Introduzione alla sicurezza informatica

Cosa si intende per sicurezza informatica

Con sicurezza informatica intendiamo la prevenzione o la **protezione contro l'accesso, distruzione o alterazione di risorse e informazioni da parte di utenti non autorizzati**. In genere, garantire la sicurezza informatica significa prevenire e proteggere contro l'accesso non autorizzato a risorse.

I crimini informatici colpiscono:

- **Hardware**: tramite la distruzione e furto di apparecchiature;
- **Software**: mediante modifiche ai software, furto di software, installazione di software infetti;
- **Dati**: con la cancellazione, lettura e modifica di dati sensibili senza autorizzazione.

Attualmente i dati costituiscono una componente molto importante e strategica per un'azienda: la compromissione di dati può avere delle conseguenze disastrose, non solo per l'utente ai quali appartenevano, ma all'organizzazione stessa.

Definizione di sicurezza informatica

Si puo' definire come sicurezza informatica, l'abilita' di un sistema di proteggere le informazioni e risorse rispetto alle nozioni di **CIA**:

- **C**onfidentiality (Secrecy and Privacy)
- **I**ntegrity
- **A**vailability

Confidenzialita'

Garantire confidenzialita' significa **assicurare che le infomazioni non siano accessibili ad utenti non autorizzati** (segretezza come sinonimo). Con **privatezza** invece si intende il **controllo delle informazioni personali** degli individui che vengono raccolte. L'individuo deve essere a conoscenza di quali informazioni vengono raccolte, chi le utilizza, chi le mantenga e per quale scopo. La privatezza include anche il diritto dell'individuo di rilasciare o meno le informazioni che lo riguardano. L'**anonimato** invece riguarda l'**impossibilita' di risalire all'artefice di una certa azione**, dunque la possibilita' di un individuo di rilasciare o meno la propria identita', il che, comunque, e' difficile da garantire nel web per via del tracciamento IP.

Integrita'

Garantire integrita' significa **assicurare che le infomazioni non siano alterabili dagli utenti non autorizzati** (in maniera invisibile rispetto quelli autorizzati). Non importa l'origine dei dati (autenticazione), in quanto durante il percorso dell'invio di un messaggio, quest'ultimo potrebbe essere stato alterato prima dell'arrivo al destinatario. Un sinonimo di mancanza di integrita' e' falsificazione.

Disponibilita'

Si intende garantire l'**accesso alle informazioni ad utenti autorizzati**, assicurando che un sistema sia operativo e funzionante in ogni momento, dunque proteggendosi da eventuali attacchi informatici.

A volte queste 3 proprieta' entrano in **confitto** tra di loro, per questo e' importante tener conto del contesto nel quale operiamo in modo da poter definire quale proprieta' ha priorita' sulle altre.

Altre proprieta'

- **Autentication**: assicurare che i soggetti siano effettivamente chi affermano di essere;
- **Non repudiation**: assicurare che il mittente di un messaggio non possa negare il fatto di aver spedito il messaggio e il destinatario non possa negare di averlo ricevuto;
- **Safety**: assicurare di aver eseguito una serie di accorgimenti atti ad eliminare la produzione di danni irreparabili all'interno di un sistema (come la gestione

corretta delle eccezioni);
- **Reliability**: assicurare la prevenzione da eventi che possono produrre danni di qualsiasi gravita' al sistema.

Hackers e Crackers

Gli attacchi informatici possono essere di natura e con scopi ben diversi, spesso la metodologia e l'obiettivo dell'attacco sono realizzati da persone molto differenti tra di loro:

- **Hacker**: persona esperta di sistemi informatici in grado di introdursi in reti protette o in generale di acquisire un'approfondita conoscenza del sistema sul quale interviene, per poi essere in grado di accedervi o adattarlo alle proprie esigenze (hacker white hat);
- **Cracker**: hacker con fini illeciti (hacker black hat);
- **Script kiddie**: utente con poca o nessuna cultura informatica che utilizza malware creati da altri.

Gli hacker storici

Gli hacker storici, soprattutto prima del 2000, erano perlopiu' hacker white hat (ma non per questo non processati, perche' svolgevano comunuqe attivita' illecite) il cui profilo e' stato cosi' riassunto dall'FBI negli anni '90:

- Maschio;
- Tra i 14 e i 34 anni;
- Appassionato di computer (in media 57 ore a settimana davanti al PC);
- Informatico con una cultura che spazia da aspetti sistemistici a programmativi;
- Single;
- Senza interesse commerciale.

Kevin David Mitnick (detto Condor)

Inventore della tecnica dell'**IP Spoofing** e forte utilizzatore di **ingegneria sociale** per accedere a sistemi spesso di societa' molto grandi. Fu arrestato dall'FBI nel 1995 e una volta rilasciato gli fu negato l'accesso ad Internet dal 2000 al 2003, ora consulente e scrittore.

Onel A. de Guzman

Il 4 Maggio 2000 fece partire il virus "I love you":

> Spediva una mail dall'oggetto che recitava "I love you" e dal testo "kindly check the attached LOVELETTER coming from me". Una volta aperto l'allegato, partiva uno script in Basic che inviava a tutti gli indirizzi della rubrica di Outlook la stessa mail: la conseguenza era di chiudere e bloccare tutti i server di posta a causa del grande numero di mail inviati (DoS). Furono infettati circa 45mln di computer, tra cui alcuni della Camera dei Lords e del Pentagono; con un danno totale stimato di circa 15mld di dollari.

Gary McKinnon (detto Solo)

Durante un periodo di disoccupazione, il sistemista ha fatto intrusione in 97 server militari degli USA e della NASA. E' stato accusato dalla giustizia statunitense di aver fatto:

> La piu' grande intrusione informatica su computer appartenenti alla difesa che si sia mai verificata in tutti i tempi.

Minacce del Cyberspazio

Nel Cyberspazio esistono delle leggi come nel mondo reale, ma non tutti le osservano. Come nella realta', esistono anche dei capitali, e alcuni violano le regole specialmente per impossessarsi illecitamente di quei capitali. Pero', a differenza di quanto accade nella realta', e' possibile sferrare attacchi a distanza perche' Internet non ha confini naturali; questo implica anche difficolta' nella gestione degli attacchi in quanto bisogna tener conto sia delle leggi nazionali che di quelle internazionali, che spesso entrano in conflitto.

Terminologia

- **Vulnerabilita'**: debolezza del sistema che potrebbe permettere violazioni alla sicurezza del sistema stesso e causare danni (es. protezione inadeguata della rete, dipendenza da un'unica fontedi energia, mancato controllo degli accessi);
- **Minaccia**: circostanza o evento che potrebbe causare violazioni alla sicurezza (es. furto, malcontento dello staff);
- **Attacco**: evento che deliberatamente sfrutta una vulnerabilita' del sistema per violarne la sicurezza.

Tipologia di attacchi

- **Non dolosi**: senza volonta' esplicita
  - Disastri naturali;
  - Errori HW e SW;
  - Errori umani.
- **Dolosi**: utenti legittimi che abusano delle proprie autorizzazioni, o illegittimi che bypassano la sicurezza
  - Sabotaggio;
  - Intrusione;
  - Falsificazione dei dati;
  - Ricerca fraudolenta di informazioni;
  - Intercettazioni.

Problemi attuali

Nel Cyberspazio le minacce sono aumentate per via dello sfruttamento dell'**automazione** perche' l'attacco puo' venir replicato per migliaia di utenti e per migliaia di eventi:

- I microfurti possono creare dei veri e propri patrimoni (es. limare 1€ da ogni transazione VISA);
- I malware sono sempre piu' complessi da intercettare, e quindi l'attacco puo' continuare nel tempo;
- La privatezza viene spesso compromessa tramite il mining dei dati personali;
- E' possibile trarre profitto da attacchi con probabilita' di successo minima.

Inoltre per via della rapidita' della propagazione delle tecnologie, gli attacchi sono replicabili da utenti comuni (script kiddies).

Vulnerabilita' intrinseche del Cyberspazio

L'uso di Internet come canale di comunicazione implica l'esistenza molteplici vulnerabilita', in quanto Internet e' un sistema distribuito con connessione a reti eterogenee dove avviene interazione con SW sconosciuti e non fidati.

Omogeneita'

Pur essendo costituito da milioni di utenti, questi ragionano **monoculture**, dunque la tipologia di hardware, i sistemi operativi, SW e applicazioni installate sono spesso gli stessi. Cio' implica che lo stesso attacco e' replicabile in moltissime circostanze.

Costi della sicurezza

Nel mercato le aziende puntano ad uscire per prime con nuovi prodotti, spesso senza avere il tempo di testarlo a sufficienza. La fase di debugging spesso comincia quando il SW e' gia' in esercizio grazie anche al feedback degli utenti (market now, fix bugs later).

Predisposizione ai bug

Alcuni linguaggi di programmazione sono piu' difficili di altri (es. nell'ambito del controllo delle eccezioni e garbage collection) e quindi piu' predisposti ad avere bug.

Progettazione della sicurezza

La sicurezza non e' un prodotto, ma un processo - Schneier 2000. La sicurezza e' un concetto non assoluto, e vanno sempre specificati il contesto e da cosa ci si vuole proteggere.

La sicurezza informatica non e' come la crittografia (che e' una scienza esatta): la crittografia dimostra che e' impossibile violare l'algoritmo RSA in tempo non-polinomiale; ma quando trattiamo di sicurezza informatica vengono coinvolti molti piu' attori, non parliamo solo di matematica applicata. Gli attori, persone e macchine, costituiscono gli anelli della catena che possono mostrare delle vulnerabilita'.

La sicurezza e' una catena e la sua resistenza e' determinata dall'anello piu' debole.

La sicurezza informatica non e' neanche l'utilizzo delle password. L'uso delle password come sistema di autenticazione e' un sistema molto debole in quanto possono essere compromessi tramite:

- Attacchi dizionario;
- Attacchi forza bruta;
- Ottenimento dell'accesso al file delle password.

Infine, la sicurezza non e' l'utilizzo di un firewall, in quanto non posso essere sicuro che a livello trasporto riesca a filtrare tutti i possibili malware.

Stato dell'arte

La sicurezza e' una proprieta' di vari livelli architetturali (OS, rete, applicativo, ecc..) ed e' costosa nel senso di risorse computazionali, gestione, mentalita' e di utilizzo. Anche i colossi dell'informatica hanno a che fare con problemi di sicurezza informatica perche' spesso per garantirla sarebbe necessario ridisegnare completamente un sistema pre-esistente, il che non e' sempre possibile.

Pianificazione della sicurezza

La sicurezza va dunque pianificata tramite degli step:

- **Prevenzione**
  - Utilizzo di teconologie che rendano il sistema non vulnerabile:
    - Crittografia (quando comunico attraverso un canale insicuro);
    - Backup (per ovviare a problemi di disaster recovery).
  - Fare in modo che solo gli utenti autorizzati accedano alle risorse:
    - Uso dei badge (e non solo richiesta di password).

- **Rilevamento**
  - Verificare che il sistema funzioni come previsto:
    - In tempo reale;
    - Tramite file di log.
- **Reazione**
  - In caso si subisca un attacco, rilevare l'attacco in tempo reale e avere un "piano B" pronto (nel caso di un sito web e di attacco DoS, ci si puo' appoggiare ad un altro server come piano B).

Esempio di prevenzione:

- Suddividere la rete in sotto-aree a seconda del livello di sicurezza che si vuole ottenere utilizzando dell'HW adeguato (tramite router, switch, ecc);
- Verificare che la configurazione del server sia aggiornata e controllare periodicamente la pubblicazione di bug noti dei SW installati;
- Fare uso di SW che limitino le interazioni con Internet (mediante firewall, router screening, ecc);
- Usare applicazioni che integrano algoritmi di crittografia in grado di codificare i dati prima della loro trasmissione in rete (es PGP, SSH, SSL, ecc).

Una volta messi in piedi tutti questi accorgimenti possiamo ridurre la possibilita' che abbia luogo una violazione o perlomeno ridurre i danni che una violazione puo' portare. Tuttavia non e' possibile eliminare del tutto la possibilita' di attacco, per questo non e' sufficiente usare metodi preventivi, bisogna prepararsi in ogni caso al rilevamento di attacchi. Il rilevamento non e' sempre possibile in tempo reale e funziona soprattutto per attacchi gia' noti, nel caso in cui si applichino dei metodi non-convenzionali il rilevamento sara' decisamente piu' difficile.

La sicurezza ha un costo in termini di:

- Acquisto, applicazione e gestione di misure aggiuntive di sicurezza;
- Aumento del carico del sistema (diminuzione delle prestazioni generali);
- Accettazione dell'utente (che e' costretto ad immettere piu' volte le proprie credenziali o caratteristiche biometriche per accedere ad un servizio di particolare criticita').

La prevenzione va bilanciata in base al valore delle risorse da proteggere e al danno che una violazione a queste porterebbe.