Cybersecurity Specialist

Cyber Security & Ethical Hacking

PROGETTO

Alejandro Cristino
S9-L5

TRACCIA

Con riferimento alla figura in slide 3, rispondere ai seguenti quesiti. Esercizio Traccia e requisiti
1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica

2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 3 con la soluzione proposta .

4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica «più aggressiva» dell'infrastruttura: anche una soluzione al punto 2) integrando eventuali altri elementi di sicurezza (integrando Budget 5000-10000 euro. Eventualmente fare più proposte di spesa

FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COMMERCE

Hacker

Rete Interna

Firewall

Internet

Utenti

DMZ

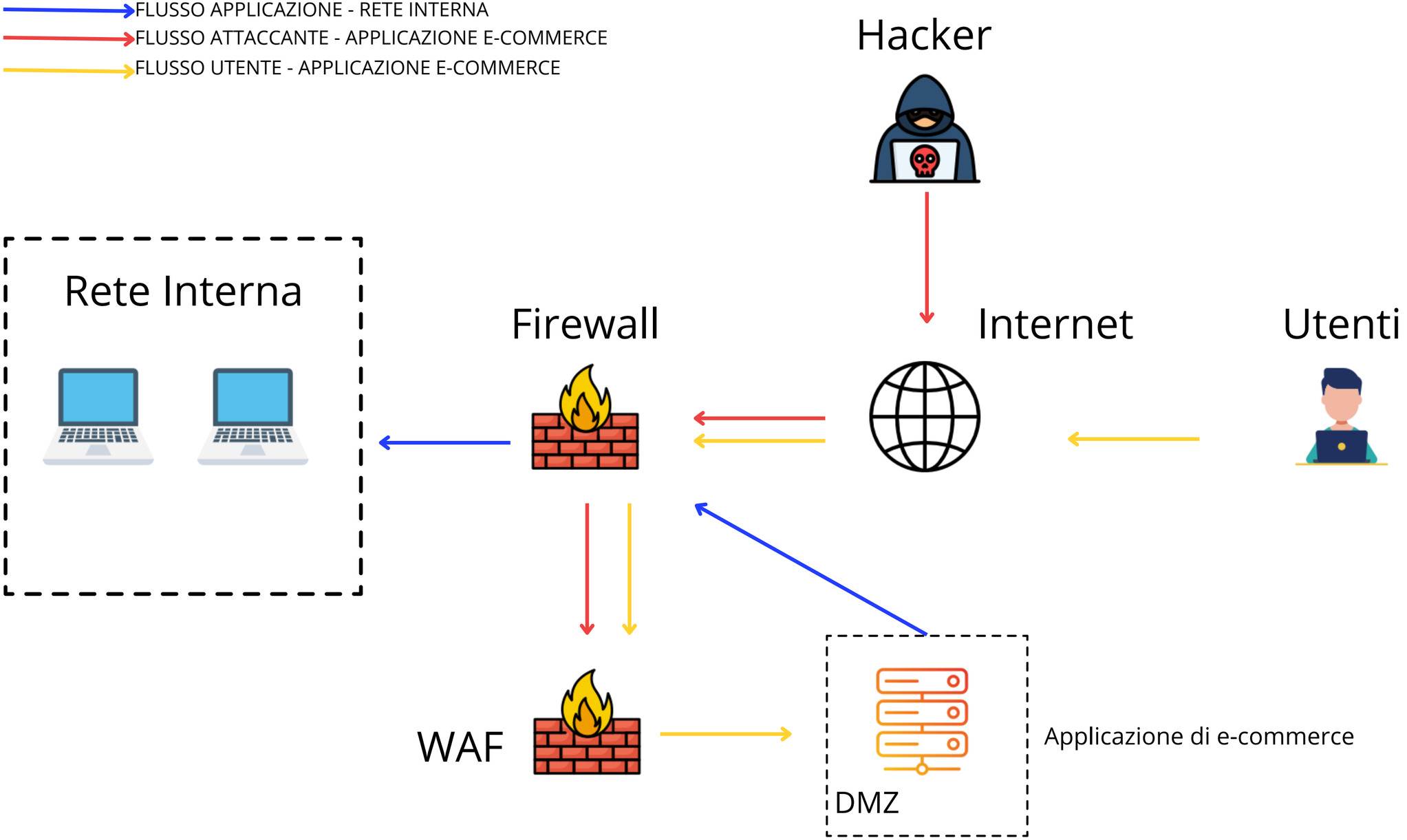
Applicazione di e-commerce

1. AZIONI PREVENTIVE: PREVENIRE ATTACCHI DI TIPO XSS E SQLI

Per prevenire attacchi come XSS e SQLi, e in generale qualsiasi tipo di attacco alle applicazioni web, è fondamentale implementare un Web Application Firewall (WAF) ben configurato. Questo strumento monitora il traffico e limita le richieste inviate alle applicazioni, garantendo così l'accesso solo agli utenti autorizzati.

Vediamo ora come implementare un WAF nella configurazione precedente.

FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COMMERCE



2. IMPATTI SUL BUSINESS

Scenario: Un attacco DDoS rende l'applicazione web non raggiungibile per 10 minuti. L'impatto economico è calcolato considerando che in mogni minuto gli utenti spendono 1.200 €.

Calcolo dell'impatto:

- Impatto economico: 10 minuti * 1.200 € = 12.000 €

Valutazione delle azioni preventive:

Per minimizzare l'impatto degli attacchi DDoS e garantire la continuità del servizio, sono consigliate le seguenti azioni preventive:

1. Implementazione di una Soluzione di Mitigazione DDoS:
- Descrizione: Utilizzo di servizi specializzati che rilevano e mitigano gli attacchi DDoS in tempo reale. Questi servizi filtrano il traffico malevolo prima che raggiunga l'infrastruttura dell'azienda, riducendo il rischio di downtime.
- Vantaggi: Protezione contro un'ampia gamma di attacchi DDoS, riduzione dei tempi di inattività, miglioramento della disponibilità del servizio.

2. Bilanciamento del Carico e Ridondanza:
- Descrizione: Distribuzione del traffico tra più server tramite tecniche di bilanciamento del carico. Implementazione di server di backup e soluzioni geograficamente distribuite per garantire la continuità del servizio in caso di attacco.
- Vantaggi: Migliora la tolleranza ai guasti, riduce il carico su singoli punti di vulnerabilità e assicura una risposta rapida alle richieste degli utenti.

3. Monitoraggio Proattivo e Allerta in Tempo Reale:
- Descrizione: Implementazione di sistemi di monitoraggio per il traffico e le risorse di rete con capacità di allerta in tempo reale per rilevare comportamenti anomali o attacchi imminenti.
- Vantaggi: Consente di identificare e rispondere rapidamente agli attacchi, riducendo i tempi di risposta e minimizzando l'impatto sul business.

4. Test di Penetrazione e Simulazione di Attacchi:
- Descrizione: Esecuzione regolare di test di penetrazione e simulazioni di attacchi DDoS per identificare vulnerabilità e migliorare le difese.
- Vantaggi: Identificazione delle vulnerabilità, miglioramento delle strategie di difesa, preparazione del team per rispondere a incidenti reali.

3. RESPONSE: PROTEZIONE DELLA RETE INTERNA

Nel contesto delineato, l’applicazione web è stata compromessa da un malware e dobbiamo impedire che questo si diffonda all’interno della rete. Ci viene inoltre comunicato che è possibile mantenere il servizio infetto accessibile dall’esterno tramite internet.

Per affrontare questa situazione, dobbiamo implementere una strategia che si basi sull’isolamento della macchina compromessa. In questo scenario, la macchina sarà direttamente connessa a Internet, accessibile all’attaccante ma non più collegata alla rete interna.

La prossima slide mostra la configurazione di rete modificata per rappresentare quanto detto sopra.

FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COMMERCE

Hacker

Rete Interna

Firewall

Internet

Utenti

DMZ

Applicazione di e-commerce

4. SOLUZIONE COMPLETA

Obiettivo: Unire le misure preventive e di risposta per formare una soluzione di sicurezza completa.

Approccio:

- Sicurezza preventiva: Implementazione di un Web Application Firewall (WAF) ben configurato.
- Response: Implementazione di una strategia basata sull’isolamento della macchina compromessa.

La prossima slide rappresenta quanto detto sopra.

FLUSSO APPLICAZIONE - RETE INTERNA
FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
FLUSSO UTENTE - APPLICAZIONE E-COMMERCE

Hacker

Rete Interna

Firewall

Internet

Utenti

WAF

DMZ

Applicazione di e-commerce

5. MODIFICA “PIÙ AGGRESSIVA” DELL’INFRASTRUTTURA

Obiettivo: Potenziare la sicurezza dell’infrastruttura esistente integrando nuove soluzioni e miglioramenti, con un budget compreso tra 5000 e 10000 euro.

Proposte di spesa dettagliate:

1. Servizi di Protezione DDoS Avanzati:
• Descrizione: Abbonamento a servizi di mitigazione DDoS avanzati che offrono protezione contro un’ampia gamma di attacchi, inclusi attacchi volumetrici, a livello di protocollo e applicativi.
• Costo Stimato: 2000 - 3000 euro per un servizio annuale base, espandibile a soluzioni più complete a seconda delle esigenze.
2. Firewall di Nuova Generazione (NGFW):
• Descrizione: Implementazione di un firewall di nuova generazione che offre funzioni avanzate come l’ispezione del traffico in tempo reale, il controllo delle applicazioni, la prevenzione delle intrusioni e la protezione contro le minacce avanzate.
• Costo Stimato: 3000 - 4000 euro, a seconda delle funzionalità e delle licenze necessarie.
3. Sistemi di Rilevamento e Prevenzione delle Intrusioni (IDS/IPS):
• Descrizione: Installazione di un sistema IDS/IPS per monitorare il traffico di rete e rilevare attività sospette o malevoli, bloccando potenziali minacce prima che possano causare danni.
• Costo Stimato: 1500 - 2500 euro, in base alla complessità e al livello di protezione offerto.
4. Formazione e Sensibilizzazione sulla Sicurezza:
• Descrizione: Programmi di formazione per il personale IT e non IT per aumentare la consapevolezza delle minacce di sicurezza e migliorare le pratiche di gestione degli incidenti. Include corsi su riconoscimento delle phishing, gestione delle password e protocolli di sicurezza.
• Costo Stimato: 500 - 1000 euro, coprendo il costo di corsi online o seminari in aula.
5. Backup e Disaster Recovery:
• Descrizione: Potenziamento delle soluzioni di backup esistenti e implementazione di un piano di disaster recovery per garantire la continuità operativa in caso di attacchi o guasti.
• Costo Stimato: 500 - 1000 euro, per aggiornamenti hardware/software o servizi di backup cloud.

Allocazione del Budget:
Il budget totale disponibile (5000 - 10000 euro) sarà allocato in base alla priorità delle soluzioni e alle esigenze specifiche dell’organizzazione