



With financial support from the AGIS Programme  
European Commission - Directorate General Justice, Freedom and Security  
Contract nr. JAI/2004/AGIS/113 - December 2004

## ***Raggruppamento Carabinieri Investigazioni Scientifiche Reparto Investigazioni Scientifiche di Roma – Sezione Telematica***

**International Conference – Rome, May 23-24, 2005**

# L'aggiornamento continuo come fattore critico di successo: l'addestramento INeS.

*Cap. CC RTL Gianluigi Me  
Comando Generale (HQ) dell'Arma dei Carabinieri  
gme@carabinieri.it*

Il tempo di messa in commercio appesantisce enormemente l'ICT causando alcuni problemi ai professionisti della sicurezza e, di conseguenza agli investigatori di crimini informatici. Gli effetti più rilevanti di questo fenomeno, in termini di severità della minaccia, nella matrice tecnica/tecnologia:

Tecnologia / Tecnica d'attacco	NEW	OLD
NEW		
OLD		

Gli esempi sono:

- NEW/NEW: nuovi attacchi che fanno affidamento su nuove tecnologie (Bluesnarfing su Bluetooth dalla fine del 2003) ;
- NEW/OLD: Un tipico esempio di nuova tecnologia / vecchio attacco è fornito dallo spam di voce sull'IP, propriamente "Split" spam sulla telefonia Internet. Anche se VoIP è una tecnologia esistente da almeno 10 anni, nel 2004 grazie a più di 24 milioni di installazioni, ha superato le installazioni PSTN. Questa larga penetrazione nel mercato consente agli hacker di effettuare attacchi con un alto impatto sul livello del servizio, sulla confidenza dell'utilizzatore con la tecnologia e sull'immagine delle compagnie.
- OLD/NEW: Overflow dei numeri interi, attacchi day-zero.
- OLD/OLD: Falle nel software che danno luogo a nuove vulnerabilità e relativi attacchi (overflow del buffer)

Gli investigatori di crimini informatici devono fronteggiare tutti questi attacchi, inclusi i più nuovi. Inoltre, come evidenziato nella letteratura esistente, la qualità dei professionisti in crimini informatici influisce pesantemente sull'intera attività investigativa (ad esempio

sulla raccolta di prove informatiche), dovuto al fatto che un computer può essere successivamente utilizzato come mezzo per condurre o pianificare un crimine “non digitale”. Infatti,

1. La maggior parte delle funzioni di pay-off criminali ha un addebito di pena pari a  $\alpha_i \cdot r_i$   
dove
  - $\alpha_i$  è la probabilità di essere individuato dalle forze dell'ordine
  - $r_i$  è la pena associata al crimine.
2. La comunità virtuale influisce sul fattore  $\alpha_i$ : infatti, nelle reti di comunicazione, ad esempio, le tecniche di crittografia e di steganografia aumentano il costo dell'attacco da parte delle forze dell'ordine, aumentando la possibilità di sfuggire all'individuazione (abbassando  $\alpha_i$ ).
3. Il coefficiente  $\alpha_i$  ha 2 componenti:
  - Pr(Evento A): probabilità di essere individuato dalle forze dell'ordine
  - Pr(Evento B): probabilità di effettuare un grosso recupero di prove da parte delle forze dell'ordine.
4. Il coefficiente  $\alpha_i$  assumerà la seguente espressione:  
 $P(A,B)=\alpha_i = P(A) \cdot P(B|A)$   
ma  $P(B|A)$ 
  - è fortemente influenzata dalla competenza degli investigatori
  - quando il crimine è strettamente collegato a forti prove (ad esempio pedofilia) con probabilità  $\approx 1$

$$P(A,B)=\alpha_i = P(A)$$

Questo termine (più alto che nel caso generale) abbassa il profitto criminale. Per questo motivo, la principale azione per affrontare i crimini legati all'informatica (anche detti, i crimini digitali) è la formazione, rivolta a migliorare la qualità di ricerca e ad espandere lo spazio di ricerca. In particolare, la capacità di affrontare indagini informatiche può essere considerata come un'arma supplementare tra le ormai consolidate tecniche investigative: in questo modo, il ricercatore può scegliere lo strumento più efficace/efficiente, secondo il particolare contesto di ricerca di crimine. Dalle considerazioni precedenti circa l'obsolescenza rapida di conoscenza nel ICT, la forza di polizia Arma dei Carabinieri ha adottato il paradigma dell'apprendimento a lunga durata per addestrare nell'affrontare crimini ad alta tecnologia i militari diffusi in tutto il territorio italiano. Dopo un corso intensivo di 12 giorni (chiamato Investigazioni Elettroniche Speciali, InES), i militari vengono addestrati a distanza con gli aggiornati best practices, con l'accesso ad archivi di informazione ed a documenti avanzati sullo stato dell'arte, con un supporto tecnico in linea. Siccome questo è l'obiettivo primario da raggiungere, assieme ad alte prestazioni nei crimini associati a computer (ad esempio la raccolta di prove informatiche), ci si può aspettare un immediato ritorno dell'investimento, con un periodo di payback stimato in meno di un anno.

Infatti

- Costo per studente
    - insegnamento: 550 €
    - permessi di viaggio e alloggio: 750 €
  - Costo totale (approssimativo): 200 K€
- Si consideri che

- Costo dell'attività di consulenza media stimato (outsource): 5 K€
- Stimando 0.5 dell'attività di consulenza (per anno, per comando)

$$\text{ROI (primo anno)} = \frac{\text{Risparmio : } 112 \cdot 0.5 \cdot 5 \text{ k€}}{\text{Costi sostenuti: (200 k€)}} = 1.4$$

Questi risultati, verificati con il primo controllo annuale, confermano che questa azione è remuneratrice in meno di 1 anno, dal lato economico, mentre stiamo prevedendo l'indice di impatto sul crimine informatico mediante il succitato FAC.

Molti altri prodotti derivati relativi, i beni in genere immateriali (per esempio popolarità), rappresentano ulteriori vantaggi dell'azione.

## **RIFERIMENTI**

Eoghan Casey, Digital Evidence and computer crime, Academic Press 2001

Harlan Carvey, Windows Forensics and Incident Recovery, Addison Wesley, 2005

Merlin Dresher, The Mathematics of Games of Strategy, Dover, 1981