Critical Thread 1: Denial of Service (E.g.)

Bsp. Angriff auf Server, der die Kommunikation zwischen Brauerei und Restaurants managed.

Denial of Service (DoS): Wenn Prozess oder ein Datenbankserver nicht in der Lage ist, eingehende Anfragen zu bedienen oder gemäß den Spezifikationen zu agieren. Dies kann auf verschiedene weißen geschehen, beispielsweise durch eine übermäßige Anzahl von Anfragen, die die verfügbaren Ressourcen überlasten, oder durch gezielte Angriffe, die darauf abzielen, die Verfügbarkeit der Dienste zu beeinträchtigen.

Grobkonzept der implementierenden Gegenmaßnahmen

1. Lastenausgleich (Load Balancing)
2. Konfiguration des Firewalls und Intrusion Prevention Systems (IPS) und Anfragen Begrenzen
3. Ressourcenüberwachung und -optimierung (Systemressourcenüberwachung und Skalierungsoptimierung)
4. Sicherheitsvorkehrungen (Penetrationstests, Wiederherstellung des Betriebs beim Angriff)

Critical Thread 2: Information Disclosure

Bsp. WebApi/Datenbank Kommunikation nach draußen (Login Daten, Restaurant daten usw.).

Wenn Informationen von einer unbefugten Partei gelesen werden können. Dies kann durch verschiedene Schwachstellen oder Angriffsvektoren verursacht werden, die es einem Angreifer ermöglichen, auf sensible Daten zuzugreifen.

Grobkonzept der implementierenden Gegenmaßnahmen

5. Verschlüsselung des Datenverkehrs
6. Nutzung sicherer Übertragungsprotokolle (z.B. HTTPS)
7. Regelmäßige Sicherheitsprüfungen
8. Zugriffskontrollen (Rollen etc.)
9. Protokollierung und Überwachung

Critical Thread 3 : Elevation of Privilege

Bsp. Rating-App und dessen Kommunikation mit Api 2.

"Elevation of Privilege" (Erhöhung von Privilegien), hierbei erlangt eine Person durch Ausnutzen eines Implementierungsfehlers eine erhöhte Fähigkeit oder Privilegierung. Es ermöglicht dem Angreifer, auf Funktionen, Daten oder Ressourcen zuzugreifen, für die er normalerweise keine Berechtigung hat. Die Schwachstelle kann in der Software, im Betriebssystem oder in anderen Teilen des Systems auftreten und wird von einem Angreifer genutzt, um sich unbefugten Zugriff und Kontrolle zu verschaffen.

Grobkonzept der implementierenden Gegenmaßnahmen

10. Regelmäßige Sicherheitsüberprüfungen und Implementierung von Sicherheitspraktiken (Codeüberprüfungen, Sicherheitsanalysen, Penetrationstests, Codierungsrichtlinien, Sicherheitsschulungen, etc.)
11. Principle of Least Privilege (Benutzer hat minimalsten Berechtigungen)
12. Überwachung und Protokollierung

Critical Thread 4: Spoofing

Bsp. Rating-App und dessen Kommunikation mit Api 2/Datenbank (bsp. Sql-Injection)

Bezieht sich auf den betrügerischen Versuch, die wahre Identität eines Prozesses oder einer Entität zu verschleiern, indem sie sich als etwas anderes ausgibt, als sie vorgibt zu sein. Dies kann verschiedene Formen annehmen, darunter die Substitution von Prozessen, Dateien, Websites oder Netzwerkadressen. Spoofing ist eine ernsthafte Bedrohung für die Integrität und Sicherheit von Systemen, da es Angreifern ermöglicht, sich unberechtigten Zugriff zu verschaffen, Daten zu stehlen oder bösartige Aktivitäten zu tarnen, indem sie sich als legitime Quellen ausgeben.

Grobkonzept der implementierenden Gegenmaßnahmen

13. Authentifizierung und Autorisierung
14. Einschränkung der Abfragen
15. Verschlüsselung es Datenverkehrs (z.b. IPsec)
16. Überwachung und Protokollierung
17. Implementierung von DNS-Sicherheitsmechanismen mit z.B. DNSSEC (DNS Security Extensions)
18. Multi-Faktor-Authentifizierung (MFA) einsetzen

Critical Thread 5: Repudiation

Api 2 Schnittstelle.

wenn ein Angreifer sich weigert, die Verantwortung für eine Aktion oder Transaktion zu übernehmen, die er durchgeführt hat. Dieser kann in der Kommunikation zwischen Systemen auftretten. Das Leugnen einer Handlung kann schwerwiegende Folgen haben, da es die Integrität von Daten und die Vertrauenswürdigkeit von Systemen gefährdet.

Grobkonzept der implementierenden Gegenmaßnahmen

19. Forensische Analyse
20. Regelmäßige Schulungen und Sensibilisierung
21. Nachweisbarkeitsüberprüfung
22. Digitale Signaturen und Authentifizierung
23. Protokollierung und Überwachung