PHANTOM SRL

REPORT

Risk Management

Prepared For :
EPIC EDUCATION srl

By Phantom srl

Alessio D'Ottavio
Davide Di Turo
Francesco Pio Scopece
Giuseppe Pignatello
Luca Iannone
Manuel Di Gangi
Marco Fasani

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

INDICE

TRACCIA

Utilizzando il framework di modellizzazione delle minacce di Adam Shostack, identifica una minaccia per un'azienda di sviluppo software. Su cosa stiamo lavorando? Cosa può andare storto? Che cosa faremo al riguardo? Abbiamo fatto un buon lavoro? Ripeti il processo, eseguendo una gap analysis per trovare i punti di miglioramento.

I controlli NIST SP 800-53 Rev. 5. possono aiutare nella modellizzazione delle minacce:
NIST SP 800-53 Rev. 5-Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-53A Rev. 5 -Assessing Security and Privacy Controls in Information Systems and Organizations

Il framework di modellizzazione delle minacce di Adam Shostack è un metodo strutturato per identificare e gestire le minacce alla sicurezza in un sistema o processo. Questo framework fornisce una struttura per comprendere e affrontare le minacce potenziali in modo proattivo, piuttosto che reagire solo dopo che si sono verificate delle violazioni di sicurezza.

Per identificare le minacce consideriamo il seguente scenario:

Su cosa stiamo lavorando?

L'azienda sta sviluppando una piattaforma di **home banking** disponibile sia per browser web che per applicazione su dispositivi mobili.

Cosa può andare storto?

Analisi delle vulnerabilità
Le vulnerabilità che potrebbero essere presenti includono:

- Vulnerabilità del Codice e della Progettazione:
  - Vulnerabilità di sicurezza del codice
  - Architettura non sicura
  - Utilizzo di librerie o framework non sicuri
  - Errori di codifica, come input non validato, che potrebbero rendere il sistema vulnerabile ad attacchi di tipo SQL injection o XSS.

- Gestione delle Sessioni e Autenticazione:
  - Scarsa gestione delle sessioni utente
  - Mancata gestione delle autenticazioni di terze parti
  - Problemi di gestione delle sessioni lato client
  - Debolezze nelle politiche di accesso e di autenticazione, che potrebbero consentire a utenti non autorizzati di accedere al sistema.

- Protezione e Crittografia dei Dati:
  - Implementazione errata della crittografia
  - Esposizione di informazioni sensibili
  - Mancanza di crittografia dei dati trasmessi tra il client locale ed il server, esponendo le informazioni a potenziali intercettazioni durante la comunicazione.

- Gestione e Manutenzione:
  - Manutenzione della sicurezza
  - Scarsa gestione degli aggiornamenti del software
  - Mancata gestione delle vulnerabilità di terze parti

- Gestione delle Risorse e Prestazioni:
  - Risorse non gestite
  - Problemi di prestazioni
  - Assenza di limiti di frequenza e controllo del rate

- Test e Monitoraggio:
  - Mancata gestione dei file caricati dagli utenti
  - Mancata gestione dei log e del monitoraggio
  - Mancata gestione dei test di sicurezza

- Interazione con Componenti Esterni:
  - Vulnerabilità nell'interazione con componenti esterni
  - Scarsa gestione degli aggiornamenti di sicurezza

- Altri Rischi:
  - Mancata gestione degli errori
  - Violazioni della privacy
  - Mancata esecuzione di backup
  - Disastri ambientali

Analisi delle minacce

Utilizzando il framework STRIDE, possiamo identificare le seguenti minacce:

- Spoofing: Un attaccante potrebbe fingersi un utente autorizzato per ottenere accesso illegittimo ai dati sensibili.
- Tampering: Manipolazione dei dati durante la trasmissione tra il server esterno e il database, compromettendo l'integrità dei dati.
- Repudiation: Un attaccante potrebbe negare di aver compiuto azioni dannose o non autorizzate, complicando la responsabilità e la gestione degli incidenti.
- Information Disclosure: Possibile esposizione di dati sensibili a causa di una comunicazione non sicura tra il server esterno e il database.
- Denial of Service (DoS): Attacco mirato per interrompere o degradare le prestazioni del sistema, rendendo indisponibili i servizi per gli utenti legittimi.
- Elevation of Privilege: Tentativo di ottenere accesso a privilegi più elevati del dovuto per eseguire operazioni non autorizzate sul sistema o sul database.

Che cosa faremo al riguardo?

Misure preventive e di mitigazione delle minacce

Utilizzando il framework di mitigazione DREAD, possiamo identificare le seguenti misure preventive:

- Defend: Implementazione di rigorosi controlli di accesso e autenticazione per garantire che solo gli utenti autorizzati possano accedere al sistema.
- Remedy: Validazione dei dati in ingresso per prevenire attacchi di tipo injection e utilizzo di crittografia per proteggere la comunicazione tra il server esterno e il database.
- Avoidance: Utilizzo di connessioni crittografate e protocolli sicuri per minimizzare il rischio di intercettazioni o manipolazioni dei dati durante la trasmissione.
- Early detection and response: Implementazione di sistemi di monitoraggio continuo per rilevare tempestivamente anomalie o attività sospette e rispondere rapidamente agli incidenti di sicurezza.

Controlli NIST SP 800-53 Rev. 5

Fornisce un insieme dettagliato di controlli di sicurezza e privacy che possono essere implementati per proteggere i sistemi informativi e le organizzazioni da una vasta gamma di minacce.

1. Identificazione della minaccia: La minaccia consiste nella compromissione dei dati sensibili dei clienti durante lo sviluppo, il testing o la distribuzione del software.
2. Analisi delle vulnerabilità: Considerando i controlli di sicurezza NIST SP 800-53 Rev. 5:
   - AC-2 Account Management: Verifica delle procedure per la gestione delle credenziali e l'accesso autorizzato ai dati.
   - SI-7 Software, Firmware, and Information Integrity: Protezione del software da modifiche non autorizzate durante lo sviluppo e la distribuzione.
   - SA-11 Developer Security Testing and Evaluation: Esecuzione di test di sicurezza durante lo sviluppo per identificare e correggere vulnerabilità.
   - CM-7 Least Functionality: Assicurarsi che il software contenga solo le funzionalità necessarie per ridurre la superficie di attacco.
   - PL-4 Rules of Behavior: implementazione di politiche e procedure per gestire correttamente le informazioni personali.
3. Pianificazione delle azioni correttive:
   - Implementare procedure di gestione delle credenziali e controllo degli accessi per garantire l'accesso autorizzato ai dati sensibili (AC-2).
   - Utilizzare firme digitali o controlli di integrità per proteggere il software da modifiche non autorizzate (SI-7).

- Integrare test di sicurezza durante il ciclo di sviluppo per identificare e correggere vulnerabilità (SA-11).
- Applicare il principio della "Least Privilege" per limitare l'accesso alle funzionalità necessarie (CM-7).
- Applicare norme stringenti per quanto riguarda il trattamento dei dati personali degli utenti (PL-4).

4. Valutazione del lavoro svolto:
   - Condurre valutazioni periodiche per garantire l'efficacia delle azioni correttive e l'adeguatezza dei controlli di sicurezza implementati.

Abbiamo fatto un buon lavoro?

Controlli NIST SP 800-53A Rev. 5
Fornisce linee guida dettagliate per valutare l'efficacia dei controlli di sicurezza e privacy implementati.

1. Identificazione dei Controlli di Sicurezza: Sono stati identificati e documentati tutti i controlli di sicurezza pertinenti implementati nel sistema, conformemente ai requisiti del NIST SP 800-53 Rev. 5.
2. Valutazione dell'efficacia dei controlli di sicurezza implementati:
   - RA-03 Risk Assessment: Valutazione del rischio associato alla compromissione dei dati sensibili durante lo sviluppo del software.
   - CA-07 Continuous Monitoring: Monitoraggio continuo dell'ambiente di sviluppo per identificare e rispondere alle minacce alla sicurezza.
   - RA-05 Vulnerability Scanning: Esecuzione di scansioni periodiche per identificare e correggere vulnerabilità nel software in fase di sviluppo.
   - SA-12 Supply Chain Protection: Valutazione e mitigazione dei rischi associati alla sicurezza nella catena di approvvigionamento del software.
   - AC-01 Policy and procedures: Controllo dellla politica di accesso basata sulla privacy, assicurando che le informazioni personali siano accessibili solo a coloro che hanno il diritto di accedervi.
3. Pianificazione dei controlli:
   - Effettuare valutazioni periodiche del rischio per identificare nuove minacce e aggiornare le contromisure di sicurezza (RA-3).
   - Implementare un sistema di monitoraggio continuo per rilevare e rispondere alle minacce alla sicurezza durante lo sviluppo del software (CA-7).
   - Utilizzare strumenti automatizzati per eseguire scansioni periodiche del software e correggere le vulnerabilità identificate (RA-5).
   - Collaborare con i fornitori per valutare e mitigare i rischi associati alla sicurezza nella catena di approvvigionamento (SA-12).
   - Valutazione del lavoro svolto: Valutare regolarmente l'efficacia dei controlli di sicurezza implementati e apportare miglioramenti continui in base alle valutazioni del rischio (AC-01).
4. Valutazione del lavoro svolto: Valutare regolarmente l'efficacia dei controlli di sicurezza implementati e apportare miglioramenti continui in base alle valutazioni del rischio.

GAP Analysis

La gap analysis confronta lo stato attuale con l'obiettivo desiderato, evidenziando le discrepanze e guidando le azioni correttive.

Obiettivi non raggiunti da affrontare - Cosa può andare storto bis.:

- Mancata gestione delle autenticazioni di terze parti;
- Implementazione errata della crittografia;
- Esposizione di informazioni sensibili;
- Manutenzione della sicurezza;
- Mancata gestione delle vulnerabilità di terze parti;
- Risorsa non gestita;
- Vulnerabilità nell'interazione con componenti esterni;
- Mancata gestione degli errori;
- Mancata esecuzione di backup;
- Disastri ambientali.

Controlli NIST SP 800-53 Rev. 5 - Cosa faremo a riguardo bis.

Fornisce un insieme dettagliato di controlli di sicurezza e privacy che possono essere implementati per proteggere i sistemi informativi e le organizzazioni da una vasta gamma di minacce.

1. Identificazione della minaccia: La minaccia consiste nella compromissione dei dati sensibili dei clienti durante lo sviluppo, il testing o la distribuzione del software.
2. Analisi delle vulnerabilità: Considerando i controlli di sicurezza NIST SP 800-53 Rev. 5:
    - IA-7 Identication e Authentication: implementazione di meccanismi di identificazione e autenticazione per gestire l'accesso ai sistemi informativi e alle risorse da parte di terze parti, come fornitori esterni, partner commerciali o appaltatori.
    - SC-28 System and communication protection: implementazione corretta e sicura della crittografia per proteggere le informazioni sensibili e le comunicazioni da accessi non autorizzati o compromessi.
    - RA-5 Risk Assestment: valutazione periodica dei controlli di sicurezza per identificare e mitigare le vulnerabilità, comprese quelle relative alla privacy, come specificato dal PL-4.
    - CM-2 Baseline Configuration: definire, documentare e applicare una configurazione di base sicura per i dispositivi, le applicazioni e i servizi, e di monitorare e gestire le modifiche alla configurazione per garantire la sicurezza e l'integrità del sistema.
    - CM-9 Configuration management plan: gestione della configurazione del sistema e stabilisce linee guida per garantire che tutti i componenti esternisiano adeguatamente gestiti e integrati nel sistema per garantire la sicurezza delle informazioni.

- RA-3 Risk Assesment: valutazione dei rischi associati agli errori, alle omissioni e alle azioni accidentali o deliberate che potrebbero compromettere la sicurezza delle informazioni o l'integrità dei sistemi.
- CP-9 System backup: pianificazione e l'esecuzione dei backup dei dati critici e dei sistemi informativi per garantire la disponibilità e l'integrità delle informazioni in caso di guasti o catastrofi.
- CP-2 Contingency Plan: sviluppo di piani di continuità operativa e di recupero di emergenza per affrontare una vasta gamma di eventi catastrofici, compresi i disastri naturali.

3. Pianificazione delle azioni correttive:
   - Durante la valutazione, sarà necessario verificare se i meccanismi di identificazione e autenticazione per terze parti sono implementati correttamente e se soddisfano i criteri stabiliti nei controlli di sicurezza. L'assenza di tali meccanismi o la loro implementazione errata potrebbero portare a una valutazione negativa della conformità. (IA-7)
   - Durante la valutazione, sarà necessario esaminare l'implementazione della crittografia per proteggere le informazioni sensibili e le comunicazioni. Se l'implementazione è carente o non adeguata, potrebbe essere identificata come un'area di non conformità e potrebbe indicare una vulnerabilità significativa. (SC-28)
   - La valutazione del rischio è un elemento chiave nelle valutazioni di conformità. Se le valutazioni del rischio non vengono condotte regolarmente o in modo completo, potrebbe essere segnalata una mancanza di conformità e una potenziale esposizione a rischi di sicurezza. (RA-5)
   - Durante la valutazione, sarà necessario esaminare se esiste una configurazione di base documentata e se è stata applicata correttamente. L'assenza di una configurazione di base sicura o la mancanza di monitoraggio delle modifiche potrebbe essere considerata una vulnerabilità significativa. (CM-2)
   - La presenza di un piano di gestione della configurazione efficace è fondamentale per garantire che le configurazioni siano gestite in modo appropriato e sicuro. L'assenza di un piano o la sua implementazione inadeguata potrebbero essere identificate come aree di non conformità durante la valutazione. (CM-9)

4. Valutazione del lavoro svolto: Valutare regolarmente l'efficacia dei controlli di sicurezza implementati e apportare miglioramenti continui in base alle valutazioni del rischio.

Abbiamo fatto un buon lavoro? bis.

Per valutare se abbiamo fatto un buon lavoro, dovremo condurre valutazioni regolari della sicurezza del software e del sistema nel suo complesso. Se siamo in grado di identificare e mitigare efficacemente i rischi e mantenere un alto livello di sicurezza dei dati, possiamo considerare di aver fatto un buon lavoro nella protezione del nostro software e dei nostri clienti

Codice Web App Home banking

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET


```
from flask import Flask, render_template, request, redirect, url_for
import sqlite3

app = Flask(HOME BANKING)

DATABASE = 'database.db'

def get_db_connection():
  conn = sqlite3.connect(DATABASE)
  conn.row_factory = sqlite3.Row
  return conn

@app.route('/login', methods=['GET', 'POST'])
def login():
  if request.method == 'POST':
    username = request.form['username']
    password = request.form['password']

    conn = get_db_connection()
    cursor = conn.cursor()
    cursor.execute('SELECT * FROM users WHERE username = ? AND password = ?', (username, password))
    user = cursor.fetchone()
    conn.close()

    if user:
      return redirect(url_for('dashboard'))
    else:
      return render_template('login.html', error="Credenziali non valide. Riprova.")

  return render_template('login.html')

@app.route('/dashboard')
def dashboard():
  # Recupera le informazioni dell'utente dal database e passale al template
  conn = get_db_connection()
  cursor = conn.cursor()
  cursor.execute('SELECT * FROM users WHERE username = ?', ('JohnDoe',))
  user_info = cursor.fetchone()
  conn.close()

  if user_info:
    return render_template('dashboard.html', user=user_info)
  else:
    return redirect(url_for('login'))

if __name__ == '__main__':
  app.run(debug=True)
```

Codice lato Server Home banking

```
#include <iostream>
#include <string>
#include <winsock2.h>
#include <ws2tcpip.h>
#include <random>
#include <chrono>
#include <thread>

#pragma comment(lib, "ws2_32.lib")

using namespace std;
using namespace chrono;

// Struttura per memorizzare le informazioni dell'utente
struct User {
    string id;
    string passwordHash;
    string sessionToken;
};

// Tempo massimo di attesa per l'autenticazione (2 minuti)
constexpr int MAX_AUTHENTICATION_TIME = 2 * 60;

// Funzione per generare un token di sessione casuale
string generate_session_token() {
    random_device rd;
    mt19937 gen(rd());
    uniform_int_distribution<> dis(0, 255);

    string token;
    for (int i = 0; i < 32; ++i) {
        token.push_back(dis(gen));
    }
    return token;
}

// Funzione per generare un codice OTP (One-Time Password) a 6 cifre
string generate_otp_code() {
    random_device rd;
    mt19937 gen(rd());
    uniform_int_distribution<> dis(100000, 999999);

    return to_string(dis(gen));
}

}
```

```
// Funzione per autenticare l'utente con l'autenticazione a due fattori
bool authenticate_user_two_factor(const string& id, const string& password, User& user) {
    // Autenticazione delle credenziali di base (ID e password)
    // Se l'autenticazione delle credenziali di base fallisce, restituisci false

    // Verifica il codice OTP (One-Time Password)
    string otp;
    cout << "Inserisci il codice OTP: ";
    cin >> otp;

    // Simuliamo la verifica del codice OTP
    string generated_otp = generate_otp_code();
    if (otp == generated_otp) {
        // Genera e memorizza un nuovo token di sessione
        user.id = id;
        user.passwordHash = password;
        user.sessionToken = generate_session_token();

        // Aggiorna il token di sessione nel database (simulato)

        return true;
    } else {
        cerr << "Codice OTP non valido. Connessione chiusa." << endl;
        return false;
    }
}

// Funzione per gestire una singola connessione
void handle_connection(SOCKET clientSocket) {
    try {
        string id, password;
        cout << "Inserisci ID: ";
        cin >> id;
        cout << "Inserisci password: ";
        cin >> password;

        User user;
        auto start_time = steady_clock::now();
        if (authenticate_user_two_factor(id, password, user)) {
            auto end_time = steady_clock::now();
            auto elapsed_seconds = duration_cast<seconds>(end_time - start_time).count();
            if (elapsed_seconds > MAX_AUTHENTICATION_TIME) {
                cerr << "Tempo massimo di attesa superato. Connessione chiusa." << endl;
                // Blocca il software per 5 minuti
                this_thread::sleep_for(minutes(5));
                // Invia una notifica al numero di telefono dell'utente (utilizza Twilio o un servizio simile)
```

```
            } else {
                cout << "Autenticazione riuscita. Token di sessione: " << user.sessionToken << endl;
            }
        } else {
            cerr << "Credenziali non valide. Connessione chiusa." << endl;
        }
    } catch (exception& e) {
        cerr << "Eccezione durante la gestione della connessione: " << e.what() << endl;
    }

    closesocket(clientSocket);
}

// Funzione per accettare le connessioni in arrivo
void start_accept(SOCKET serverSocket) {
    while (true) {
        sockaddr_in clientAddr;
        int clientAddrLen = sizeof(clientAddr);
        SOCKET clientSocket = accept(serverSocket, reinterpret_cast<sockaddr*>(&clientAddr),
&clientAddrLen);
        if (clientSocket != INVALID_SOCKET) {
            thread(handle_connection, clientSocket).detach();
        } else {
            cerr << "Errore durante l'accettazione della connessione: " << WSAGetLastError() << endl;
        }
    }
}

int main() {
    WSADATA wsaData;
    int iResult = WSAStartup(MAKEWORD(2, 2), &wsaData);
    if (iResult != 0) {
        cerr << "Errore durante l'inizializzazione di Winsock: " << iResult << endl;
        return 1;
    }

    SOCKET serverSocket = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
    if (serverSocket == INVALID_SOCKET) {
        cerr << "Errore nella creazione del socket: " << WSAGetLastError() << endl;
        WSACleanup();
        return 1;
    }

    sockaddr_in serverAddr;
    serverAddr.sin_family = AF_INET;
    serverAddr.sin_addr.s_addr = htonl(INADDR_ANY);
    serverAddr.sin_port = htons(8080);
```

```
if (bind(serverSocket, reinterpret_cast<sockaddr*>(&serverAddr), sizeof(serverAddr)) == SOCKET_ERROR) {
    cerr << "Errore nell'associazione del socket: " << WSAGetLastError() << endl;
    closesocket(serverSocket);
    WSACleanup();
    return 1;
}

if (listen(serverSocket, SOMAXCONN) == SOCKET_ERROR) {
    cerr << "Errore nella messa in ascolto del socket: " << WSAGetLastError() << endl;
    closesocket(serverSocket);
    WSACleanup();
    return 1;
}

start_accept(serverSocket);

closesocket(serverSocket);
WSACleanup();

return 0;
```

Il Programma :

Questo programma è un server che gestisce l'autenticazione degli utenti tramite un processo a due fattori, utilizzando un codice OTP (One-Time Password). Inizia inizializzando la libreria Winsock per consentire la comunicazione via socket. Successivamente, crea un socket TCP per accettare le connessioni in arrivo dai client e lo associa a una porta specifica e all'indirizzo IP locale. Il server poi inizia ad ascoltare le connessioni in arrivo utilizzando la funzione listen e accetta le connessioni utilizzando la funzione accept. Una volta accettata una connessione, avvia un nuovo thread per gestire la connessione.

Nel thread di gestione della connessione, il server richiede all'utente di inserire l'ID e la password e successivamente richiede anche il codice OTP. Se l'autenticazione è riuscita sia per l'ID e la password che per il codice OTP, il server genera un token di sessione e lo restituisce al client. In caso contrario, chiude la connessione. Il server utilizza funzioni apposite per generare il codice OTP e il token di sessione casuali.

Il server ha un tempo massimo di attesa per l'autenticazione (2 minuti). Se questo tempo viene superato, il server blocca l'accesso per 5 minuti e invia una notifica al numero di telefono dell'utente. Quando il server viene terminato, chiude il socket e rilascia le risorse utilizzate.

Conclusioni

L'azienda implementa diverse misure per affrontare le minacce, ma ci sono ancora alcuni punti di miglioramento identificati attraverso questa gap analysis. Concentrarsi su questi punti può aiutare l'azienda a rafforzare ulteriormente la sua sicurezza e a gestire meglio le minacce emergenti nel contesto del software finanziario.

GRAZIE

BY

PHANTOM SRL

Prepared For :
EPIC EDUCATION srl

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET