Esercizio Teorico: Cloud, Backup e RAID Studente

Studente: Rocco Paolo Caccamo

Corso: Cybersecurity & Ethical Hacking

Data: 12 Febbraio 2026

---

1. Ricerca sui principali fornitori di servizi cloud

I tre principali provider che dominano il mercato globale. Dal punto di vista della sicurezza informatica, condividono il modello di responsabilità condivisa, ma hanno specificità diverse:

- **AWS (Amazon Web Services)**
  - **Descrizione:** È il pioniere del cloud computing e attuale leader di mercato per quota di utilizzo. Offre la gamma di servizi più ampia (oltre 200).
  - **Caratteristiche:** Estrema flessibilità e granularità. È la scelta standard per molte architetture "cloud-native".
  - **Focus Security:** Dispone di strumenti molto avanzati per la gestione degli accessi (IAM), ma la complessità di configurazione porta spesso a errori umani (es. *S3 Buckets* lasciati pubblici).
- **Microsoft Azure**
  - **Descrizione:** La piattaforma cloud di Microsoft, progettata per integrarsi perfettamente con i software aziendali esistenti (Windows Server, Office, Active Directory).
  - **Caratteristiche:** È leader nelle soluzioni "Ibride" (che collegano i server fisici dell'azienda al cloud).
  - **Focus Security:** Il fulcro è la gestione dell'identità tramite **Entra ID** (ex Azure AD). È il bersaglio principale per attacchi che mirano a scalare i privilegi dai sistemi locali al cloud.
- **Google Cloud (GCP)**
  - **Descrizione:** Costruito sull'infrastruttura che fa girare Google (Search, YouTube).
  - **Caratteristiche:** Eccelle nella gestione dei dati (Big Data), Intelligenza Artificiale e container (Kubernetes).
  - **Focus Security:** Molto automatizzato, ma richiede attenzione nella gestione delle chiavi API e dei *Service Account*, spesso bersaglio di furto se lasciati nel codice.

---

2. Descrizione dei Modelli di Servizio Cloud

I modelli di servizio definiscono quanto controllo (e quanta responsabilità di sicurezza) ha l'utente rispetto al provider.

- **IaaS (Infrastructure as a Service)**
    - **Descrizione:** Il provider offre risorse di calcolo virtualizzate (CPU, RAM, Storage, Rete). L'utente deve installare e gestire il Sistema Operativo e i software.
    - **Esempio:** Amazon EC2, Azure Virtual Machines, Google Compute Engine.
    - **Vantaggi:** Massimo controllo sulla configurazione del server (simile a un server fisico).
    - **Nota Security:** L'utente è responsabile del patching del sistema operativo e della configurazione del firewall.
- **PaaS (Platform as a Service)**
    - **Descrizione:** Il provider fornisce una piattaforma hardware e software pre-configurata per sviluppare applicazioni. L'utente gestisce solo il codice e i dati.
    - **Esempio:** AWS Elastic Beanstalk, Google App Engine, Heroku.
    - **Vantaggi:** Sviluppo rapido, nessuna preoccupazione per la manutenzione dei server o gli aggiornamenti del sistema operativo.
    - **Nota Security:** La sicurezza dell'infrastruttura è gestita dal provider; l'utente deve concentrarsi sulla sicurezza del codice (AppSec).
- **SaaS (Software as a Service)**
    - **Descrizione:** Il provider gestisce l'intera infrastruttura e l'applicazione. L'utente accede al software via internet (solitamente browser).
    - **Esempio:** Google Workspace (Gmail), Microsoft 365, Salesforce, Dropbox.
    - **Vantaggi:** Nessuna installazione, accessibilità immediata da qualsiasi dispositivo.
    - **Nota Security:** Il perimetro di sicurezza è l'**Identità**. La protezione dipende quasi interamente dalla robustezza delle password e dall'uso della MFA (Multi-Factor Authentication).

---

3. Conclusioni e Sintesi per la Sicurezza

Da questo esercizio emergono tre pilastri fondamentali per il nostro percorso di Ethical Hacking:

1. **Il Cloud non è magico, è il computer di qualcun altro.** Spostare i dati nel cloud non significa delegare la sicurezza *in toto*. Il provider protegge il perimetro fisico e l'hardware (Security *of* the Cloud), ma sta a noi proteggere i dati, gestire gli accessi e configurare i firewall (Security *in* the Cloud).
2. **La minaccia #1 è la "Misconfiguration".** La maggior parte dei *data breach* su AWS o Azure non avviene perché gli hacker hanno "bucato" l'infrastruttura di Amazon o

Microsoft, ma perché gli amministratori hanno lasciato permessi troppo aperti. Il nostro lavoro è individuare questi errori umani prima che vengano sfruttati.