Sicurezza Informatica & “Computer Crime”

Carlo Carlesi
Istituto di Scienza e Tecnologie dell’Informazione
“Alessandro Faedo”

Introduzione

Lo studio della comunicazione tra sistemi elettronici risale alla meta' degli anni 60 e possiamo dire che abbia avuto inizio con il progetto di rete geografica ARPA e successivamente ARPANET, voluto e finanziato dal Dipartimento della Difesa degli Stati Uniti. Il progetto condotto e sviluppato nell’ambito di prestigiose università americane e laboratori di ricerca privati (IBM, AT&T, Xerox, Digital), porto' alla realizzazione di una rete geografica costituita da 4 nodi. Lo sforzo dei ricercatori di allora fu principalmente finalizzato alla realizzazione di un sistema di comunicazione robusto, aperto e in grado di consentire anche la condivisione di risorse ed informazioni tra sistemi remoti eterogenei. A partire dagli anni 70, nell'ambito delle comunita' scientifiche, dove erano presenti, piu' che altrove, ingenti risorse di calcolo dedicate alla ricerca (computer mainframe) si ando' diffondendo il concetto di sviluppo di software aperto e gratuito (Open Source Software/Free Software), mentre in campo industriale, il software, come l'hardware veniva considerato un prodotto di mercato proprietario e da proteggere. Sono questi gli anni che vedono nascere anche le prime figure di “hacker”, termine quanto mai controverso e dalle numerose definizioni che vanno dall'esperto e puro cavaliere che ama la sfida intellettuale per superare o aggirare le limitazioni imposte da un programma software, al losco personaggio che tenta di scoprire informazioni sensibili per ‘intrufolarsi’ ed approfittare dei sistemi altrui.

Il mondo accademico, avvertiva allora, come oggi, la necessità di diffondere tempestivamente e in modo semplice informazioni e documenti per cui la tendenza dei progettisti e degli sviluppatori e’ stata quella di favorire al massimo l'interoperabilita' delle applicazioni magari a scapito di specifici meccanismi di sicurezza. A partire dagli anni 90 con la crescita dei sistemi connessi alla rete Internet, il diffondersi dell'uso quotidiano dei servizi telematici, la facilita' di fare un uso improprio di taluni servizi, e la crescita di azioni illecite ha portato alla necessita' di regolamentare l'uso della rete e definire misure di sicurezza dei sistemi informatici e dei dati in essi contenuti.

In relazione a quelle che possono essere definite le azioni illecite nel settore dei sistemi informatici (“computer crime”) possiamo distinguere due categorie:

1) illeciti commessi con l’ausilio di un computer;
2) illeciti dove il computer e’ il bersaglio.

Tra gli illeciti che si possono classificare nella categoria 1, ce ne sono alcuni che riguardano anche rilevanti aspetti sociali quali la pornografia, la pedofilia, l’adescamento e le molestie sessuali perpretate via Internet. Esperti industriali Americani hanno stimato che nel 2002 solo negli stati Uniti ci siano 45 milioni di bambini che possono connettersi ad Internet. Questi ragazzi utilizzano la rete per parlare con altri amici, fare i compiti scolastici a casa, esplorare musei, biblioteche

ed universita', ma allo stesso tempo possono interagire ed essere contattati anche da male-intenzionati.
Non esistono statistiche precise sui crimini sessuali via Internet, tuttavia in un rapporto della polizia postale degli Stati Uniti (U.S. custom service), viene fatto rilevare che a maggio del 1999, i casi di pornografia con bambini, provenivano per il 95% da Internet e che L'FBI dal gennaio 1998, all'agosto del 1999 ha operato oltre 460 arresti per lo scambio di materiale pornografico con bambini via Internet. In questo rapporto si fa anche presente che il materiale pornografico, tradizionalmente ristretto al solo scambio, sta rapidamente diventando "un'attivita' economica" non indifferente se si considera che gia' due anni fa' sono state arresate persone che "guadagnavano" fino a 25.000$ il giorno con CD-ROMs pornografici che coinvolgevano minorenni.

Nel seguito di questo documento parleremo di sicurezza dei sistemi informativi in relazione ad azioni illecite classificate nella categoria 2 che hanno come obiettivo un sistema informativo ed i suoi dati o comunque un computer in qualche modo connesso alla rete Internet.

Sicurezza dei sistemi informativi e riservatezza dei dati.

Le reti elettroniche di comunicazione e i sistemi informativi accessibili via rete telematica costituiscono, come abbiamo detto, una parte essenziale della vita quotidiana dei cittadini del mondo e rappresentano uno strumento fondamentale per il successo dell'economia delle imprese, delle istituzioni scientifiche e pubbliche.
Il problema della sicurezza informatica, non e' tuttavia solo un aspetto tecnico d'interesse degli addetti ai lavori ma, come abbiamo gia' accennato, un problema sociale che coinvolge anche lo stato e le sue leggi. Lo stato Italiano e' stato tra i primi paesi in Europa a legiferare in merito alla sicurezza dei sistemi informatici, al trattamento dei dati e alla riservatezza dei dati memorizzati. L'AIPA (Autorita' per l'Informatica nella Pubblica Amministrazione) ha costituito nel 1999 un gruppo di lavoro sulla "sicurezza informatica" che ha prodotto il documento "Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione" corredato di due allegati riguardanti il "panorama normativo di riferimento" e i "virus informatici". Numerose sono anche le misure legislative emanate riguardanti il commercio elettronico, la firma digitale ed il trattamento dei dati personali; in particolare, nell'ambito della sicurezza e riservatezza dei dati personali (privacy) (legge n. 675 del 31 Dic. 1996), con decreto del Presidente della Repubblica (n.318 del 28 Luglio 1999) e' stato emanato il regolamento delle norme e delle misure minime di sicurezza da adottare per il trattamento dei dati personali. Si tenga presente che la legge prevede anche la responsabilità del gestore del sistema informatico che in caso di omessa adozione di misure di sicurezza e' passibile di sanzioni sia civili che penali.
La tutela della riservatezza, infatti, non puo' prescindere dai criteri di sicurezza dei dati informatici stessi che devono risultare essere sicuri, ovvero protetti da misure di sicurezza efficaci e in grado di garantire il raggiungimento dei seguenti obiettivi:

- riservatezza: ovvero, la prevenzione dall'utilizzo indebito di informazioni

riservate;
- integrita': ovvero, la prevenzione dall'alterazione o manipolazione indebita delle informazioni;
- disponibilita': ovvero, la garanzia dell'accesso controllato alle informazioni;
- autenticita': ovvero, la garanzia e la certificazione della provenienza dei dati.

Anche a livello dell'Unione Europea (di seguito UE) in questi ultimi anni, il problema della sicurezza informatica e' fortemente sentito e numerose sono le iniziative avviate nell'ambito di tutti gli stati membri per una maggiore sensibilizzazione in materia di sicurezza delle reti elettroniche e dell'informazione (Consiglio Europeo di Stoccolma del 23/24 marzo 2001). Nel novembre 2001 l'UE ha adottato il documento "Convention on Cybercrime (ETS no. 185); con lo scopo principale di armonizzare e rafforzare la co-operazione internazionale nella lotta al crimine informatico. Sempre nell'ambito dell'UE nel corso del 2002 e' stata elaborata una proposta relativa agli attacchi contro i sistemi di informazione "Decisione-Quadro del Consiglio" (COM(2002)173 definitivo, Bruxelles, 19.04.2002). Gli obiettivi di tale proposta sono appunto quelli di razionalizzare le normative penali nel settore degli attacchi ai sistemi di informazione e costituire un contributo all'impego dell'UE nella lotta contro la criminalita' organizzata ed il terrorismo.
Sono inoltre disponibili e raccomandati dall'UE dei documenti standard per la definzione dei requisiti di sicurezza e per la gestione della sicurezza delle reti nelle organizzazioni pubbliche e private, quali ISO-15408 (Criteri Comuni) e ISO-17799 (Codice di buona pratica per la sicurezza dell'informazione).

La protezione dei sistemi informatici in rete.

(Cosa proteggere, da cosa proteggersi)
Il primo passo da compiere per la definizione di un piano di protezione e' l'individuazione degli elementi che necessitano di protezione e delle minacce a cui gli stessi possono essere soggetti. Nel caso specifico di un sistema connesso alla rete Internet la componente "gestione e modalita' di accesso al sistema" e' di rilevanza fondamentale a fronte del rischio di una intrusione con la possibile perdita dell'integrita' e riservatezza dei dati contenuti nel sistema stesso. E' fondamentale quindi procedere alla classificazione del bene informativo in funzione di elementi quali, integrita', riservatezza, e disponibilita' e attribuire al bene un valore per poter successivamente valutare il livello di esposizione al rischio. Sono disponibili diverse metodologie di valutazione del bene, alcune basate su principi qualitativi (efficienza del servizio offerto, perdita di immagine, violazione norme legislative etc.) altre basate su principi quantitativi (costi di ripristino, costi di ri-elaborazione etc.). E' opportuno inoltre definire in modo chiaro le varie responsabilita' ed il livello di sicurezza (costi/benefici) che si vuole raggiungere per ogni classe di oggetto. La sicurezza implica necessariamente un costo che generalmente aumenta con il grado di sicurezza che si intende raggiungere ed in funzione del valore assegnato all'oggetto da proteggere. Una regola comune e se vogliamo anche banale e' quella che "il costo della protezione di un oggetto a fronte di un rischio, dovrebbe essere minore del costo per il recupero dell'oggetto se il rischio si avvera".

Tipologie di attacco ai sistemi informatici.

Un attacco intenzionale ad un sistema informativo puo' essere lanciato da un qualsiasi posto nel mondo, in un qualsiasi momento. Gli attacchi possono assumere una grande varieta' di forme, e finalita' tra cui citiamo le piu' comuni quali, l'accesso illecito ad un sistema, la diffusione di codice malizioso (virus) e il diniego di servizio ("denial of service").
Consideriamo in maggior dettaglio alcune di queste tipologie di attacco:

a) Accesso non autorizzato ai sistemi di informazione.
Questo tipo di attacco, puo' avere la finalita' di copiare, modificare o distruggere dati, oppure di accedere senza pagare a servizi con accesso condizionato. Molto spesso, si riscontrano intrusioni su macchine che non contengono dati sensibili e di particolare valore, che vengono effettuate al solo scopo di utilizzarle per attacchi ad altri obiettivi e rendere il piu' difficile possibile risalire all'attaccante. Le tecniche di intrusione vanno dallo sfruttamento di informazioni interne, all'intercettazione di password di accesso o allo sfruttamento di "bachi" software di talune applicazioni (buffer overflow, etc).

b) Interruzione del funzionamento dei sistemi di informazione
Questo tipo di attacco, comunemente indicato come "denial of service" (DoS), mira principalmente ad interrompere l'erogazione dei servizi del sistema attaccato. Ci sono parecchi modi di portare questo tipo di attacco, tra cui quello di saturare il sistema attaccato mediante l'invio continuo e ripetuto di richieste ad opera di piu' sistemi contemporaneamente (molto spesso a loro volta compromessi per questo scopo) o attraverso la distruzione di dati e/o parti di programmi del sistema attaccato.

c) Esecuzione di software "maligni" che modificano o distruggono i dati.
Questo tipo di attacco generalmente noto con il nome di "virus", e condotto molto spesso atrraverso il servizio di posta eletrronica, ed e' tra i piu' diffusi proprio perche' ha la finalita' di replicarsi a macchia d'olio da un sistema all'altro. Ci sono "virus" che creano disfunzioni ma non danneggiano in modo irreversibile il sistema colpito, altri che invece distruggono dati e sistema operativo e talvolta creano anche guasti hardware.

d) Intercettazione di comunicazioni e falsificazione della propria identita'.
L'intercettazione dolosa delle comunicazioni ("sniffing"), oltre a compromettere la riservatezza dei dati utente e' spesso utilizzata per ottenere informazioni da utilizzare a fini dolosi, come l'usurpazione dell'identita' di un soggetto ("spoofing") o l'acquisizione di password per l'accesso su altri sistemi.

La politica della sicurezza.

La sicurezza informatica, come si e' detto, ha l'obiettivo principale di garantire, riducendo i rischi, un adeguato grado di protezione del bene informativo (inteso come insieme di dati e di risorse tecnologiche). Per una efficace strategia di difesa della propria infrastruttura telematica si deve partire dalla definizione ed attuazione di una specifica e costantemente rinnovata politica della sicurezza. La politica della sicurezza si deve basare su criteri generali indipendenti dalle tecnologie correntemente in uso e determinare il modello logico della sicurezza fissandone gli obiettivi. La politica deve anche tenere presente l'effettivo costo/beneficio della sicurezza, e definire misure di sicurezza coerenti con il "valore" del patrimonio informativo da proteggere, in linea con la propria missione istituzionale. Le linee guida indicate nella politica, dovranno ovviamente essere coerenti con le normative vigenti in tema di sicurezza, con le politiche di sicurezza informatica espresse dal Governo ed in particolare, per quanto riguarda le pubbliche amministrazioni, con l'indirizzi espressi in materia dall'AIPA.

Bibliografia

AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella pubblica amministrazione, [1999]

Computer Crime: A JOINT REPORT, State of New Jersey – Commission of Investigatione & Office of the Attorney General, [June 2000]

Decisione-Quadro del Consiglio relativa agli attacchi contro i sistemi di informazione, COM(23002)173 definitivo, 2002/0086(CNS), [Aprile 2002]

Common Criteria for Information Technology Security Evaluation, CCIMB-99-031, [August 1999]