Politecnico di Milano

Facoltà di Ingegneria dell'Informazione
Corso di Laurea Specialistica in Ingegneria Informatica

Stefano Galli (matr. 674611), Ilaria Marzolla (matr. 654450)

Criminalità Informatica

Relazione per il corso di *Deontologia ed Etica delle Tecnologie dell'Informazione*
prof. Piercarlo Maggiolini

Anno Accademico 2004-2005

L'ottimista vede opportunità in ogni pericolo, il pessimista vede il pericolo in ogni opportunità

Winston Churchill

Indice

Capitolo 1

Introduzione

La globalizzazione delle comunicazioni ed il superamento dei tradizionali vincoli di spazio e tempo ci mostrano una realtà digitalizzata che è, nello stesso tempo, sia motivo di sviluppo, sia causa di debolezze strutturali con possibili ripercussioni negative sulla sicurezza pubblica.

Lo studio del computer crime è un settore della Criminologia dove si profilano rapidi cambiamenti di scenario e dove sembra manifestarsi con più insistenza l'esigenza di percorsi conoscitivi nuovi. Questo settore delinquenziale è legato all'influenza delle nuove tecnologie informatiche e telematiche sul sistema sociale e alle conseguenti contromisure.

L'impatto dell'information technology sull'uomo agisce infatti su tre dimensioni, poste su livelli diversi ma interagenti tra loro. La prima dimensione è quella sociale, strettamente legata all'aumento dell'allarme politico-istituzionale e alla produzione di un corpo normativo specifico.

La seconda dimensione è relativa alle organizzazioni ed è riferibile alla necessità da parte delle aziende e delle istituzioni di affrontare il problema del cyberspazio come proprietà privata, essendo esso divenuto il luogo di concentrazione di interessi economici ed elevati investimenti, oltre che lo spazio di interconnessione tra i vari comparti della Pubblica Amministrazione. In tale ambito si assiste infatti a un notevole sforzo per prevenire e contrastare azioni illegali attuate mediante tecnologie informatiche.

La terza dimensione del fenomeno infine, quella individuale, è soprattutto legata all'impatto dell'informatica sugli schemi cognitivi degli individui, e alla sua induzione di alterazioni percettive che possono interferire, a vario titolo, sui livelli di consapevolezza dei delinquenti durante le loro azioni criminali.

L'ingresso nell'era dell'ICT rappresenta quindi per gli studiosi del comportamento umano una fase di diffusione di una nuova modalità comunicativa, strettamente correlata alle tecnologie digitali. La cultura, le abitudini, la psicologia dei singoli individui e delle organizzazioni si trovano, a seguito di tale diffusione, "costrette" ad una sorta di ristrutturazione mentale che condurrà probabilmente entro breve tempo a vere e proprie mutazioni comportamentali stabili.

L'influenza del digitale sul crimine Attualmente l'information technology agisce sulla criminalità modificando forme delinquenziali classiche, introducendo forme criminali nuove e alterando i processi di percezione del crimine:

1. *Modifica di forme criminali tradizionali.* Il crimine, soprattutto quello professionale, si adatta a tutte le innovazioni che migliorano la sua efficienza, compreso quindi l'ICT. L'avvento di internet e dell'informatica ha così indotto delle modifiche di alcune forme criminali, già da tempo radicate nel tessuto sociale:

    - Furti di informazioni e spionaggio

- Truffe e frodi
- Gioco d'azzardo
- Prostituzione
- Traffici vari (armi, droga)
- Molestie, minacce
- Pedofilia (adescamento, pornografia)
- Criminalità organizzata (riciclaggio, comunicazioni)
- Terrorismo
- Proselitismo delle sette sataniche

2. *Nascita di nuovi crimini.* La diffusione dell'I.C.T. ha anche portato delle forme criminali nuove, in grado di articolarsi solamente all'interno dei nuovi sistemi di comunicazione digitale:

   - Cyberpedofilia (scambio di pedopornografia)
   - Cyberterrorismo
   - Hacking
   - Diffusione di virus informatici
   - Truffe telematiche via email
   - Spamming
   - Net-strike
   - Diffusione di informazioni illegali on-line (violenza, razzismo, esplosivi, droghe, sette sataniche, pedofilia ecc.)

3. *Le alterazioni nella percezione del crimine.* L'uomo, come tutte le altre specie del resto, si adatta continuamente alle modifiche dell'ambiente, fornendo delle risposte adattive che dopo un certo tempo si stabilizzano in caratteristiche strutturali. Si rileva ad esempio, talvolta, in alcuni soggetti osservati, una certa difficoltà nell'identificare il limite che separa la realtà dal virtuale o nella capacità di tornare velocemente in una situazione di realtà dopo una certa permanenza in un fase di virtualità, e tale difficoltà assume rilevanza in Criminologia in special modo nello studio della fase di percezione, distinzione e valutazione, da parte dell'autore di un crimine, degli effetti provocati con il proprio comportamento. L'uomo è ancora abituato ad ottenere un riscontro diretto delle sue azioni osservando modificazioni evidenti su oggetti tangibili, fisici, nonché sull'emotività dell'interlocutore e tale riscontro sembra risultare meno efficace quando è mediato da un messaggio di ritorno digitale che pur se in continua raffinazione, costituisce ancora una rappresentazione imperfetta. Pensiamo ad esempio a quanto la prova tangibile degli effetti negativi prodotti sulla vittima possa rappresentare un deterrente al crimine in soggetti dotati di un quadro morale ben strutturato e come la mediazione di uno spazio virtuale tra l'autore del crimine e la sua vittima possa invece attenuare la percezione di tali effetti.

La spiegazione del crimine in ottica digitale Le azioni criminali, così come documentato dalla moderna letteratura specialistica, risultano 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. I crimini vengono infatti costruiti, elaborati (e spesso impediti) da un processo di pensiero che molto si basa sull'anticipazione mentale degli effetti del proprio comportamento.

Gli uomini, infatti, orientano il proprio comportamento in base a una serie di informazioni che provengono dalla loro esperienza e dall'ambiente esterno, soprattutto dall'interazione con gli altri individui e con le norme (giuridiche e sociali) attinenti a tale comportamento.

È possibile insomma definire il criminale, ma anche la persona comune, come "*social cognizer*", vale a dire una persona che seleziona, organizza le informazioni provenienti dal mondo esterno, costruendosi in questo modo rappresentazioni del contesto in cui vive.

Analizzando il crimine informatico in funzione delle interazioni, si può quindi avanzare una definizione di computer crime come tutti quei casi in cui "*il computer si interpone tra l'autore del crimine e la vittima o comunque rappresenta lo strumento principale per eseguire una determinata azione criminale*", sottolineando la sua capacità di alterare ad esempio la percezione di gravità dell'azione criminale, la percezione della vittima, la stima dei rischi di essere scoperto e catturato.

Ad esempio, in alcuni casi di pedofilia online, le modalità di approccio dei pedofili nelle chatline evidenziano una netta sottostima dei rischi di essere scoperti rispetto alle modalità di approccio classico del mondo reale. Tale circostanza potrebbe costituire un fattore disinibente per taluni soggetti e in un certo senso una facilitazione per il passaggio all'atto.

Uno studio sulle truffe condotte con le carte di credito ha evidenziato una maggiore "disponibilità al crimine" da parte di soggetti completamente estranei alle dinamiche criminali classiche nel momento in cui vengono proiettati in un contesto digitale laddove la *scena criminis* si trasferisce tra monitor e tastiera.

Le esperienze di ricerca sugli hackers, hanno spesso posto in evidenza la frequente percezione "ludica", e comunque a scopo di ricerca, delle intrusioni clandestine.

La nascita di una nuova forma di terrorismo che sfrutta le nuove tecnologie di informazione, già definito "cyberterrorismo", comincia a proporre le sue dottrine, le sue logiche e le sue azioni in ambito virtuale, selezionando probabilmente nuove figure di terroristi lontane dallo stereotipo del "duro" degli anni di piombo. Insomma alcuni comportamenti illegali "tecnomediati" possono essere effettuati da soggetti che difficilmente eseguirebbero azioni in ambito non digitale, come ad esempio:

- pedofili che non avrebbero il coraggio di adescare un bambino per strada
- terroristi psicologicamente non adatti ad azioni militari
- truffatori che non reggerebbero l'impatto con la vittima "faccia a faccia"
- impiegati scontenti che non avrebbero il coraggio di compiere azioni di sabotaggio tradizionali nella propria azienda
- ladri di informazioni che non sarebbero in grado di introdursi in un ufficio che contiene informazioni da sottrarre

L'uso delle tecnologie dell'informazione, oltre ad abbattere eventuali barriere di natura psicologica, come detto fino ad ora, si è rivelato un catalizzatore per attività delittuose: è evidente, infatti,

come organizzazioni criminali e terroristiche abbiano tratto giovamento dalle possibilità offerte dalla rete per migliorare la loro efficienza operativa. Ed infine la rete stessa, data l'interconnessione e l'interdipenza dei vari utenti che si avvalgono di sistemi informatizzati per la loro attività, costituisce uno strumento offensivo efficace per colpire gli obiettivi di volta in volta individuati.

Capitolo 2

Classificazione ed analisi dei crimini

Un computer, collegato in rete o in stand alone, può essere il bersaglio di un reato ed in questo caso l'obiettivo del malintenzionato si ravvisa nel sottrarre o distruggere le informazioni contenute nella memoria dello stesso. È il caso, ad esempio, del malintenzionato che penetra in un sistema informatico cambiando la homepage del sito vittima realizzando il cosiddetto *defacement*.

Può costituire un mezzo per la commissione di reati, ad esempio nel caso di chi utilizzi il computer per la realizzazione di frodi o furti. Significativo è il caso dell'impiegato di banca che, utilizzando il computer di lavoro, prelevi dai conti correnti dei clienti una piccola somma di denaro per depositarla nel suo conto corrente (fenomeno noto come *salami slice*) o dell'utente della rete internet che divulghi notizie infamanti ed ingiuriose.

La rete Internet può infine essere utilizzata in modo del tutto lecito da soggetti criminali o terroristi che ne sfruttano le potenzialità per migliorare l'efficacia della propria azione.

Le organizzazioni criminali o terroristiche tendono ad utilizzare la rete internet come valore aggiunto alla propria efficienza organizzativa. Esempi significativi possono essere il riciclaggio, lo scambio di informazioni, evitando dinamiche comunicative pericolose rappresentate dal contatto diretto.

L'ICT rappresenta peraltro il tessuto connettivo di tutte le attività istituzionali, economiche, sociali dei paesi moderni, nei quali ogni processo di vita della collettività, da quello più semplice come, ad esempio, la gestione della contabilità familiare, a quello più complesso, si pensi alla gestione del traffico aereo, è informatizzato.

Si è venuto pertanto a creare in tutto il pianeta un sistema estremamente complesso e articolato, organizzato in strutture critiche informatizzate, interconnesse ed interdipendenti, che prescinde dai confini nazionali, e dalle quali dipende la sopravvivenza stessa di gran parte della popolazione mondiale.

Alla luce di quanto visto, possiamo suddividere i cybercrimes in tre macrocategorie:

1. **informatici**, ovvero quelle azioni il cui bersaglio primario sono sistemi hardware/software, le basi di dati, e in generale le informazioni. Lo scopo di questo genere di attacchi può essere di varia natura: furto di segreti industriali e informazioni riservate; danneggiamento di impianti, servizi e sistemi di business; intrusione in reti protette

2. **sociali**, atti che colpiscono il tessuto sociale sfruttando mezzi tecnologici. Il bersaglio può essere la singola persona, come nel caso della pedofilia; una minoranza, quando ad agire sono sette sataniche e gruppi razzisti; o intere popopolazioni, mira dei gruppi terroristici

3. **economici**, fenomeni di truffa, abusi, riciclaggio di denaro sporco, e in generale tutte quelle

operazioni illecite che si avvalgono dell'infomation technology per ottenere un immediato ritorno finanziario

Informatici	Sociali	Economici
Intrusione in sistemi protetti	Cyberterrorismo	Truffe e frodi
Diffusione di virus informatici	Cyberpedofilia	Traffici vari (armi, droga)
Net-strike	Molestie (cyberstalking)	Criminalità organizzata (riciclaggio)
Furti di informazioni e spionaggio	Proselitismo delle sette sataniche	Spamming
Defacement	Spamming	
Denial of Service		
Phreaking		

2.1 Crimini prettamente informatici

Osserviamo in dettaglio queste tipologie criminali, iniziando dai fenomeni prettamente informatici:

2.1.1 Intrusione in sistemi protetti

Consiste nel violare un apparato informatico senza averne i permessi di accesso, scavalcando dei meccanismi di sicurezza. Può essere effettuato per diversi scopi: dalla semplice sfida (concetto presente nella cultura hacker), al furto o danneggiamento di informazioni riservate (progetti industriali, numeri di carte di credito, dati personali, ...) per arrivare all'abuso del sistema colpito per asservirlo a finalità illecite (accesso in incognito ad altri sistemi, denial of service, netstrike, ecc...).

Per mettere in atto un'intrusione possono essere sfruttati diversi strumenti, tra cui:

- *Trojan horse*: sono programmi malevoli camuffati da software innocui. Un cavallo di Troia può essere usato per aprire una backdoor[1] in un sistema informatico, per consentire al criminale di ottenere l'accesso in un secondo tempo
- *Virus* e *worm* (si veda a riguardo il prossimo paragrafo)
- *Vulnerability scanner*: strumento usato per controllare rapidamente dei computer su una rete in cerca di vulnerabilità note. Un esempio sono i *port scanner*, usati per verificare quali port su un determinato computer sono "aperte" e quindi disponibili per infiltrarsi nella macchina
- *Sniffer*: applicazione che cattura il traffico di rete, ivi comprese password e dati sensibili. Se trasmessi in chiaro (non crittati), questi dati possono essere individuati da malitenzionati, e usati per azioni illecite
- *Exploit*: applicazioni preparate ad hoc per sfruttare una vulnerabilità ben nota
- *Social engineering*: uso di tecniche per ottenere informazioni confidenziali manipolando utenti legittimi. Prevede generalmente l'uso del telefono o di Internet per inganare le persone, fargli

[1] per *backdoor* ("porta sul retro") si intende un generico metodo per bypassare le normali procedure di autenticazione o, più in generale, per ottenere il controllo remoto di un sistema. Una backdoor può prendere la forma di un programma apposito installato all'insaputa dell'amministratore (trojan, virus, ...), oppure essere una modifica attuata ad un programma legittimo già esistente sul sistema.

rivelare informazioni o compiere azioni contro le politiche aziendali. Il social engineering, quindi, sfrutta la naturale tendenza delle persone a fidarsi della parola data, avvalorando la credenza "gli utenti sono l'anello debole", diffusa tra gli addetti ai lavori.

- *Root kit*: insieme di strumenti usati per nascondere il fatto che la sicurezza di un sistema è stata compromessa. I root kit possono includere copie artefatte di alcuni files eseguibili, modificati in modo da non rendere possibile agli utenti legittimi di rilevare la presenza di un intruso ad esempio osservando la lista dei processi attivi

Quando l'intrusore non commette tali azioni guidato da un'etica (l'etica hacker), ma al contrario ha un tornaconto personale che lo spinge a danneggiare il prossimo, viene generalmente definito *cracker.*

2.1.2 Diffusione di virus informatici

[2]Viene generalmente definito "virus informatico" un ridotto insieme di istruzioni che, una volta penetrato in un elaboratore, ha la capacità di auto-replicarsi diffondendo l'infezione. Volendo essere più precisi bisogna distinguere tra virus e worm:

- *virus*: un virus è un programma auto-replicante che si diffonde attaccando copie di sè stesso all'interno di altri eseguibili o documenti; quindi un virus informatico si comporta esattamente come un virus biologico, il quale si diffonde viaggiando all'interno di cellule viventi

- *worm*: si tratta anche in questo caso di un programma auto-replicante, ma a differenza dei virus, i worm non hanno bisogno di attaccarsi ad altri eseguibili, sono perciò programmi a sè stanti. Ritornando al paragone biologico, i worm sono pertanto simili ai batteri

Alcuni virus hanno obiettivi dichiaratamente offensivi (ad esempio distruggere dati), altri sono quasi innocui, progettati solo per visualizzare determinati messaggi al verificarsi di un dato evento. La caratteristica comune, però, è quella della replicazione, che in ogni caso spreca le risorse (computazionali e di banda) della macchina infetta, e di tutte le macchine che saranno colpite al prossimo passo dell'epidemia.

Gli scopi per cui vengono scritti i virus sono spesso diversi. Alcuni nascono come progetti di ricerca, altri sono semplici burle o atti di vandalismo. Spesse volte dietro un'infezione vi è l'intenzione di attaccare i prodotti di una specifica compagnia (Microsoft su tutte), o di diffondere messaggi di natura politica.

Nonostante sia vista nella maggior parte dei casi come un'azione criminale, la creazione dei virus viene percepita dagli stessi virus writer come arte, e lo scatenare un'epidemia è spesso un hobby coltivato da giovani programmatori ansiosi di dimostrare le loro conoscenze informatiche.

In rari casi si è anche assistito alla creazione di virus benevoli, il cui scopo originario era quello di apportare migliorie ai programmi infetti, o debellare altre infezioni. Purtroppo è capitato che alcuni di questi virus venissero a loro volta infettati, diventando ironicamente vettori per nuove e più pericolose epidemie.

Nella maggior parte dei casi, comunque, lo scopo di un virus è quello di asservire il maggior numero di macchine al proprio creatore, che potrà sfruttarle per azioni criminali godendo dell'anonimato e delle ingenti risorse computazionali e di banda offerte da un tale sistema distribuito. Moltissime azioni di DDoS (Distributed Denial of Service) e di spamming di massa vengono messe in atto sfruttando le decine di migliaia di computer infettati da un dato virus. Di pari passo con

la diffusione dei vari servizi di home banking si assiste, infine, al proliferare di particolari tipi di worm specializzati nel furto di informazioni su conti correnti bancari e relativi dati di login.

La diffusione di virus può avvenire in diversi modi: tramite l'invio di messaggi di posta elettronica contenenti allegati infetti, sfruttando particolari debolezze dei sistemi operativi, visitando siti web malevoli.

Secondo i dati di TrendMicro, azienda leader nel settore dei software antivirus, nel solo anno 2003 i danni provocati da epidemie di virus a livello mondiale sono ammontati a 55 miliardi di dollari (circa 40 miliardi di euro): cifra enorme e preoccupante, se si tiene conto che - sempre stando a TrendMicro - lo sviluppo di virus è in continua progressione. Dopo una lieve flessione nel 2004, l'inizio del 2005 ha visto, nel solo mese di gennaio, la nascita di oltre 3100 tra virus worm e trojan, con un incremento del 50% rispetto al mese precedente.

Il problema dei virus è grave, e forse sottostimato, anche in Italia: molti degli attacchi denunciati alla Polizia Postale e delle Comunicazioni si sono spesso rivelati, in seguito ad accurate indagini, effetti di virus informatici contratti in seguito a comportamenti negligenti da parte dei dipendenti nell'uso delle postazioni internet all'interno dell'azienda.

2.1.3 Net-strike

Manifestazione di massa organizzata da gruppi di persone per rendere pubblico il proprio dissenso nei confronti di un'iniziativa, una legge o in generale una qualsiasi organizzazione. Il Netstrike è un particolare caso di Denial of Service, paragonabile ad un corteo civile che sfila per le strade di una città: invece di darsi appuntamento in un preciso luogo fisico, i partecipanti di un netstrike cooperano ad intasare un dato sito web, occupandone le preziose risorse di calcolo e banda mediante continui reload e download massicci.

In Italia un eclatante caso di netstrike si verificò il 15 Marzo 2001, quando, in occasione del Global Forum di Napoli, manifestanti no-global attaccarono il sito di Banca Fineco, una delle più consolidate realtà di trading online dell'epoca.

2.1.4 Furti di informazioni e spionaggio

Il furto di informazioni riservate si può verificare sia per effetto di una intrusione nel sistema protetto di un'organizzazione, che per l'azione di un dipendente disonesto dell'organizzazione stessa (insider) intenzionato a rivendere i dati rubati alla concorrenza. Oltre a segreti industriali e progetti, ad essere oggetto di furto possono essere informazioni confidenziali come numeri delle carte di credito, dati finanziari, dati personali di dipendenti e clienti. Quest'ultimo aspetto si ricollega al problema sociale della violazione della privacy e può comportare un duplice danno per l'organizzazione colpita: sia dal punto di vista dell'immagine che da quello legale: a seguito del furto di 70'000 numeri di carta di credito, la compagnia EggHead, operante nel campo dell'e-commerce, subì un danno di immagine tale che portò ad una caduta del 20% del fatturato.
EggHead fu poi assorbita da Amazon.

2.1.5 Defacement

Insieme di azioni atte a colpire un sito web con l'intento di danneggiarne il proprietario e, in secondo luogo, i fruitori del servizio; viene realizzato mediante intrusione illecita o sfruttando bugs dell'applicazione web su cui è basato il sito, sostituendo ai contenuti originari delle informazioni devianti, spesso diffamatorie nei confronti dell'organizzazione colpita. Il più delle volte il defacement si limita a modificare l'home page, al fine di diffondere un messaggio (politico, razzista, o di

altra natura), sfruttando la visibilità di cui gode il sito. Il danno provocabile attraverso un crimine di questo tipo può essere sia di natura prettamente economica (ad esempio se il sito offre servizi a pagamento o inserzioni pubblicitarie) che di immagine, a seconda del tipo di messaggio lasciato dal defacer.

2.1.6 Denial of Service

Corrisponde letteralmente alla "negazione del servizio", ovvero l'impossibilità da parte di un server di gestire le richieste degli utenti legittimi, provocata dall'attacco congiunto di più macchine contemporaneamente. La mole di richieste simultanee provenienti da tali macchine causa una saturazione della banda ed un esaurimento delle risorse di calcolo a disposizione del server, che non è dimensionato per supportarla.

Può essere effettuato secondo 2 modalità:

- **DoS** semplice: gli attacker inviano consapevolmente flussi falsi di richieste di servizio;
- **DDoS**, ovvero DoS Distribuito: gli attacker sfruttano macchine asservite tramite un virus/worm per moltiplicare il potere distruttivo della loro azione, comandando loro di effettuare richieste fasulle al server.

Il Denial of Service può essere perpetrato sfruttando diverse vulnerabilità:

- consumo di risorse quali banda, spazio su disco, capacità di calcolo
- danneggiamento di tabelle di routing [2], con il risultato di tagliare il server bersaglio fuori dalla rete Internet
- distruzione fisica di apparati di rete

Il primo caso è il più diffuso, anche perchè è il più semplice da mettere in atto, ad esempio attraverso una di queste tecniche:

- *smurf*: viene inviato un messaggio fasullo ad un gran numero di IP. Il messaggio contiene come mittente l'indirizzo del sistema bersaglio dell'attacco, così che le macchine contattate rispondano in massa a quell'indirizzo, sovraccaricando il server
- *banana attack*: i messaggi in uscita da un sistema vengono reindirizzati sul sistema stesso, impedenedo l'accesso esterno e al contempo subissando il bersaglio con i propri stessi messaggi
- *flood*: massiccio invio di richieste di servizio, ad esempio ICMP o HTTP, è il caso più classico di DoS

[2] le tabelle di routing sono gli elementi fondamentali per l'*instradamento* dei pacchetti sulla rete Internet. Forniscono ai *router* le informazioni necessarie per scoprire un cammino attraverso cui far viaggiare il flusso di informazioni da mittente a destinatario.

2.1.7 Phreaking

I phreakers, o phone-phreakers, sono hacker che prediligono il settore telefonico: il loro obiettivo è truffare le compagnie telefoniche costruendo circuiti elettronici che riescono a confondere i centralini. Con l'avvento della telefonia cellulare, è stata proprio quest'ultima la principale vittima di questo genere di attacchi. Il telefono cellulare è uno strumento gestito e organizzato da un software che è modificabile o comunque sostituibile. Si capisce perciò che tutti gli strumenti tecnologici impiegati per fornire i servizi di comunicazione, in quanto gestiti da sistemi informatici, possono essere oggetto di illecite intrusioni

2.2 Crimini sociali

Analizziamo ora i crimini a sfondo sociale

2.2.1 Cyberterrorismo

Sono sempre più frequenti i casi di attacchi informatici finalizzati alla diffusione di messaggi intimidatori tipici del terrorismo convenzionale. Un gruppo definitosi Pakistani Hackerz Club, per esempio, tempo fa ha effettuato il defacement del sito dell'American Israel Public Affairs Committee rimpiazzando la home page della potente lobby filoebraica con frasi anti Israele. Gli stessi pakistani, inoltre, si sono inseriti nel database del sito, impossessandosi del numero di carta di credito dei settecento sostenitori e inviandoli via mail a 3500 membri dell'Aipac per vantarsi del loro exploit.

Nel 1997 la rete informatica del Pentagono ha subito più di seicento attacchi, nonostante non sia collegata ad alcuna altra rete pubblica, né alla rete di internet. Quello del cyberterrorismo è un nuovo pericolo che si caratterizza per due considerazioni. La prima è che questo tipo di terrorismo colpisce in modo più duro gli Stati più sviluppati dal punto di vista tecnologico: tanto più uno Stato è tecnologicamente avanzato, tanto più il terrorismo informatico è potenzialmente distruttivo visto il grado di integrazione tra ICT e vita comune.

La seconda notazione è che i mezzi richiesti per porre in essere azioni di questo tipo sono alla portata di chiunque a bassi costi. Inoltre i potenziali obiettivi sono numerosissimi, dai sistemi informatici pubblici (non esclusi quelli militari) a quelli privati, come ad esempio le banche. L'utilizzo della rete da parte dei nuovi terroristi trova spesso finalità di propaganda e di proselitismo e il nuovo media sembra aver portato ad una modificazione della strategia comunicativa.

Ma l'ambito dove internet sembra poter offrire maggiori opportunità di sviluppo ai gruppi terroristici è quello logistico e organizzativo, soprattutto nelle comunicazioni segrete tra cellule distanti tra loro anche migliaia di chilometri. La rete, inoltre, grazie alla facilità d'accesso e all'ampia diffusione, viene sempre più spesso usata per dare risalto alle rivendicazioni delle proprie azioni sovversive.

2.2.2 Cyberpedofilia

[6]Con lo sviluppo di internet, gli studiosi e gli investigatori hanno dovuto rilevare la presenza di una nuova dimensione organizzata della pedofilia, centrata prevalente sulla pornografia, che sembra essere in fase di incremento quantitativo. La rete mette infatti in connessione pedofili di tutto il mondo apparentemente con minori rischi di essere scoperti vista l'enorme quantità di collegamenti che la rete accoglie.

Il pedofilo ha infatti ottenuto attraverso internet la possibilità di "nutrire" la sua particolare perversione sessuale mediante l'acquisto o lo scambio con altri pedofili di materiale pedopornografico. In alcuni casi però compiono attività più allarmanti. L'attività investigativa ha infatti individuato dei soggetti che, grazie anche all'anonimato garantito dalla natura della rete, avvicinavano i minori in chat e li conducevano su tematiche sessuali o addirittura tentavano di incontrarli fuori dalla rete. Talvolta, attraverso internet i pedofili cercano anche di ottenere un contatto con un bambino già abusato (e magari ricattato) da un altro pedofilo.

2.2.3 Molestie, minacce (CyberStalking)

[8]Il cyberstalking è l'evoluzione tecnologica del classico fenomeno dello stalking, e cioè "*un insieme di comportamenti ripetuti ed intrusivi di sorveglianza e controllo, di ricerca di contatto e comunicazione nei confronti di una vittima che risulta infastidita e/o preoccupata da tali attenzioni e comportamenti non graditi*", secondo una definizione coniata dal Dipartimento di Patologia Neuropsicosensoriale dell'Università di Modena.

Alla luce delle ricerche più recenti, sviluppate in prevalenza nel mondo scientifico statunitense, è possibile sintetizzare una tipologia semplificata di persecutori:

- soggetti che non riescono ad accettare l'abbandono del partner o di altre figure significative e attuano una vera e propria persecuzione nel tentativo maldestro di ristabilire il rapporto o semplicemente vendicarsi dei torti subiti nel corso del distacco. Sono i molestatori statisticamente più pericolosi per quanto riguarda la possibilità che lo stalking degeneri in atti di violenza fisica nei confronti della vittima

- soggetti che sfogano attraverso lo stalking un rancore dovuto a cause molteplici nei confronti di una persona con cui sono entrati in conflitto, al di fuori di un rapporto affettivo. Tipico il caso dell'ex collega di lavoro "che si è comportato male con lui" o del professionista (es. Un medico) che gli ha provocato un danno giudicato grave. Normalmente questi stalker presentano in livello di pericolosità contenuta, la violenza fisica viene rappresentata attraverso le molestie e gli insulti ma difficilmente messa in atto

- molestatori sessuali abituali o conquistatori maldestri, che individuano l'oggetto del loro desiderio nella vittima (anche sconosciuta) ed effettuano una serie di tentativi di approccio incapaci o incuranti dei segnali di fastidio da parte della vittima. I soggetti appartenenti a questa categoria talvolta presentano modalità compulsive o possono giungere a vere e proprie forme di delirio. Per ciò che attiene agli indici di pericolosità i molestatori sessuali abituali possono divenire potenziali stupratori mentre la categoria dei cosiddetti conquistatori maldestri normalmente è pressoché innocua

2.2.4 Proselitismo delle sette sataniche

Alcuni gruppi utilizzano il web per svolgere attività di proselitismo a bassi costi raggiungendo moltitudini di persone con i loro messaggi. Nel caso delle sette sataniche o di gruppi razzisti, ad esempio, si assiste al proliferare di siti web che offrono contenuti illegali talvolta ad alto rischio come violenza, esortazione al suicidio, esortazione all'odio razziale eccetera: materiale che comunque di rado è esplicitamente criminale.

2.2.5 Spamming

Con *spamming* si intende l'invio massiccio di messaggi e-mail indesiderati. Tali messaggi possono essere di due tipi:

- **Unsolicited Commercial Email** (UCE):messaggi di carattere commerciale con invio massivo
- **Unsolicited Bulk Email** (UBE): messaggi non commerciali con invio massivo. Capita sempre più spesso di ricevere messaggi che ci avvertono di micidiali virus, omaggi o guadagni facili da reinvestire nei propri debiti, comunicazioni di improbabili vincite, "matcher" amorosi, truffe a schema piramidale, messaggi pietoso-commoventi, immagini pedopornografiche, materiale warez[3] o l'ultima patch della Microsoft, nonché comunicazioni riguardanti falsi siti Internet o false petizioni, catene di S. Antonio...

Secondo dati comunicati dall'Authority per la privacy, in Italia la percentuale di messaggi indesiderati supera ormai il 50% del totale (nel 2001 lo spam rappresentava solo il 7% della posta mondiale) e la sola Tiscali filtra circa 800.000 messaggi al giorno, ossia circa 5 milioni di messaggi non sollecitati la settimana. Il fenomeno virus ha sposato ben presto quello dello spamming, realizzando così un binomio inscindibile, un perfetto connubio missivo per veicolare false informazioni, messaggi promozionali, trojan, spyware e worm di qualsiasi natura. Sono ormai diffusi dei programmi (una sorta di spider) che analizzano le pagine web pubblicate in rete alla ricerca di indirizzi e-mail.

Gli indirizzi trovati vanno ad alimentare dei database che poi vengono utilizzati per l'invio di e-mail pubblicitarie di vario genere. Ad aiutare la raccolta di ingenti quantitativi di indirizzi, concorre la pessima abitudine di inoltrare qualsiasi genere di messaggio a tutti gli indirizzi della propria rubrica senza avere l'accortezza di includerli come destinatari nascosti (undisclosed recipient).

Contrariamente a quanto si possa pensare, gli spammer non sono ignoti: il 90% dello spam proviene da un gruppo di persone molto ristretto (circa 200), di cui si conosce nome, cognome ed indirizzo. Costoro raccolgono le "ordinazioni" da organizzazioni che vogliono pubblicizzare un prodotto o servizio e, sfruttando risorse Internet proprie e altrui (pc asserviti di utenti ignari), compiono l'opera.

Il giro d'affari è enorme: circa 7,3 miliardi di dollari nel 2005 a fronte di un bassissimo investimento: un database di 156 milioni di indirizzi email può essere acquistato a soli 200 dollari. Il danno inflitto alle aziende, d'altro canto, è ingentissimo: si è ipotizzato che nel solo anno 2002 il costo generato dalle e-mail spazzatura per le imprese europee abbia raggiunto i 2,5 miliardi di euro in termini di maggior utilizzo delle strutture di comunicazione, di perdita di tempo e soprattutto di produttività.

2.3 Crimini a sfondo economico

Per ultimo approfondiamo i crimini a sfondo economico

2.3.1 Truffe e frodi

vi sono diverse tipologie di truffe attuabili attraverso mezzi informatici

[3] materiale coperto da copyright scambiato in violazione della relativa licenza

- *Phishing*: Tra le truffe informatiche il phishing è tra le più insidiose. Consiste infatti nell'uso di e-mail e nella creazione di pagine web ideate per simulare comunicazioni ufficiali da parte di una istituzione: obiettivo, impadronirsi di password e numeri di conto, account e, in ultima analisi, denaro altrui. La procedura adottata è la seguente: si formatta una pagina html con lo stesso aspetto di quella del login di un sito istituzionale, la si rende accessibile attraverso un URL abbastanza simile a quello originale e tramite spamming si invia una falsa richiesta di reimmissione dei propri dati personali a scopo di verifica. Gli utenti disattenti, si lasciano ingannare dalla somiglianza - apparente - con il sito vero e proprio. Una volta inseriti i propri dati si danno all'organizzazione criminale le informazioni necessarie per effettuare un login legittimo ed accedere, ad esempio, al proprio conto bancario.

- *Truffe con carte di credito*: Se da un lato si può osservare che la carta di credito è lo strumento di pagamento più utilizzato per le transazioni economiche sul web, esso è anche quello più esposto al rischio di possibili truffe. Al riguardo, comunque, recenti studi hanno evidenziato un tasso di frode nel suo utilizzo che oscilla fra l'8 ed il 9 per mille a fronte di una percentuale di utilizzo pari al 98,5% delle transazioni on line. Per il settore del commercio on-line, sono state citate alcune operazioni che simboleggiano le varie tipologie in cui si può manifestare la minaccia all'e-commerce e che schematicamente si possono riassumere in:

  - contraffazione del supporto magnetico o riproduzione dei dati in esso contenuti
  - uso fraudolento della carta di credito per l'acquisto di beni materiali tramite la rete

- *Truffe via email (Scam)*: attraverso la posta elettronica sono possibili imbrogli di ogni genere, la cui attuazione è semplificata dall'anonimato del mittente e favorita dall'enorme quantità di destinatari (e quindi possibili vittime) raggiungibili con un click.
  È un fenomeno ormai datato, ma che continua a mietere vittime. Il meccanismo in fondo ha ben poco a che fare con internet, nel senso che utilizza la rete solo come principale strumento di comunicazione ma in realtà sfrutta due esche psicologiche irresistibili: 1) diventare ricchi velocemente e senza fatica 2) ovviamente "noi" siamo speciali, diversi da tutti gli altri, ci siamo meritati una grande fortuna. Nella nostra casella email improvvisamente arriva un messaggio, da un perfetto sconosciuto. Costui si presenta come avvocato, dipendente di una banca, figlio di un dittatore tragicamente scomparso oppure erede di un cospicuo patrimonio (di norma stiamo parlando di decine di milioni di dollari). Il mittente dichiara di avere la possibilità di sbloccare questa montagna di soldi ma ha bisogno di un piccolo aiuto, di solito nel suo paese c'è una guerra civile o qualcosa del genere quindi ha bisogno di noi: ha bisogno di una persona affidabile in occidente dove dirottare temporaneamente questa fortuna per entrarne in pieno possesso; insomma ha bisogno di un complice affidabile con un conto corrente in occidente, lui (o lei) provvederà all'emissione di un bonifico internazionale mettendo sul conto i soldoni. Naturalmente lui si fida ciecamente di noi e quindi sa che, una volta completata la transazione, noi gli restituiremo i soldi trattenendo una provvigione per il disturbo. Ci sono numerose varianti della truffa ma tutte hanno in comune una particolare generosità dato che la commissione va dal 10 al 40% dell'importo totale. Una volta ricevuta risposta da qualche credulone, il ricco straniero chiede alla vittima contatti e dati bancari per poter successivamente effettuare il bonifico, salvo poi incappare in una serie di problemi burocratici, a suo dire facilmente risolvibili corrompendo qualche impiegato locale; siccome il tesoro è ancora bloccato, il truffatore ha bisogno di un piccolo anticipo da parte dell'ignara vittima, che in molti casi purtroppo "abbocca" all'inganno, perdendo talvolta ingenti cifre.

2.3.2 Criminalità organizzata

[4]La globalizzazione delle attività finanziarie, insieme al rapido sviluppo delle tecnologie dell'informazione, se da un lato offrono nuove opportunità di crescita dell'economia, dall'altro, aumentano i rischi d'inquinamento connessi al riciclaggio di capitali illeciti.

Con internet, infatti, viene ampliata quella "distanza" tra il riciclatore ed il capitale, frutto dell'attività illecita, che gli assicura uno spazio relativamente tranquillo ove operare in due modi possibili, senza incorrere in particolari controlli.

In primo luogo, gli strumenti telematici e quindi la rete internet possono essere usati come un ulteriore mezzo di comunicazione, che si aggiunge a quelli tradizionali, offrendo un canale ulteriore per le operazioni di riciclaggio senza modificarne comunque i meccanismi di fondo. In secondo luogo, l'avvento di internet può modificare i meccanismi di riciclaggio on-line offrendo delle opportunità irrealizzabili nel sistema di transazioni finanziarie tradizionali, dando vita così al cosiddetto *cyberlaundering*.

Nella prima delle ipotesi considerate, internet offre maggiori possibilità sia per quanto riguarda l'anonimato che la velocità delle transazioni, senza dimenticare l'assoluta indifferenza alle distanze geografiche. La seconda, invece, è un'ipotesi suggestiva relativa ad un nuovo contesto in cui la rete telematica può divenire strumento per effettuare acquisti di beni e spostare capitali in un'economia che si avvia alla piena dematerializzazione dei suoi prodotti, facilitando in maniera radicale le varie modalità del processo di riciclaggio. Ad esempio, è praticamente impossibile verificare se, a fronte di una somma sborsata per servizi tipo "sex-on-line" verso un sito web straniero, il servizio virtuale sia stato effettivamente erogato o se questo sia un'artificiosa rappresentazione necessaria per giustificare il transito di ingenti quantità di capitali.

Capitolo 3

Quadro normativo

[1]Il computer crime, definito come "*Ogni comportamento previsto e punito dal codice penale e dalle leggi speciali in materia, in cui un qualsiasi strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione dell'illecito*" può manifestarsi in modalità: reati commessi **a danno** di un sistema informatico (accesso abusivo, danneggiamento, ...) reati commessi **per mezzo** di un sistema informatico (pedofilia, truffe, ...).

Data la peculiarità della rete internet (transnazionalità, aterritorialità), il crimine informatico costituisce un fenomeno giuridico assai complesso che non può essere affrontato con le tradizionali tecniche d'indagine adottate nella lotta al crimine comune. Innanzitutto, la dimensione globale della Rete non permette una copertura normativa assoluta e richiede da parte del Legislatore una continua opera d'innovazione, aggiornamento e di armonizzazione con le normative internazionali vigenti in materia.

Un aspetto giuridico importante connesso alla perseguibilità del reato, è l'individuazione del cosiddetto "*Locus commissi delicti*"[1] decisivo per stabilire quale sfera di competenza sia interessata dall'illecito.

Le tematiche da affrontare riguardano se e con che limiti si possano applicare le previsioni di diritto penale nazionale al cosiddetto villaggio globale privo di confini territoriali, ponendo così problematiche di diritto penale internazionale.

A tal proposito occorre sottolineare come un notevole passo avanti sia stato fatto, sul piano della collaborazione internazionale, nell'attività di contrasto al computer crime, attraverso la stipula della "Convenzione sul Cybercrime", sottoscritta a Budapest il 23 novembre 2001 da 29 stati, tra i quali l'Italia, che rappresenta lo sforzo della comunità internazionale per indirizzare l'azione preventiva e repressiva delle forze dell'ordine in materia di crimini informatici.

3.1 Reati informatici in generale

Nella lotta ai crimini informatici il modello "evolutivo" adottato dal nostro Paese ha previsto modifiche ed aggiunte alle norme già esistenti nel codice penale e ampliato i poteri degli inquirenti nella fase di acquisizione delle prove prevedendo intercettazioni informatiche e telematiche. Emblematico è l'art. 1 della Legge 547 del 1993 ove il concetto di violenza sulle cose si estende alla categoria dei beni informatici.

Nello specifico, la legge in questione tutela, tra gli altri, i seguenti comportamenti illeciti:

[1]Questo consiste, ad esempio, nel determinare se un truffatore statunitense che utilizzi un server sudafricano per frodare un francese commetta il reato negli USA, in Sudafrica o in Francia

- *Attentato ad impianti di pubblica utilità* (art. 420 c.p.): punisce chiunque commetta un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, sistemi informatici o telematici o dati, informazioni e programmi in essi contenuti o pertinenti; la pena prevista è la reclusione da 1 a 4 anni.

- *Accesso abusivo ad un sistema informatico o telematico* (art. 615 ter c.p.): punisce chiunque si introduca abusivamente o si mantenga, contro la volontà espressa o tacita, in un sistema informatico o telematico protetto da misure di sicurezza; la pena prevista è la reclusione fino a 3 anni. Nel caso di danneggiamento di sistemi militari, o in generale di interesse pubblico, la pena prevista può arrivare a 8 anni.

- *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici* (art. 615 quater c.p.): punisce chiunque ai fini di procurare - a sè o ad altri - un profitto, o per arrecare ad altri un danno, abusivamente si procuri, diffonda, riproduca, comunichi, consegni codici, parole chiave o altri mezzi, o comunque fornisca indicazioni o istruzioni idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza; la pena prevista è la reclusione fino ad un anno e multa fino a 5000 euro.

- *Diffusione di programmi diretta a danneggiare o interrompere un sistema informatico* (art. 615 quinquies c.p.): punisce chiunque diffonda, comunichi o consegni un programma informatico (da lui stesso o da altri redatto) che ha per effetto o per scopo il danneggiamento di un sistema informatico o telematico o dei dati e programmi in esso contenuti, ovvero l'interruzione o l'alterazione del funzionamento di un sistema informatico; la pena prevista è la reclusione fino a 2 anni e multa fino a 10'000 euro.

- *Danneggiamento di sistemi informatici o telematici* (art. 635 bis c.p.): punisce chiunque distrugga, deteriori, renda inservibili in tutto o in parte sistemi informatici o telematici altrui oppure dati, programmi e informazioni altrui; la pena prevista è la reclusione da 6 mesi a 3 anni.

- *Frode informatica* (art. 640 ter c.p.): punisce chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto con qualsiasi modalità sui dati, le informazioni e i programmi contenuti in un sistema informatico o telematico, procuri a sè o ad altri un ingiusto profitto con altrui danno; la pena prevista è la reclusione da 6 mesi a 3 anni, e multa da 50 a 1000 euro.
  Altra forma di frode informatica è l'indebito utilizzo di una carta di pagamento magnetica, che si trova disciplinata in una legge ad hoc, all'art.12 della l. 5 luglio 1991 n°197.

- *Violazione, sottrazione e soppressione di corrispondenza* (art. 616 c.p.): punisce chiunque prenda cognizione del contenuto di una corrispondenza chiusa a lui non diretta, sottragga o distrugga una corrispondenza chiusa o aperta a lui non diretta; la pena prevista è la reclusione fino ad 1 anno, o multa da 30 a 500 euro.

- *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617 quater c.p.): punisce chiunque intercetti, impedisca o interrompa comunicazioni relative ad un sistema informatico o intercorrenti tra più sistemi, nonchè - mediante qualsiasi mezzo di informazione al pubblico - riveli il contenuto delle comunicazioni di cui sopra; la pena prevista è reclusione da 6 mesi a 4 anni.

- *Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche* (art. 617 sexies c.p.): punisce chiunque ai fini di procurare a sè o ad altri un

profitto o arrecare ad altri un danno, formi falsamente, alteri o sopprima in tutto o in parte il contenuto (intercettato anche occasionalmente) di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi; la pena prevista è da 1 a 4 anni.

La legge inoltre equipara il supporto informatico contenente dati, informazioni e programmi al documento cartaceo o di qualsiasi altra natura diversa da quella informatica o telematica, riconoscendo pienamente l'inviolabilità del contenuto, da considerarsi segreto, di tale supporto.

3.2 Pedofilia

Con l'approvazione della legge 3 agosto 1998, n. 269 recante "*norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno dei minori, quali nuove forme di riduzione in schiavitù*", l'Italia è stata tra i primi Paesi ad adottare una normativa specifica per contrastare lo sfruttamento sessuale dei minori sotto ogni aspetto, compreso quello della pedofilia on-line.

La legge consta di 19 articoli che introducono alcune novità sia a livello sostanziale per quanto riguarda la configurazione di nuove fattispecie di reato nel codice penale, sia sotto il profilo procedurale, introducendo nel codice di rito nuovi istituti per rendere più efficace l'attività della polizia giudiziaria. La legge, infatti, delinea precise linee d'intervento volte a contrastare:

1. l'induzione alla prostituzione dei minori;
2. la produzione, diffusione e detenzione di materiale pornografico coinvolgente minori;
3. il turismo sessuale all'estero in danno di minori;

Per quel che riguarda il materiale pedopornografico, vengono colpiti quei soggetti che in vario modo (tramite siti web, applicazioni di file sharing, semplice scambio di email) lo diffondono a qualsiasi titolo, dietro pagamento o semplice cessione.

Tuttavia, tali innovazioni, valide nella realtà materiale, rischiano di risultare sterili nella realtà virtuale ove le tradizionali categorie giuridiche sono inficiate dalla aterrorialità e dalla globalizzazione connessa alle transazioni on-line. In relazione all'elevato tecnicismo richiesto dalle attività nella rete Internet e per evitare confusioni e duplicazioni di indagini in una materia così delicata e complessa come quella della pedofilia on-line, la legge affida, in via esclusiva, al Servizio Polizia Postale e delle Comunicazioni, organo del Ministero dell'Interno deputato alla sicurezza delle comunicazioni ed al contrasto dei crimini informatici, alcuni specifici poteri e strumenti investigativi che saranno discussi in seguito.

3.3 Spamming

I Garanti della Privacy di molti Paesi europei - coordinati proprio dall'allora Garante Italiano, prof. Stefano Rodotà - hanno emanato nuovi regolamenti per contrastare il fenomeno spamming.

Il nuovo Codice in materia di Protezione dei Dati Personali - entrato in vigore a partire dal 1° gennaio 2004 - ha senza dubbio introdotto importanti innovazioni nella tutela della Privacy e ha contribuito ad uniformare la normativa italiana a quella europea. In particolare, per quanto riguarda la lotta allo spamming, la nuova normativa ribadisce il principio dell'opt-in[2] , (art.130),

[2]Sono emersi due approcci - opposti e contrastanti - nella lotta allo spam.

perciò è consentito l'invio di comunicazioni mediante sistemi automatizzati (posta elettronica, fax, dispositivi automatici di chiamata) solo con il preventivo consenso dell'utente interessato: tale tutela è stata estesa anche all'invio di messaggi pubblicitari tramite SMS e MMS.

Resta comunque il problema legato alla globalità del fenomeno: il ricorso al Garante, infatti, è valido solo per l'Italia e per quei paesi dell'Unione Europea che hanno adottato l'opt-in. Purtroppo, nella stragrande maggioranza dei casi, le e-mail spazzatura che ogni giorno intasano le caselle di posta elettronica degli utenti italiani proviene dall'estero. In questo caso l'unico modo per difendersi è segnalare lo spam ai provider, anche se generalmente questo serve ben a poco: molto spesso gli stessi provider sono spammer...

Negli Stati Uniti, patria della gran parte degli spammer mondiali, in virtù della Legge federale CAN-SPAM 2003 vige il principio dell'*opt-out*: un indirizzo email può quindi essere incluso all'interno di un database, ma deve essere garantita la rimozione dietro espressa richiesta del possessore dell'email.

In Europa, invece, secondo una direttiva del 2002 è stato adottato l'*opt-in*: perciò al fine di inserire un indirizzo in un database pr scopi di inoltro massivo, è necessaria la richiesta diretta del possessore dell'indirizzo email.

Capitolo 4

Contromisure

4.1 Introduzione e origini storiche

Lungo le vie consolari dell'impero romano si snodavano, almeno fin dai tempi di Traiano, linee di comunicazione ottiche le cui stazioni erano costituite da torri, ciascuna delle quali trasmetteva alla successiva segnali luminosi in codice, generati mediante esposizione di fiaccole, accese in vario numero e in varie posizioni; le torri erano cinte da palizzate, per proteggerle, verosimilmente, da incursioni nemiche (nelle provincie di confine) o da razzie di predoni, e per rendere così più sicura la trasmissione.

Come già duemila anni fa la questione della sicurezza nella trasmissione delle informazioni costituiva un problema, al giorno d'oggi la protezione di comunicazioni e dati, che hanno assunto nel tempo un valore sempre più critico, si ripresenta sotto nuove forme per adattarsi al progresso tecnologico e all'evoluzione di crimini e criminali.

La sicurezza dell'informazione è una scienza interdiscipinare che affonda le sue radici teoriche in varie branche specialistiche della matematica, della fisica, della statistica e della complessità computazionale e coinvolge delicati aspetti sociali, etici e giuridico-legali.

Le principali fasi in cui essa può essere suddivisa sono:

1. analisi dei rischi, per individuare e quantificare i pericoli e le minacce a cui l'informazione si trova esposta
2. realizzazione delle contromisure, intese come strumenti atti a ridurre quanto più possibile i suddetti rischi
3. problemi di natura sociale, etica e giuridico-legale connessi con la sicurezza dell'informazione
4. certificazione della sicurezza.

Per quanto riguarda le contromisure di sicurezza, esse appartengono generalmente a tre grandi famiglie: misure di tipo fisico, misure di tipo logico e misure di tipo organizzativo.

- Le misure di tipo fisico comprendono tutti gli accorgimenti "materiali" finalizzati ad evitare l'uso improprio delle risorse, il loro danneggiamento volontario od accidentale, o l'accesso non autorizzato ad esse: si va così dai meccanismi di controllo degli accessi ai sistemi di videosorveglianza, dai rivelatori di fumo agli allarmi anti-intrusione e così via. Come si nota si tratta di misure difensive di tipo tradizionale, anche se spesso le tecnologie impiegate sono moderne e sofisticate (ad esempio lettori di impronte digitali per aprire le porte d'accesso ai

locali protetti). Naturalmente questo tipo di misure si possono applicare solo alla sede fisica del soggetto da proteggere, e non sono in grado di contrastare attacchi "non fisici" quali le intrusioni via rete o la diffusione di virus informatici.

- Le misure di tipo logico comprendono invece tutti gli strumenti di controllo, protezione, identificazione ed autorizzazione in grado di agire a livello informatico. È questo il settore più ampio e variegato, perché molteplici sono i veicoli di minaccia contro cui agire e per ciascuno di essi sono innumerevoli le possibili soluzioni tecnologiche di protezione. Si va così dagli antivirus installati su ogni singola stazione di lavoro ai firewall che presidiano tutto il traffico di dati da e verso Internet, dai sistemi di intrusion detection in grado di rilevare tentativi di intrusione sulla rete interna ai dispositivi crittografici in grado di proteggere i messaggi di posta elettronica contro le intercettazioni, e così via.

- Le misure di tipo organizzativo, infine, riguardano la definizione e l'attuazione di procedure corrette per la gestione delle risorse e dei dati secondo processi documentati e verificabili. Esse, definendo le opportune modalità di azione e stabilendo chiare responsabilità nei soggetti che le devono attuare, mettono al sicuro i dati e le informazioni contro i rischi dovuti ad un utilizzo improprio, sia accidentale che intenzionale, ma anche ad esempio contro i rischi di danneggiamento dovuto ad errori o dimenticanze umane. Le procedure operative possono inoltre riguardare aspetti legali connessi alla sicurezza dei dati, ad esempio stabilendo chi e con quali modalità possa avere accesso a determinati tipi di archivio.

Andiamo ora ad analizzare nel dettaglio le misure di tipo logico, distinguendole nelle loro componenti hardware e software.

4.2 Hardware

[12]Nel campo hardware l'elemento fondamentale per garantire la sicurezza di una rete è il *firewall*, ovvero un dispositivo che seleziona e collega due o più tronconi di rete, che viene così divisa in due sottoreti:

- rete esterna, comprendente internet
- rete interna, comprendente una sezione composta da apparati di rete locali o *"trusted"*

La funzione principale del firewall è quella di proteggere i sistemi informatici presenti nella sezione interna da eventuali attacchi provenienti dall'esterno. Il firewall agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di controllo, modifica e monitoraggio; questo grazie alla sua capacità di "aprire" il pacchetto IP[1] per leggere le informazioni presenti sul suo header[2], e in alcuni casi anche di effettuare verifiche sul contenuto del pacchetto. Una delle configurazioni più ricorrenti e più efficaci che possiamo ritrovare in molte reti aziendali è rappresentata in Figura 4.1. Analizzando lo schema notiamo la presenza di una nuova area: la DMZ (DeMilitarized Zone, zona smilitarizzata), una rete *semipubblica* tra intranet e Internet;

[1]IP (Internet Protocol) è uno dei due protocolli - insieme al TCP - che stanno alla base del funzionamento della rete Internet. IP è un protocollo *a pacchetto*, cioè nella comunicazione tra due host non vi è un percorso predefinito su cui viaggiano tutte le informazioni, esse perciò vengono spezzettate in unità base - i pacchetti - che vengono inviati attraverso la rete, verso il destinatario.

[2]L'header di un pacchetto IP contiene, tra le altre cose, informazioni sul protocollo in uso e sugli indirizzi sorgente e destinazione. L'analisi di questi parametri è alla base del filtraggio dei pacchetti ad opera dei firewall

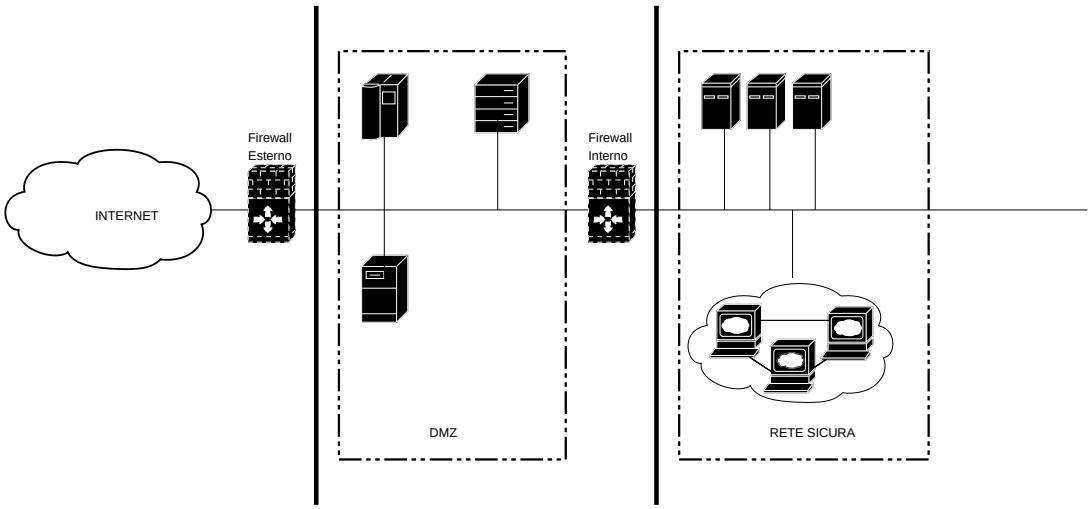

Figura 4.1: Schema di rete a DMZ

l'idea di base è che gli utenti esterni possano accedere solo alla DMZ, e limitatamente ai servizi resi disponibili, mentre le risorse interne restano nella zona privata e non sono accessibili dall'esterno.

Nella DMZ si ospitano i server pubblici (sito Web, server FTP, DNS, mailserver in ingresso,...) che non erogano applicazioni critiche per l'azienda. La zona smilitarizzata resta comunque un'area ad altissimo rischio, quindi le comunicazioni in arrivo dalla DMZ vanno considerate inaffidabili quanto quelle esterne.

Spostando l'attenzione dalla difesa di intere reti a quella delle singole macchine, e rientrando per un momento nella categoria delle misure di tipo fisico, per garantire la sicurezza negli accesi vengono adottate delle misure hardware di identificazione ed autenticazione capaci di determinare l'identità di una persona in base a:

- *ciò che si è*: sistemi biometrici per il riconoscimento dell'utente in base alle proprie caratteristiche fisiche
- *ciò che si ha*: token quali chiavette USB, smartcard, RFID, certificati digitali
- *ciò che si sa*: login/password

4.3 Software

Per quanto riguarda il lato software, le soluzioni sono molteplici, spaziando tra antivirus, crittografia, firma digitale, ACL, IDS. Analizziamoli nel dettaglio:

ANTIVIRUS Un antivirus è un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi come worm, trojan e dialer. Il suo funzionamento si basa principalmente sulla ricerca nella memoria o all'interno dei file presenti in un computer di uno schema tipico di ogni virus. Ogni antivirus ha infatti un database interno che contiene le definizioni dei virus, database che è bene tenere sempre aggiornato

CRITTOGRAFIA La crittografia (dal greco *kryptos*, nascosto, e *graphein*, scrivere) è la scienza che si occupa dello studio delle scritture "segrete" e viene impiegata per la protezione delle informazioni digitali.

Per sistema crittografico si intende un sistema in grado di cifrare e decifrare un messaggio attraverso l'uso di un algoritmo e di una chiave. I sistemi crittografici si possono distinguere a seconda del metodo adottato:

- *crittografia simmetrica* (detta a chiave singola o a chiave segreta): si utilizza una sola chiave per cifrare e decifrare; la sicurezza non deve dipendere dall'algoritmo utilizzato ma dalla segretezza della chiave. Il problema principale nella comunicazione a crittografia simmetrica è appunto lo scambio della chiave condivisa tra mittente e ricevente attraverso un mezzo insicuro.

- *crittografia asimmetrica* (detta a chiave pubblica o a doppia chiave): come si evince dal nome ogni persona possiede una coppia di chiavi:

  – la chiave privata, personale e segreta, viene utilizzata per decodificare un documento criptato con la corrispondente chiave pubblica e per criptare messaggi dei quali si vuole garantire l'autenticazione del mittente;
  – la chiave pubblica, che deve essere nota e accessibile a chiunque, serve a crittare un documento destinato alla persona che possiede la relativa chiave privata e a decifrare un messaggio con essa criptato.

  Ovviamente da una chiave non deve essere possibile risalire all'altra. Il problema dello scambio della chiave simmetrica attraverso una canale insicuro viene qui risolto brillantemente.

La crittografia, sia essa simmetrica o asimmetrica, rende vani tentativi di intercettazione e alterazione di comunicazioni, furto di informazioni, violazione della privacy, ecc...

FIRMA DIGITALE Ha lo scopo di garantire l'**integrità** del testo inviato e l'**autenticazione** del mittente; è il risultato di due fasi:

1. il testo del messaggio viene dato in pasto ad una funzione di *hash* [3]che ha il compito di creare il cosiddetto *message digest* o "impronta del messaggio".

2. il *message digest* viene crittato con la chiave privata del mittente, dando luogo alla firma digitale vera e propria Grazie al fatto che la firma digitale può essere decrittata solo con la chiave pubblica del mittente, saremo certi che è stato proprio lui a comporre il messaggio; l'integrità del messaggio viene invece garantita dal confronto tra il digest calcolato dal destinatario e quello pervenutogli con la firma digitale.

La firma digitale ha ora valore legale equivalente alla firma autografa.

[3]la *hash* è una funzione matematica che gode delle seguenti proprietà:

(a) data una stringa in input di qualunque lunghezza, la funzione di hash genera una stringa in output di dimensione fissa

(b) dalla stringa di output non si può in alcun modo risalire alla stringa di input

(c) se cambia anche un solo bit della stringa di input può cambiare fino al 50% della stringa di output

(d) due stringhe diverse in input generano sempre output diversi

ACL (Access Control List) Comprende quell'insieme di regole o policy tese a determinare i permessi accordati ad ogni utente per l'accesso a risorse, dispositivi e dati; vengono inoltre definiti i privilegi del medesimo, intendendo con ciò l'insieme delle operazioni concesse. Le ACL vengono solitamente integrate ai sistemi di autenticazione di cui si è discusso in precedenza, e seguono l'operato dell'utente durante tutta la sessione di lavoro

IDS (Intrusion Detection System) Sistema per la rilevazione di intrusioni o accessi non consentiti in un sistema informatico; può essere implementato in due modalità:

- *Anomaly Detection*: vengono definiti dei modelli di comportamenti "normali" con i quali si confrontano continuamente gli eventi rilevati sul sistema; in base ad una *soglia di anomalia* definita ad hoc, l'IDS segnalerà eventuali deviazioni significative. Questo tipo di segnalazione, però, viene riportata solo ad intrusione avvenuta, quando cioè è chiaro uno scostamento dalla normalità.
- *Misuse Detection*: rileva, in corso d'opera, le caratteristiche di un'intrusione, comparando gli eventi rilevati con degli schemi noti e ben definiti di attacco; è necessario perciò tenere ben aggiornata la raccolta dei pattern di attacco.

4.4 Informazione e sensibilizzazione

Come abbiamo visto nella corso della trattazione, molti crimini giocano sulla componente umana delle vittime: è quindi importante sensibilizzare l'utenza nei confronti di quelli che sono i problemi reali della rete.

Bisogna cioè insegnare a *non offrire terreno fertile ai possibili criminali.*

Per quanto riguarda il problema *spamming*, ad esempio, sarebbe buona norma non divulgare pubblicamente il proprio indirizzo email in chiaro su forum e newsgroup, trasformando la @ nella parola inglese "AT". Alla ricezione di un messagio di spam è altamente sconsigliato inviare una risposta, per non dare allo spammer la certezza che il proprio indirizzo di posta è attivo, e quindi renderlo maggiormente mira delle sue attenzioni. Nell'invio di messaggi a più destinatari (forward e simili) è bene nascondere gli indirizzi, realizzando la cosiddetta "Copia carbone cieca" (*Blind Carbon Copy*, Bcc).

Per evitare il contagio da parte di virus, oltre a dotarsi di un software apposito, mantenuto debitamente aggiornato, è importante non aprire gli allegati di posta di ignota provenienza, non visitare siti web contenenti materiale warez, e configurare correttamente browser web e client di posta elettronica per non eseguire automaticamente oggetti indesiderati senza il preventivo consenso dell'utente.

Infine, per quanto riguarda i rischi corsi dalle fasce più deboli (bambini, anziani, ecc.) è necessario intervenire preventivamente sia adottando filtri per la navigazione, capaci di oscurare materiale potenzialmente pericoloso, che educando ad un uso corretto della rete.
Ad esempio, è importante non fornire mai i propri dati personali, e soprattutto le proprie fotografie, agli sconosciuti; non replicare a messaggi di natura volgare o offensiva, accompagnare la navigazione online dei bambini, e così via...

Capitolo 5

Lotta al crimine

[5, 11, 9, 10, 3, 7]L'Italia è stato uno dei primi Paesi europei ad attivarsi nella lotta tecnologica ai nuovi crimini, ed in particolar modo alla pedofilia, contro la quale, grazie alla legge 269/98, è possibile svolgere azioni sotto copertura sul web: negli ultimi cinque anni sono stati identificati dalla Polizia di Stato più di duemila soggetti implicati in attività di pedofilia su internet. Gli agenti, grazie ad una specifica dispensa data da tale legge, possono realizzare siti pedofili "civetta" e possono fingersi pedofili per entrare nelle loro comunità segrete.

Chi effettua queste attività investigative è sottoposto ad uno specifico addestramento. I componenti della squadra imparano con il tempo a simulare gli schemi di pensiero dei pedofili e a comunicare con loro senza destare alcun sospetto. Imparano anche a controllare le loro emozioni che, visto il genere di interlocutore, potrebbero vanificare l'investigazione. Talvolta gli agenti della Postale si fingono anche dei bambini e riescono così ad individuare e catturare dei pedofili che tentano di adescarli nelle chat. Poichè le investigazioni undercover possono protrarsi nel tempo, gli investigatori che simulano di essere pedofili o bambini sono oggetto di un continuo monitoraggio psicologico per prevenire gli effetti dello stress investigativo.

Un'efficace azione di contrasto alle nuove strategie digitali dei criminali deve per forza di cose passare per la rete: attraverso il controllo mirato delle comunicazioni (soprattutto di chat ed e-mail) e attraverso la localizzazione di segmenti di informazioni illegali sui siti web, pur sempre rimanendo in un ambito di prevenzione e di intelligence.

Per ciò che attiene alla presenza sulla rete di informazioni illegali o pericolose, proposte da movimenti terroristici, sette sataniche o da altri gruppi pseudoreligiosi, è utile l'impiego di strumenti software di analisi testuale (*spider*) in grado di localizzare ed evidenziare tali informazioni, ricercandole tra i moltissimi newsgroup che trattano problematiche politiche, esoteriche e pseudoreligiose presenti sul web.

Per quanto concerne i crimini prettamente informatici tendenzialmente diretti nei confronti di aziende e pubblica amministrazione, da un'indagine svolta dall'FBI sulle grandi Corporations, è emerso che il 90% di esse ha subito qualche intrusione informatica, ma solo nel 34% dei casi la cosa era stata denunciata alle autorità di Polizia. In Italia, sebbene il fenomeno sia dimensionalmente ridotto, l'aspetto omertoso è ugualmente diffuso, forse per il desiderio da parte delle aziende colpite di non subire danni d'immagine dovuti alla pubblicazione dell'evento da parte dei media. Tutto ciò non semplifica il lavoro delle autorità, dato che in questi casi la cooperazione è fondamentale per perseguire i responsabili.

Capitolo 6

Conclusioni

Con questo documento abbiamo tentato di fornire una panoramica di quelli che sono i nuovi crimini introdotti dall'ICT e delle modificazioni subite dai crimini tradizionali per effetto dell'avanzamento tecnologico. Abbiamo dato una rapido sguardo alle modalità di attuazione e alle corrispondenti contromisure.

Vorremmo concludere ottimisticamente, parlando di un caso recentissimo che ha dimostrato come gli sforzi della Polizia Postale e delle Comunicazioni Italiana abbiano permesso di contrastare uno dei fenomeni più aberranti della società moderna: la pedofilia.

Citiamo a riguardo un articolo tratto da www.guidasicilia.it del 24 maggio 2005.

Maxioperazione anti-pedofilia in 16 regioni italiane. Tra gli indagati anche tre preti e un sindaco *Da un sito Internet segreto, non presente nei motori di ricerca e al quale si poteva avere accesso soltanto con una password, scaricavano filmati con bambine di età compresa tra i 4 e gli 8 anni vittime di abusi sessuali e sevizie. Tra le 186 persone indagate dalla Procura di Siracusa nell'ambito di una maxi inchiesta sulla pedopornografia online, anche degli eccellenti "cittadini al di sopra di ogni sospetto": tre sacerdoti, un vigile urbano, un assistente sociale, un sindaco e due assessori. L'inchiesta, denominata 'Video privé', coordinata dal procuratore della Repubblica aggiunto di Siracusa, Giuseppe Toscano, e dai sostituti Antonio Nicastro e Manuela Cavallo, è scaturita da una serie di dettagliate denunce presentate dall'associazione Telefono Arcobaleno - l'associazione che si occupa proprio di stanare sul web i pedofili che commerciano materiale pornografico con i bambini nel ruolo di involontari protagonisti - presieduta da Giovanni Arena.*

Gli indagati risiedono in ben 16 regione italiane. Nei loro confronti sono ancora in corso perquisizioni compiute da polizia postale, carabinieri e guardia di finanza. Sui computer dei tre sacerdoti coinvolti, che prestano il loro ministero in Sicilia, Lombardia e Trentino Alto Adige, sono state trovate diverse collezioni di filmati pedopornografici. Accertamenti sono stati eseguiti anche nella casa di un educatore all'infanzia siciliano, di un agente di polizia municipale marchigiano, di un operatore di un centro oncologico veneto, di un sindaco e di un assessore di due comuni lombardi. Nel corso delle perquisizioni sono stati sequestrati anche alcuni filmati di produzione 'artigianale', sul quale sono in corso indagini per identificare i bambini coinvolti nelle riprese.

Le indagini eseguite dal Nit, Nucleo investigativo telematico, hanno fatto emergere l'esistenza di un sito Internet al quale erano in grado di accedere soltanto gli utenti ben inseriti nei sodalizi internazionali di promozione e scambio della pedofilia. Gli indagati, individuati a conclusione di 11 mesi di accertamenti, sono tutti uomini, di media età, di varie estrazioni sociali: 34 sono residenti in Lombardia, 22 in Veneto e altrettanti nel Lazio, 17 in Piemonte, 13 in Emilia Romagna, 11 in

Campania e Toscana, 10 in Sicilia ed altrettanti in Liguria, 8 in Trentino, 7 nelle Marche, 5 in Puglia, Friuli e Abruzzo, 4 in Calabria e 2 in Basilicata.

Il sito era stato aperto su un server italiano, estraneo all'inchiesta e che ha collaborato con gli investigatori, con una tecnica da "mordi e fuggi": è stato infatti in funzione soltanto nove giorni, per evitare di essere identificato. Il breve tempo ha permesso così una "selezione" dei fruitori che potevano essere soltanto esperti del settore della pedopornografia. La sua esistenza, infatti, era pubblicizzata su una "bacheca" aperta su Internet su un sito "specializzato" aperto in un Paese orientale. Su un altro indirizzo web era disponibile la password che permetteva di accedervi, composta da una combinazione di 15 caratteri alternati di lettere e numeri. L'indirizzo del sito era inoltre privo di una pagina di indice per evitare che potesse essere individuato e catalogato dai motori di ricerca.

Terribili i filmati che si potevano visionare una volta entrati nel sito, dove innocenti protagoniste bambine subivano abusi sessuali e venivano picchiate e seviziate, in maniera violenta. Gli esperti dal Nucleo investigativo telematico sono riusciti a violare la rete di protezione estesa attorno al sito Internet e a identificare i computer di italiani che vi si erano collegati. La Procura di Siracusa negli ultimi due anni ha disposto il sequestro di oltre 400 siti Internet italiani con contenuti pedopornografici.

Bibliografia

[1] Avv. Raffaella Bonsangue. Appunti di diritto penale delle tecnologie informatiche.

[2] Francesco Donnarumma e Linda Grilli Fabio Battelli, Stefano Tassi. Dossier: allarme virus e spaming in italia. Telematic Journal of Clinical Criminology*, 2004.*

[3] Corrado Giustozzi. Il computer crime e la politica della security in azienda. Telematic Journal of Clinical Criminology*, 2002.*

[4] Alessandro Pansa. Web e riciclaggio: dalle banche un ruolo di garanzia. Telematic Journal of Clinical Criminology*, 2001.*

[5] Alessandro Pansa. Le strategie di constrasto al crimine informatico. Telematic Journal of Clinical Criminology*, 2002.*

[6] Marco Strano. I pericoli di internet. Telematic Journal of Clinical Criminology*, 2002.*

[7] Marco Strano. Investigazioni telematiche e web intelligence nell'era di internet. Telematic Journal of Clinical Criminology*, 2003.*

[8] Marco Strano. Cyberstalking. Telematic Journal of Clinical Criminology*, 2004.*

[9] Domenico Vulpiani. La polizia delle comunicazioni e la lotta alla pedofilia on-line. Telematic Journal of Clinical Criminology*, 2001.*

[10] Domenico Vulpiani. La criminalità informatica: metodi d'indagine e la collaborazione delle aziende bancarie. Telematic Journal of Clinical Criminology*, 2002.*

[11] Domenico Vulpiani. L'esperienza italiana nel contrasto al crimine informatico. Telematic Journal of Clinical Criminology*, 2002.*

[12] Ing. Stefano Zanero. Appunti di sicurezza degli impianti informatici.