softScheck
we identify vulnerabilities others don't

Use Case: Medizinprodukte

Aufgabenstellung: Im Auftrag eines Herstellers für Medizinprodukte für den amerikanischen Markt, haben wir ein Threat Modeling und ein Penetration Test durchgeführt. Dies wird von der U.S Food and Drug Administration (FDA) gefordert, bevor ein Produkt auf den amerikanischen Markt verkauft werden darf.

Threat Modeling (Bedrohungsanalyse)
unterstützt die methodische Entwicklung eines sicheren Systementwurfs und einer Architektur in der Designphase der Softwareentwicklung (Security Design).

1. Die Identifizierung der Bedrohungen auf das System begann mit der Analyse der verfügbaren Dokumentation – insbesondere des Sicherheitsdesigns – sowie einer Untersuchung der Programmablaufpläne. Aus der Analyse wurden (Eingabe-)Schnittstellen, Kommunikationskanäle, zu schützende Ressourcen, Vertrauensgrenzen sowie externe Entitäten (potenzielle Angreifer, Administratoren, normale Benutzer, andere Systeme, …), die auf das System zugreifen können, systematisch ermittelt.
2. Mit diesen Informationen wurden die Datenflüsse des zu untersuchenden Systems mit mehreren Datenflussdiagrammen (DFDs) von sehr grob bis zu sehr fein visualisiert. Damit können alle sicherheitsrelevanten Datenflüsse bis hin zu einer schützenswerten Ressource im untersuchten System grafisch nachvollzogen werden.

   Durch eine systematische und vollständige Analyse der DFDs wurden mögliche Threats (Bedrohungen) vollständig identifiziert.
3. Die identifizierten Threats wurden mit der verfügbaren Dokumentation abgeglichen und soweit möglich mitigiert. So wurde z. B. in einer Dokumentation vermerkt, dass Passwörter in einer verschlüsselten Datenbank gespeichert werden. Somit wäre der Threat des Passwortdiebstahls mitigiert.

   Allerdings könnte ein fehlerhaft implementierter Verschlüsselungsalgorithmus geknackt werden oder der benutzte Schlüssel z.B. durch Ausprobieren erraten werden. So entstand Schritt für Schritt ein Attack Path aus nicht-mitigierten Threats.

   Während des gesamten Threat Modeling Process haben wir sehr eng mit dem Kunden zusammen gearbeitet, um mögliche Unklarheiten in der Dokumentation sofort zu klären.

Penetration Testing: Das Vorgehen sieht wie folgt aus:

1. **Information Gathering:** Im Rahmen eines Penetrationstests ist dies ein wichtiger und sehr kritischer Prozess. Es werden so viele sicherheitsrelevante Informationen wie möglich über das Zielsystem gesammelt. Neben Dokumentationen werden Tool-gestütze Informationen über das Zielsystem eruiert.
4. **Testing:** Das System wird sowohl mit dem Einsatz verschiedener Tools wie auch manuell auf Sicherheitslücken überprüft. Schwerpunkte hierbei sind folgende Kategorien:
   - Configuration and Deployment Management Testing
   - Authorization Testing
   - Session Management Testing
   - Input Validation Testing
   - Testing for weak Cryptography
   - Client Side Testing
   - Error Handling

   Wir identifizieren mit Tools nur ca. 25 % aller von uns identifizierten Sicherheitslücken. 75 % aller von uns identifizierten Sicherheitslücken werden also nicht von Tools erkannt, sondern müssen durch ‚händische' Analyse identifiziert werden.

5. **Risikobewertung:** Für jede identifizierte Sicherheitslücke wird eine Bewertung und Priorisierung vorgenommen: Eine Priorisierung unterstützt die Entscheidung, welche Sicherheitslücken zuerst gepatcht werden müssen, welche nachrangig gepatcht werden können und bei welchen auf ein Patching verzichtet werden könnte. Aus Wirtschaftlichkeitsgründen beheben Hersteller meist nicht alle Sicherheitslücken. Die Bewertung der Sicherheitslücken erfolgt anhand einer Risikobewertung. Die identifizierten Sicherheitslücken werden hinsichtlich ihrer Kritikalität (High, Medium, Low) bewertet – auf Wunsch auch mit CVSS v3.

Aufwand: Mittel bis Hoch. Je nach Umfang und Qualität der Dokumentation und Dauer des Penetrationstests.

Fazit: Nach Abschluss der Tests wurde das Produkt erfolgreich in den amerikanischen Markt aufgenommen.