regole. La competenza e la professionalità dello psicologo-criminologo in tale ambito sono legate proprio alla capacità di costruire uno strumento di indagine in grado di cogliere anche gli "indicatori secondari" e non manifesti degli atteggiamenti. E' inoltre necessario lenire le "resistenze" (anche inconscie) e i timori con un valido breefing pre-somministrazione. L'assoluta anonimità dello strumento completa infine i requisiti necessari. I risultati ottenuti dalla somministrazione dell'assessment psicologico dell'ICAA sono apparsi molto utili per la successiva progettazione di interventi correttivi mirati sulla specifica realtà aziendale, attuabili attraverso una formazione diffusa di tutto il personale o mediante un'azione di sensibilizzazione mirata da parte dei Dirigenti all'interno dei gruppi di lavoro.

Riferimenti bibliografici

www.criminologia.org
www.icaa-italia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

Galdieri P., Giustozzi C. Strano M, *Sicurezza e privacy in azienda*, Apogeo editore, Milano, 2001.
Rogers M., *Organized Computer Crime and More Sophisticated Security Controls: Which Came First the Chicken or the Egg?*, Dept. Of Psychology, University of Manitoba, 1999 –
Rogers, M. *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. Unpublished dissertation, 2001
Rogers M., Psychological *Theories of Crime and "Hacking"*, Department of Psychology, University of Manitoba, Telematic Journal of Clinical Criminology, www.criminologia.org , 2003
Strano M., Computer crime, Edizioni Apogeo, Milano, 2000
Strano M., *Il computer crime nelle aziende* in BYTE, gennaio 1999;
Strano M., Bruzzone R., *Il computer crime nelle aziende: gli insiders*, in: M. Strano (a cura di) Manuale di Criminologia Clinica, See Edizioni, Firenze, 2003