M5 - Progetto Finale - Response

La priorità indicata è chiara: prevenire la propagazione del malware sulla rete interna, accettando che l'attaccante possa mantenere l'accesso alla macchina infetta. Questo richiede una strategia di contenimento rigoroso.

Soluzione Proposta: Isolamento della DMZ e Segmentazione della Rete tramite Firewall

La misura più efficace in questo scenario è sfruttare e rafforzare il firewall esistente tra la DMZ e la "Rete interna" per isolare completamente la zona compromessa.

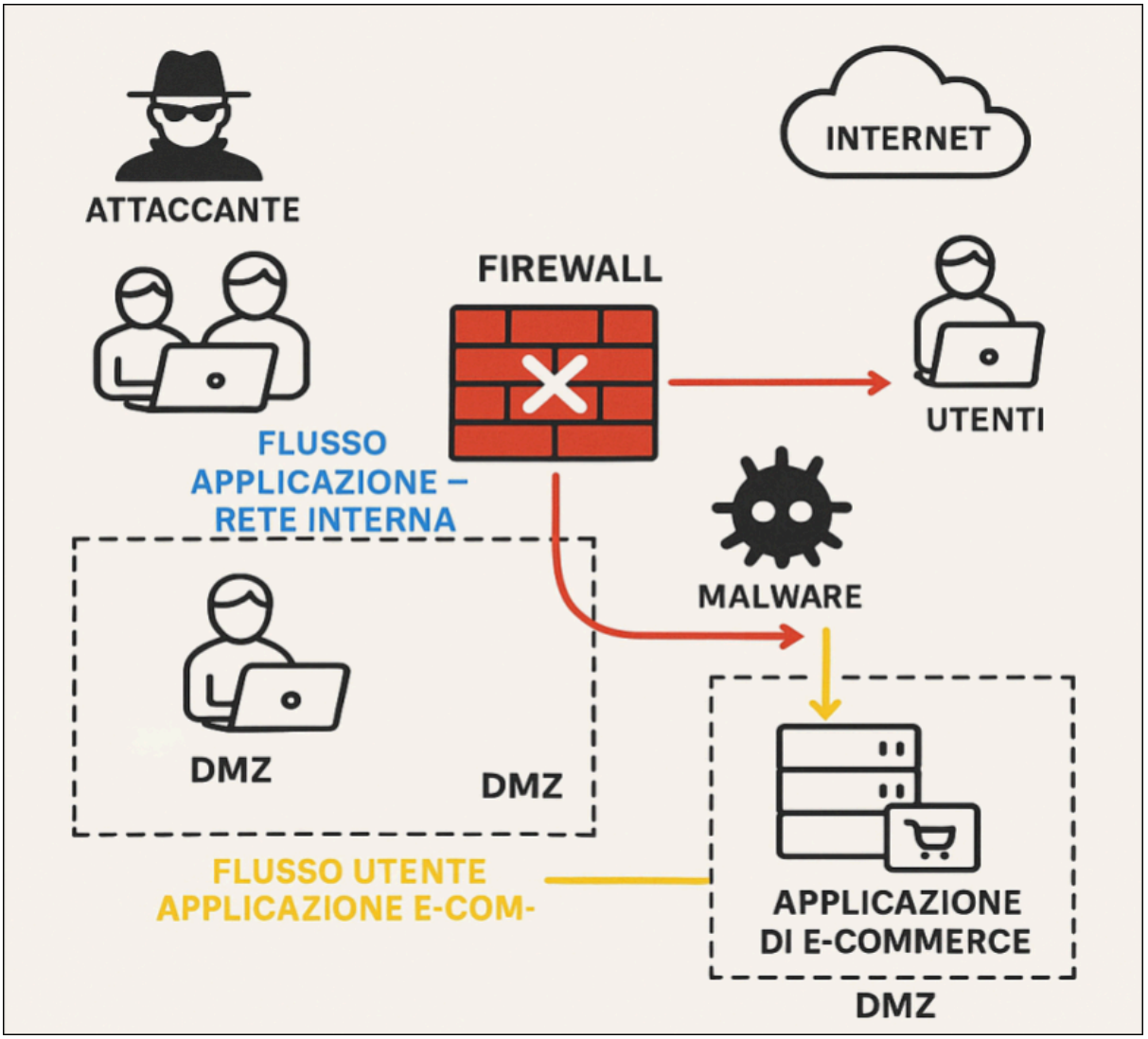
Azione Principale: Rafforzamento delle Regole del Firewall

- Implementazione: Il firewall posizionato tra la DMZ e la "Rete interna" deve essere immediatamente configurato per bloccare **tutto il traffico in uscita dalla DMZ verso la "Rete interna"**. Ciò significa che qualsiasi tentativo del malware (o dell'attaccante tramite la macchina infetta) di stabilire connessioni verso i sistemi o gli utenti nella rete interna verrà bloccato.
- Funzionalità: Questo tipo di regola di firewall, basata sul "deny by default" per il traffico da DMZ a interno, impedisce al malware di eseguire scansioni di rete, tentativi di exploit, o di stabilire comunicazioni C2 (Command and Control) con altre macchine all'interno della rete aziendale. In pratica, la DMZ diventa una "gabbia" per il malware.
- Benefici: Garantisce che il malware rimanga confinato all'interno della DMZ, proteggendo gli asset critici e i dati sensibili presenti nella "Rete interna" dalla compromissione. La priorità di non propagazione è soddisfatta efficacemente.

Considerazioni Aggiuntive (se applicabili)

- Revisione del traffico legittimo DMZ→Rete interna: Se esistono flussi applicativi legittimi dalla DMZ verso la rete interna (come ad esempio connessioni a database interni o servizi di autenticazione), questi dovrebbero essere esaminati attentamente. Idealmente, tali flussi dovrebbero essere già minimi e basati sul principio del minimo privilegio. In una situazione di infezione, si potrebbe considerare di disabilitarli temporaneamente o di monitorarli con estrema attenzione fino alla bonifica.

Rappresentazione Architetturale della Response



Conclusioni

Di fronte a un'infezione malware sulla macchina dell'applicazione e-commerce, la priorità di impedire la propagazione sulla rete interna è cruciale per la continuità del business e la protezione dei dati sensibili. La strategia più efficace per raggiungere questo obiettivo, data l'architettura fornita, consiste nel rafforzare immediatamente le regole del firewall esistente tra la DMZ e la rete interna. Bloccando quasi tutto il traffico in uscita dalla DMZ verso l'ambiente interno, si crea una barriera invalicabile che confina il malware, impedendogli di compromettere ulteriori sistemi. Sebbene si accetti temporaneamente l'accesso dell'attaccante alla macchina infetta, questo contenimento mirato minimizza il raggio d'azione dell'attacco e protegge l'integrità complessiva dell'infrastruttura di rete.