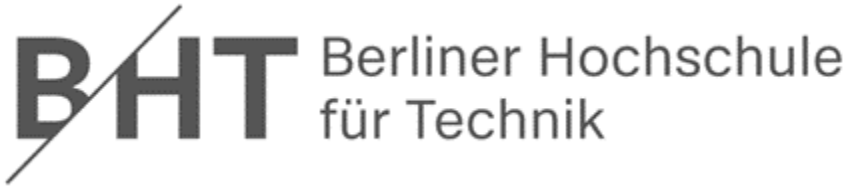
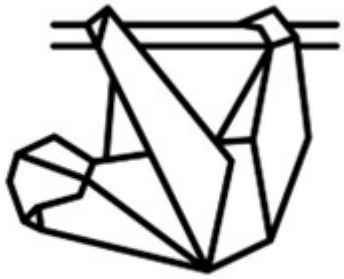


Fachbereich VI - Informatik und Medien
Studiengang IT-Sicherheit Online / Medieninformatik

Vorbereitung 7 - Bedrohungsmodellierung, Unternehmensebene



PARETO CONSULTING

Modul:	Sicherheitsmanagement
Dozent:	Sven Zehl
vorgelegt von:	Gruppe 1 Christine Kuczera Dirk Drutschmann Hicham Naoufal Michael Schröter Jan Zimmermann Ivo Valls

Aufgabe 1a) Ermitteln Sie im Rollenspiel Kosten der Sicherheit im Interview mit ihrem Geschäftsführer folgende Eckpunkte:

1. Unternehmenswerte 2) Anwenderanforderung 3) Sicherheitsziele
2. Angreifer

Antwort Nach Rücksprache mit dem Kunden, wurde Folgendes identifiziert:

Unternehmenswerte	**Anwenderanforderungen**	**Sicherheitsziele**	**Angreifer**
Auktionsdaten müssen vertrauenswürdig und unveränderlich sein	Auktionsdaten dürfen nicht manipulierbar sein	Integrität	Insider-Bedrohungen, Hacker
Zahlungsinformation	Zahlungsinformationen dürfen nicht an Unbefugte gelangen	Vertraulichkeit	Finanzamt, Hacker
Nur berechtigte User dürfen auf ihre Konten zugreifen und persönlicher Informationen müssen vertraulich behandelt werden	Sichere Authentifizierung mittels zweifelsfreier Identitätsprüfung	Authentizität	Phishing-Angreifer, Identitätsdiebe

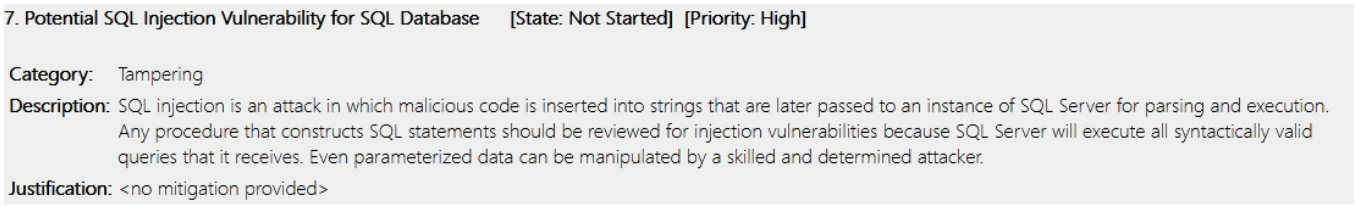
Aufgabe 1b) Laden Sie das Microsoft Threat Modeling Tool herunter, installieren Sie es und vollziehen Sie AntrAnw-I nach. - Windows.

Antwort

Das Microsoft Threat Modeling Tool bietet mit AntrAnw-I (Anwendung von Angriffszenarien auf Anwendungsschnittstellen) eine Methode zur Durchführung dieser Art von Analyse, indem es eine systematische und strukturierte Herangehensweise bietet, um potenzielle Bedrohungen zu identifizieren und zu bewerten. Es ermöglicht den Entwicklern, verschiedene Angriffszenarien auf die Anwendungsschnittstellen anzuwenden und daraus resultierende Risiken zu visualisieren, um geeignete Gegenmaßnahmen zu planen und umzusetzen.

Anhand einiger Beispiele aus dem angehangenen Report, würden sich folgende Maßnahmen ergeben.

SQL Injection


7. Potential SQL Injection Vulnerability for SQL Database [State: Not Started] [Priority: High]

Category: Tampering
Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
Justification: <no mitigation provided>

Art des Angriffs

Mittels speziell präperierten Eingaben, können Angreifer Code in der Datenbank ausführen.

Angreifer

Typischerweise wird diese Art von Angriff von automatisierten Tools und Skript Kiddies ausgeführt, da sehr niederschwellig ausnutzbar.

Mögliche Abwehrstrategien

Verwendung von prepared Statements und befolgen allgemein guter Programmierpraktiken.

Evaluation of Privilege Using Remote Code Execution

61. Web Auktionshaus May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Payment Service 1 may be able to remotely execute code for Web Auktionshaus.
Justification: <no mitigation provided>

Art des Angriffs

Schwachstelle in der Anbindung zu einem externen Bezahlservice, bieten die Möglichkeit schadhaften Code einzuschleusen und auszuführen. Durch den Remote Code Execution-Angriff können Angreifer Ausführungsberechtigungen der Anwendung übernehmen und erweiterte Privilegien erlangen.

Angreifer

Hacker oder böswilliger Zulieferer.

Mögliche Abwehrstrategien

Updates und Sicherheitspatches für die Anwendung implementieren, um bekannte Schwachstellen zu beheben und potenzielle Angriffsvektoren zu minimieren. Ebenso wie sichere Eingabevalidierung und sicheres Datenbankmanagement. Implementierung strenger Zugriffskontrollen und Berechtigungsmechanismen, stellen sicher, dass nur autorisierte Benutzer auf sensible Funktionen und Ressourcen zugreifen können. Dies kann dazu beitragen, dass selbst bei einem erfolgreichen Angriff die Privilegien des Angreifers begrenzt sind.

Denial Of Service

23. Data Store Inaccessible [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: An external agent prevents access to a data store on the other side of the trust boundary.
Justification: <no mitigation provided>

Art des Angriffs

Die Angreifer schaffen es die Datenhaltung anzugreifen, so dass das die Anwendung nicht mehr auf gespeicherte Daten zugreifen kann, z.B. über Ransomware.

Angreifer

Hacker, Naturkatastrophen, Sabotage.

Mögliche Abwehrstrategien

Etablieren von Backups und Prozeduren, diese wieder einzuspielen. Diese sollten regelmäßig getestet und auch durchgeführt werden. Außerdem kann der Dienst über mehrere physikalische Lokationen verteilt werden, um sich z.B. vor Naturkatastrophen zu schützen.