Sicurezza delle Reti

Riccardo Aziani

Ottobre 2024

Indice

Capitolo 1

Standard e Concetti base

1.1 Sicurezza informatica - definizioni

Ci sono standard internazionali a cui si può fare riferimento quando si parla di sicurezza; utilizzando questi standard si può determinare se un sistema è sicuro o meno.

- insieme di approcci, linee guida, strumenti che possono essere utilizzate per proteggere l'ambiente e le risorse dell'organizzazione e degli utenti
- i beni dell'organizzazione e degli utenti comprendono i dispositivi connessi, il personale, infrastrutture, ecc. e la totalità delle informazioni trasmesse e/o archiviate nel cyberspazio
- la sicurezza informatica si impegna a garantire il raggiungimento e mantenimento delle proprietà di sicurezza dell'organizzazione contro i possibili rischi

La sicurezza informatica si può divedere in:

- **Sicurezza delle informazioni:** devono essere rispettate le proprietà come integrità, confidenzialità e disponibilità
- **Sicurezza della rete:** protezione delle reti e del loro servizio da modifiche non autorizzate; garanzia che la rete svolga sempre le sue funzioni correttamente

Le sfide della sicurezza informatica

- La sicurezza non è semplice (requisiti semplici ma meccanismi complessi)
- Nello sviluppo di un meccanismo di sicurezza, si devono sempre considerare potenziali attacchi

- Decidere dove utilizzare i meccanismi di sicurezza (fisicamente in che punto della rete e logicamente a che livello dell'architettura)
- I meccanismi di sicurezza generalmente coinvolgono più di un algoritmo o protocollo
- Battaglia tra progettista e attaccante
- Percezione di scarsi benifici dall'investemento nella sicurezza (fino a quando non si verifica un errore)
- La sicurezza richiede un monitoraggio costante
- La sicurezza è troppo spesso a posteriori (dopo che il sistema è stato progettato)
- La sicurezza avanzata può rappresentare un impedimento al funzionamento efficiente e di facile utilizzo

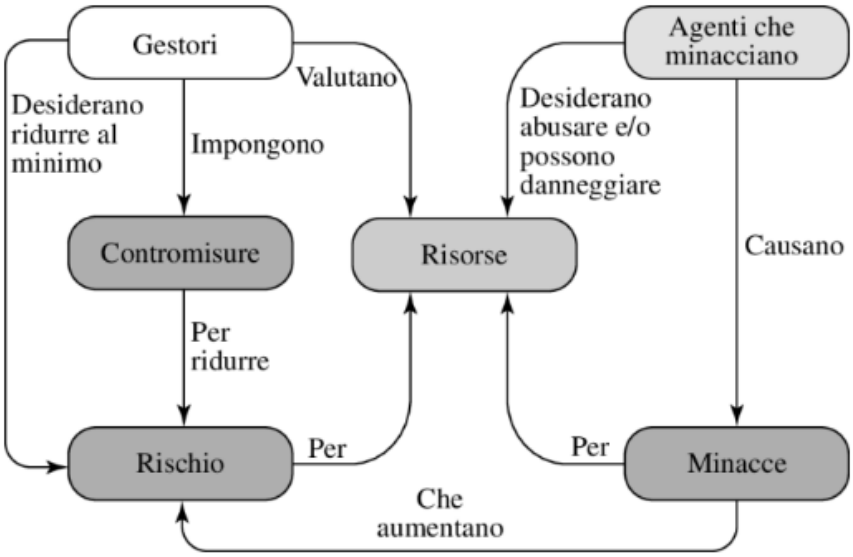

Figura 1.1: Concetti di sicurezza

- **Attacchi** alla sicurezza: qualsiasi azione che comprometta la sicurezza di un'informazione
- **Meccanismi** di sicurezza: un processo progettato per rilevare, prevenire o recuperare da un attacco
- **Servizi** di sicurezza: contrastano gli attacchi, si avvalgono di uno o più meccanismi per fornire il servizio

Attacchi passivi e attivi

- **Attacchi passivi:** NON alterano le informazioni; lo scopo dell'attacco è ottenere informazioni sui messaggi trasmessi
  - accesso al contenuto del messaggio
  - analisi del traffico di rete (la frequenza o la lunghezza dei messaggi potrebbero rivelare la natura della comunicazione)
- **Attacchi attivi:** modificano il flusso delle informazioni
  - fingere di essere qualcun'altro
  - denial of service

1.2 Minacce e conseguenze

Per threat si intende una potenziale violazione della sicurezza.

Le azioni che potrebbero causare una violazione devono essere protette o preparate; queste azione vengono chiamate **attacchi**.

Le minacce possono essere divise in quattro gruppi:

- **Divulgazione non autorizzata;** è una minaccia alla confidenzialità.
  - **esposizione**: un errore umano, software o hardware conduce alla rivelazione di dati sensibili
  - **intercettazione**
  - **inferenza**: l'attaccante è in grado di ottenere dalla sola osservazione del traffico
  - **intrusione**: un attaccante ottiene accesso a dati sensibili superando un controllo di accesso
- **Inganno;** è una minaccia all'integrità dei dati.
  - **mascheramento:** tentativo da parte dell'attacante di ottenere l'accesso a un sistema fingendosi un utente autorizzato
  - **falsificazione:** alterazione di dati validi o inserimento di dati falsi in un database
  - **ripudio:** un utente rinnega di aver inviato o ricevuto dei dati
- **interruzione;** è una minaccia alla disponibilità o integrità di un sistema
  - **interdizione:** danneggiamento dell'hardware
  - **corruzione:** le risorse funzionano in modo non voluto
  - **ostruzione:** interferire con le comunicazioni alterandone i collegamenti

- **usurpazione;** è una minaccia all'integrità del sistema.
  - **approprazione indebita:** ad esempio una sottrazione del servizio (DDOS)
  - **uso improprio:** ad esempio dopo che un utente ha ottenuto un accesso non autorizzato

Superificie di attacco

È costituita dalle vulnerabilità raggiungibili e sfruttabili in un sistema, come ad esempio:

- le porte aperte verso l'esterno
- servizi disponibili all'interno di un firewall
- codice che elabora dati in entrata
- un dipendente con accesso a dei dati sensibili (social engeneering)

Alcune superfici di attacco:

- **superificie di attacco di rete**; sono incluse vulnerabilità del protocollo di rete
- **superificie di attacco software**; sono incluse vulnerabilità nel codice delle applicazioni
- **superificie di attacco umano;** sono incluse vulnerabilità create dal personale (errori, social engeneering)