M5 - Progetto Finale - Soluzione Completa

La "Soluzione Completa" integra le misure preventive contro SQLi/XSS e la strategia di risposta al malware in un'unica visione architetturale. Questo dimostra come l'infrastruttura possa essere progettata per proteggersi da minacce comuni e, al contempo, per reagire efficacemente a incidenti di sicurezza per contenere i danni.

Componenti chiave della soluzione integrata:

- Web Application Firewall (WAF): Posizionato di fronte all'applicazione e-commerce nella DMZ, continua a filtrare il traffico in entrata, proteggendo da attacchi a livello applicativo come SQLi e XSS.
- Isolamento della DMZ: Il firewall tra la DMZ e la Rete Interna è configurato per bloccare il traffico in uscita dalla DMZ verso la rete interna, prevenendo la propagazione di malware in caso di compromissione dell'applicazione di e-commerce.
- Indicazione di infezione: L'applicazione di e-commerce è visivamente indicata come infetta da malware, illustrando uno scenario post-compromissione in cui le misure di contenimento sono attive.

Rappresentazione Architetturale