Sicurezza

Alessandro Savioli

Marzo 2025

Contents

1 Capitolo 1 **2**
1.1 CIA 2
1.2 Livelli d'impatto 4
1.3 Un modello per la sicurezza informatica 5
1.4 Attacchi e Conseguenze 6
1.4.1 Rilascio non autorizzato 7
1.4.2 Inganno 7
1.4.3 Interruzione 8
1.4.4 Usurpazione 8
1.5 Attacchi passivi e attivi 9

2 Capitolo 2 **10**
2.1 Strumenti per la crittografia 10
2.2 Confidenzialità con chiave simmetrica 10

Introduzione
Secondo il **NIST** (National Institute of Standards and Technology) il termine *sicurezza informatica* può essere definito come:

> Misure e controlli che assicurino **confidenzialità, integrità e disponibilità** di asset del sistema informatico che includono hardware, software, firmware e informazioni processate, memorizzate e comunicate.

1 Capitolo 1

1.1 CIA

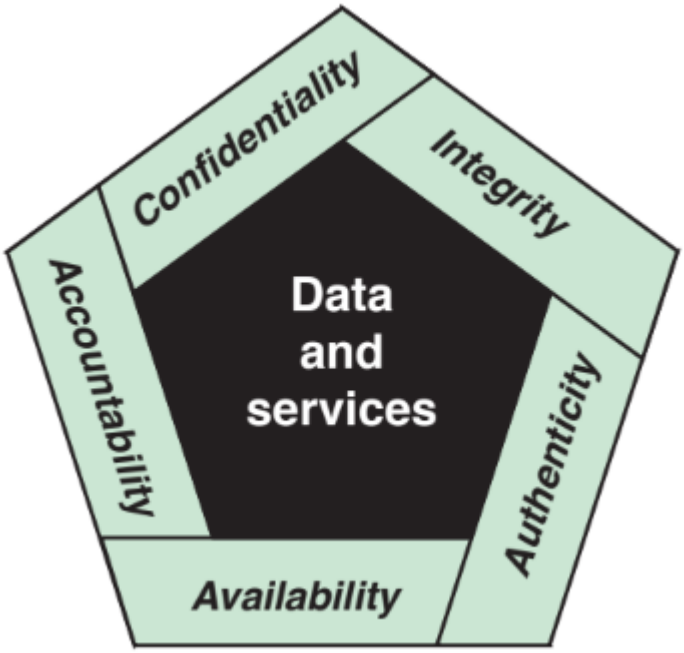
Nel campo della sicurezza informatica possiamo trovare tre obiettivi o requisiti principali:

- **Confidentiality**, ovvero preservare l'accesso autorizzato e prevenire la divulgazione di informazioni, come dati sensibili o proprietari;
- **Integrity**, ovvero la prevenzione contro la modifica o la distruzione impropria di informazioni, assicurando anche che un informazione non possa essere ripudiata oltre che quest'ultima sia autentica;
- **Availability**, ovvero assicurare l'accesso ad una determinata informazione.

A questi tre obiettivi principali se ne possono accostare ulteriori due, così da formare un quadro completo di tutto ciò che serve ad un sistema per essere sicuro:

- **Authenticity**, ovvero la proprietà di un utente di essere verificato e affidabile. Questo significa verificare che gli utenti siano chi dicono di essere e che gli input del sistema derivino sempre da una fonte affidabile;

- **Accountability**, ovvero la capacità di tracciare le attività di una qualsiasi entità all'interno del sistema, così da poter ricondurre un attacco ad un responsabile e tenere traccia di cosa sia successo per andare poi a migliorare la sicurezza del sistema.



1.2 Livelli d'impatto

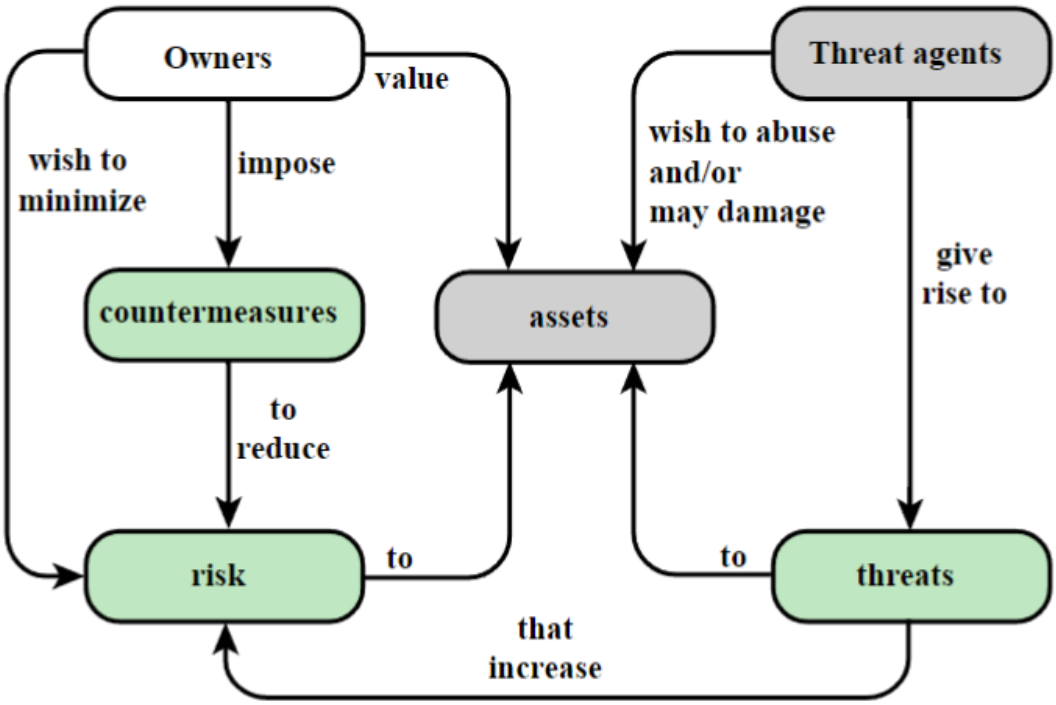
Analizziamo ora i diversi livelli d'impatto che un attacco può procurare ad una organizzazione:

1. **Impatto basso**, causa una degradazione lieve alle funzioni dell'organizzazione, che risulta ancora in grado di svolgere le sue funzioni principali ma con efficacia ridotta. Può causare danni **minori** ad assets, finanze o danni agli individui;

2. **Impatto moderato**, causa una degradazione significativa alle funzioni dell'organizzazione, che risulta ancora in grado di svolgere le proprie funzioni ma con efficacia nettamente ridotta. Può causare danni **significativi** ad assets e finanze o agli individui, senza includere perdite di vite;

3. **Impatto elevato**, causa una degradazione severa alle funzioni dell'organizzazione, che non risulta più in grado di svolgere una o più delle sue funzioni primarie. Può causare danni **severi o catastrofici** ad assets e finanze o agli individui, includendo anche perdite di vite.

1.3 Un modello per la sicurezza informatica



Diamo ora alcune nozioni su termini di base nella sicurezza informatica:

- **Systes Resource (Asset)**, che può essere hardware, software, dati o reti;
- **Vulnerability (di un asset)**, ovvero una debolezza nel sistema informatico, nelle procedure di sicurezza, controlli interni o nell'implementazione che potrebbe essere superata da un attacco. Possiamo distinguere 3 principali debolezze, in quanto un sistema può essere: **Corrupted, Leaky, Unavaiable**;
- **Threat (minaccia)**, ovvero ogni circostanza o evento con il

potenziale di avere un impatto negativo verso l'organizzazione o anche specifiche funzioni;

- **Adversary (threat agent)**, ovvero un individuo, un gruppo o una organizzazione che conduce o ha l'intento di condurre un attacco;
- **Attack**, qualsiasi tipo di attività malevola che prova a ottenere, distruggere, vietare o modificare le risorse di un sistema informatico o il sistema informatico stesso;
- **Countermeasure**, uno strumento o delle tecniche che hanno come obiettivo di proteggere o prevenire attacchi informatici;
- **Risk**, una misura che indica il rischio che una risorsa venga attaccata, che risulta essere il prodotto tra l'impatto negativo che si avrebbe se questa risorsa fosse attaccata e la probabilità che questo succeda;
- **Security Policy**, un insieme di criteri standard per la sicurezza di sistemi informatici o risorse.

1.4 Attacchi e Conseguenze

Possiamo suddividere le conseguenze di un attacco in 4 tipi:

1. Rilascio non autorizzato;
2. Inganno;
3. Interruzione;
4. Usurpazione.

Cerchiamo di vederli nel dettagli e capire quali sono gli attacchi che possono portare a queste conseguenze:

1.4.1 Rilascio non autorizzato

Il rilascio non autorizzato si verifica quando un'entità non autorizzata ottiene l'accesso ad informazioni. Gli attacchi che portano a questa conseguenza possono essere di tipo:

- **Exposure**, in cui un utente autorizzato invia direttamente delle informazioni ad un utente non autorizzato;
- **Interception**, in cui un utente non autorizzato accede a delle informazioni che stanno passando in rete tra due utenti autorizzati;
- **Inference**, in cui un utente non autorizzato ottiene indirettamente l'accesso a dei dati grazie a delle caratteristiche o scarti della comunicazione;
- **Intrusion**, in un utente non autorizzato ottiene l'accesso a dei dati dopo aver superato le protezioni di sicurezza.

1.4.2 Inganno

L'inganno si verifica quando un'entità autorizzata riceve una falsa informazione credendo che sia vera. Gli attacchi che portano a questa conseguenza sono di tipo:

- **Masquerade**, in cui un'entità non autorizzata ottiene l'accesso al sistema e si finge un utente autorizzato;
- **Falsification**, in cui false informazioni ingannano un'entità autorizzata;
- **Repudiation**, in cui un'entità ne inganna un'altra negando la responsabilità di un'azione ingiustamente.

1.4.3 Interruzione

Un'interruzione si verifica quando un attacco blocca il corretto funzionamento dei servizi di un sistema. Gli attacchi che portano a questa conseguenza sono di tipo:

- **Incapacitation**, interrompe una o più funzioni di sistema disabilitando un componente di sistema;
- **Corruption**, altera le operazioni di sistema modificando delle funzioni o i dati;
- **Obstruction**, interrompe i servizi di sistema ostacolando le operazioni.

1.4.4 Usurpazione

Un'usurpazione si verifica quando un'entità non autorizzata prende il controllo del sistema o di alcune funzioni di esso. Gli attacchi che portano a questa conseguenza sono di tipo:

- **Misappropiation**, in cui un'entità assume il controllo fisico o logico non autorizzato di una risorsa di sistema;
- **Misuse**, in cui si spinge un componente di sistema a svolgere azioni che abbassano il livello di sicurezza del sistema.

1.5 Attacchi passivi e attivi

Nel campo della sicurezza informatica possiamo distinguere due tipi di attacchi:

1. **Passivo**, caratterizzato dal fatto che le risorse di sistema non vengono in nessun modo intaccate, l'intento è solo quello di estrapolare informazioni, questo è possibile in due modi:
   - Rilascio di contenuti di messaggi;
   - Analisi del traffico.
2. **Attivo**, caratterizzato dall'intenzione di andare ad intaccare risorse di sistema o le sue operazioni, per questo tipo di attacco possiamo evidenziare quattro categorie:
   - **Attacco replay**, dove ci si impossessa di un'unità di informazioni e la si ritrasmette per produrre un effetto non autorizzato;
   - **Attacco Masquerade**, dove un'entità finge di essere un'entità autorizzata;
   - **Modifica dei messaggi**, dove alcune porzioni di un messaggio leggittimo vengono alterate, oppure vengono ritardati o riordinati alcuni di questi per produrre un effetto non autorizzato;
   - **Denial of Service**, dove si inibisce il normale uso dei canali di comunicazione.

2 Capitolo 2

2.1 Strumenti per la crittografia

Un elemento importante in tutti i servizi e applicazioni di sicurezza è sicuramente l'uso di algoritmi per la crittografia. Questo capitolo fornisce una panoramica sui vari tipi di algoritmo, insieme alla loro applcabilità.

2.2 Confidenzialità con chiave simmetrica