IT-Sicherheit für mein System

Herausgeber: Mixed Mode GmbH
Lochhamer Schlag 17
82166 Gräfelfing

Autor: Michael Schnelle

Version: 1.0

1 Einleitung

Das folgende Dokument soll Sie bei der Entwicklung und Absicherung von IT-Systemen unterstützen. Hierfür bieten wir Ihnen eine Checkliste an Fragen, die für ein sicheres System meist relevant sind und eine Vorgehensweise zur Durchführung einer Bedrohungs- und Risikoanalyse.

2 Checkliste

Folgende Checkliste soll als Leitfaden bei der Entwicklung sicherer Systeme betrachtet werden.

- ☐ **Mitarbeiter werden im Hinblick auf IT-Sicherheit geschult**
  Entwickler können nur dann wirklich sichere Software entwickeln, wenn sie regelmäßig in den Grundbegriffen der IT-Sicherheit, sowie der sicheren Programmierung geschult werden.
- ☐ **Es existiert ein Prozess, der es erlaubt auf Sicherheitslücken im aktiven Betrieb zu reagieren**
- ☐ **Es existiert ein Prozess, der die IT-Sicherheit meiner Applikation (und im ganzen Unternehmen) kontinuierlich verbessern soll**
- ☐ **Die Architektur meiner Applikation ist dokumentiert**
  Eine Applikation kann nur sinnvoll auf Bedrohungen analysiert werden, wenn die Komponenten, mit allen internen und externen Schnittstellen ausführlich dokumentiert ist. Es bieten sich Sequenz- und Datenflussdiagramme zur übersichtlichen Darstellung an.
- ☐ **Die Use- und die Misuse Cases meiner Applikation sind dokumentiert**
  Eine Applikation kann nur dann sinnvoll abgesichert werden, wenn deren Kontext bekannt ist. Eine Online-Banking Software stellt andere Kriterien an die Absicherung als z.B. eine Suchmaschine.
- ☐ **Die Rechte und Rollen meines Systems sind dokumentiert**
  Benötigt meine Applikation verschiedene Benutzungsrechte so muss sie anders abgesichert werden, als eine Applikation mit nur einer Klasse von Benutzern.
- ☐ **Das System wurde auf ungesicherte physikalische Schnittstellen untersucht**
- ☐ **Es werden eine Bedrohungs- und Risikoanalyse durchgeführt**
  Zur Durchführung von Bedrohungs- und Risikoanalysen existieren verschiedenste Vorgehensweisen. Bei Systemen mit starkem Netzwerkverkehr und vielen Schnittstellen bietet sich zur Bedrohungsanalyse das STRIDE Vorgehen (siehe unten) an. Durch DREAD kann das Risiko der Bedrohungen eingeteilt um Priorisierung zu ermöglichen.
- ☐ **Wurden ergänzend Bedrohungslisten betrachtet**
  Top-X Listen, wie die OWASP IoT-Top 10 Liste bieten eine einfache und sinnvolle Ergänzung zur Bedrohungsanalyse.
- ☐ **Es werden Code-Reviews aus Sicherheitsaspekten und zur Qualitätskontrolle durchgeführt.**
  Code Reviews sichern die Qualität der Software und senken durch das Vier-Augen Prinzip auch die Wahrscheinlichkeit, dass sich ein Sicherheitsfehler "einschleicht".
- ☐ **Meine Applikation wird regelmäßig automatisiert getestet**
  Automatisierte Tests auf Unit-, System- und Integrationsebene sichern den Funktionsumfang der Applikation und sorgen so indirekt auch für Sicherheit.
- ☐ **Meine Applikation wird vor der Auslieferung einem finalen Sicherheitscheck und einem Penetration-Testing unterzogen**

3 Bedrohungsanalyse nach STRIDE[1]

Die Anwendung wird nach Netzwerkbedrohungen, Hostbedrohungen und Anwendungsbedrohungen in den STRIDE-Kategorien untersucht. Die gefundenen Bedrohungen werden dokumentiert. Dieses Vorgehen eignet sich insbesondere für Applikationen mit vielen Schnittstellen nach Außen und viel Netzwerkverkehr.

- **Spoofing Identity:**
  Hierbei täuscht ein Angreifer eine falsche Identität vor. Es kann entweder eine falsche Client-Identität oder eine falsche Server-Identität vorgetäuscht werden. Eine Gegenmaßnahme ist unter anderem eine nötige Authentifizierung.
- **Tampering with Data:**
  Ein Angreifer manipuliert Daten. Er kann entweder persistente Daten wie Passwort-Datenbanken oder Audit-Logs, oder aber Netzwerkpakete manipulieren. Gegenmaßnahmen sind das Verwenden von Signaturen, Hash-Codes oder der Einsatz von Verschlüsselungsmechanismen.
- **Repudiation:**
  Ein Angreifer führt eine Aktion durch und streitet sie im Nachhinein ab. Ein Angreifer kann beispielsweise behaupten, dass er eine Bestellung nicht getätigt, oder eine Datei nicht gelöscht hat. Gegenmaßnahmen sind unter anderem digitale Signaturen oder Audit Logs.
- **Information Disclosure:**
  Ein Angreifer sieht Daten, die er nicht sehen soll. Das können lokale Daten, Netzwerkdaten, Informationen über die Infrastruktur, Datenbanktabellen oder sogar Fehlermeldungen im System sein. Zu den Gegenmaßnahmen zählen Authentifizierung, Verschlüsselung und ein sensibler Umgang mit Informationen.
- **Denial of Service (DoS):**
  Ein Angreifer stört die Verfügbarkeit der Anwendung. Hierbei kann ein Angreifer beispielsweise Distributed Denial of Service (DDoS) Angriffe durchführen. Eine mögliche Gegenmaßnahme ist die Erhöhung der Verfügbarkeit durch redundante Instanzen.
- **Elevation of Privileges:**
  Ein Angreifer findet einen Weg seine Berechtigungen zu erhöhen. Beispielsweise durch den Versuch, Zugriff auf eine Administrator-Konsole zu erhalten. Angriffsmöglichkeiten sind hier Buffer-Overflow-Angriffe oder SQL-Injections bei Webanwendungen. Gegenmaßnahmen sind z.B. sichere Programmierung, die ständige Anwendung des Least-Privilege-Prinzips und Eingabevalidierung

[1] Vorgehen entnommen aus dem Microsoft SDL (https://www.microsoft.com/en-us/sdl/)

4 Risikoanalyse nach DREAD[2]

Im Software Development Lifecycle von Microsoft wurde - neben der STRIDE-Methode zur Erfassung von Bedrohungen - auch die DREAD-Methode zur Durchführung einer Risikoanalyse eingeführt. DREAD steht für **D**amage, **R**eproducibility, **E**xploitability, **A**ffected und **D**iscoverability.

- **Damage (Schadenspotenzial):** Wie groß ist der Schaden, falls die Sicherheitslücke ausgenutzt wird?
- **Reproducibility (Reproduzierbarkeit):** Wie leicht kann der Angriff reproduziert werden?
- **Exploitability (Ausnutzbarkeit):** Wie leicht kann ein Angriff gestartet werden?
- **Affected (Betroffene):** Wie viele Benutzer können ungefähr betroffen sein?
- **Discoverability (Auffindbarkeit):** Wie leicht kann die Sicherheitslücke aufgefunden werden?

Die Bedrohungen werden nach den DREAD-Kriterien in einem festgelegten Bewertungssystem (z.B. 1 – 3) bewertet. Die resultierenden Werte werden anschließend addiert und ergeben die Gesamtbewertung. Auf Basis des Ergebnisses werden die Bedrohungen priorisiert und Gegenmaßnahmen erarbeitet.

5 Schlussbemerkung

Diese Guidelines sollen die Entwicklung sicherer Systeme vereinfachen. Jedoch ist die IT-Sicherheit ein sehr komplexes und umfangreiches Thema. Existieren gehobene Sicherheitsansprüche für eine Applikation wird eine zusätzliche Beratung von IT-Sicherheitsexperten empfohlen.

6 Information

MicroConsult führt in Kooperation mit Mixed Mode das Training "**Internet of Things (IoT): Technologien und Entscheidungsgrundlagen für das Internet der Dinge**" durch. Es beleuchtet praxisnah zahlreiche Aspekte der Produktentwicklung für das IoT.

[2] Vorgehen entnommen aus dem Microsoft SDL (https://www.microsoft.com/en-us/sdl/)