# [Sicurezza informatica](https://fad.its-ictpiemonte.it/course/view.php?id=943)

rischio = è la probabilità di ricevere un danno rischio = probabilità . danno

nella valutazione del rischio si cercherà di ridurre la probabilità che accada l'evento (non arriverà mai a zero) e il danno creando metodi di fuga per evitare perdite.

sicurezza informatica:Cosa vogliamo proteggere?

-Livello personale: Finanze,Sanità,Identità,Sociale,Lavoro,Hardware

-Livello aziendale:Idee e brevetti,Finanze,Hardware/Software,Dipendenti,Clienti

-Livello nazionale:Cittadini,Energia,Comunicazione,Segreti,Intelligence,Cyber Warfare

* Confidenzialità: COMPONENTE DELLA PRIVACY proprietà che indica che le informazioni siano o no disponibili a terzi
* Integrità: Assicura che la completezza e l'accuratezza siano identiche all'originale
* Disponibilità: Le informazioni devono essere disponibili quando richiesti

TIPOLOGIA DI ATTACCHI ATTIVI

mascheramento repitizione

spoofing replay modifica ripudio denial of service

TIPOLOGIA DI ATTACCHI PASSIVI

Lettura dei messaggi

SCRIPT KIDDIES: hacker novellini che scaricano potenti malware sviluppati da professionisti uno esempio sarebbe “kali linux”

WHITE HAT:hacker etico

GRAY HAT: spinto dalla curiosità ma illegale ma non per scopo di lucro

BLACK HAT: illegale con o senza vantaggio personale profitto economico o politico

ORGANIZED HACKERS

organizzazioni criminali hacktivist state-sponsored

MINACCE INTERNE

* malicious insider:vende informazioni di azienda
* inside agent: Dipendenti malintenzionati per far cadere la concorrenza
* emotional employees: dipendenti che provoca danni a causa vendetta
* reckless employees dipendenti che non seguono le regole di sicurezza
* third- party users: collaboratore che si avvale dei dati

VULNERABILITA

* zero day: una qualunque vulnerabilità non nota agli sviluppatori
* exploit: un attacco che sfrutta una vulnerabilità per eseguire un rootkit o provocare comportamenti imprevisti
* rootkit: un software malevolo in grado di mascherare la propria presenza ideato per abilitare l'accesso ad un sistema
* backdoor: un metodo alternativo all'autenticazione per superare le difese informatiche di un sistema

SOFTWARE HARDWARE PROTOCOLLI

MALWARE

VIRUS TROJAN WORM RANSOMWARE BOTNET SPYWARE KEYLOGGER SCAREWARE/ROGUEWARE

tecniche di intrusioni

tempi di attacco