**A9 Using Components with Known Vulnerabilities**

* **Leicht Verwundbar, wenn**
  + Man die Schwachstellen der genutzten Komponenten nicht kennt (direkten oder indirekten)
  + Die Software die benutzt wird nicht auf dem aktuellen Stand ist
* **Beispiel Attacken**
  + Fehler im Programmcode können großen Schaden verursachen 🡪 Fehler können ausversehen oder absichtlich (Hintertür in Komponenten) sein
  + Beispiel für verwundbare Komponenten sind:
    - CVE-2017-5638 Sicherheitsanfälligkeit für die Remotecodeausführung , die ermöglicht beliebigen Code auf dem Server auszuführen
    - Internet of Things(IoT) unterschiedlich dazu: fast unmöglich zu patchen
  + Es gibt automatisierte Tools, die Angreifern helfen unpatched oder falschkonfigurierte Systeme ausfindig zu machen
* **Wie verhindert man Attacke auf verwundbare Stellen der/des Software/Betriebssystems**
  + Lösche ungenutzte Abhängigkeiten, unnötige Funktionen, Komponenten, Dateien und Dokumentationen
  + Prüfen der Versionen der serverseitigen und benutzerseitigen Komponenten und deren abhängigen Tools
  + Benutze nur Komponenten von offiziellen Quellen und wenn möglich, signierte Pakete um die Chance zu reduzieren modifizierte, böswillige Komponenten zu bekommen

**A10 Insufficient Logging & Monitoring**

Unzureichende Protokollierung, Erkennung, Überwachung und aktive Reaktion

tritt jederzeit auf:

* Überprüfbare Ereignisse, wie Einloggen, fehlgeschlagene Einlogversuche und Werte Transaktionen werden nicht gespeichert.
* Protokolle von Anwendungen und APIs werden nicht auf Fehler überprüft
* Alarmschwellen und Antworteskalationen wie das Risiko die Daten bei der Anwendung zu halten ist nicht effektiv

Beispiel Attacken:

* Eine Open-Source Projekt Forum Software, laufend bei einem kleinen Team, wird gehackt durch einen Fehler in seiner Software. Die Angreifer haben es geschafft den Foruminhalt und das Quellcode-Repository zu löschen. Es konnte wiederhergestellt werden, aber der Mangel an Überwachung, Protokollierung oder Alarmierung führte zu einer weitaus schlimmeren Verletzung. Das Software Forum Projekt ist dadurch nicht mehr aktiv
* Ein Angreifer benutzt für jeden bekannten Benutzer ein übliches Passwort. Er kann damit herausfinden, welcher Benutzer dieses Passwort benutzt. Bei allen anderen bleibt nur ein falscher Loginversuch. Nach ein paar Tagen wird es mit einem anderen Passwort wiederholt

Wie es verhindert werden kann:

* Gemäß dem Risiko der Datenspeicherung von der Anwendung:
  + Alle Anmeldeversuche, Eingabefehler oder ähnliches sollten mit ausführlichen Benutzerdaten gespeichert werden und protokolliert werden, um ausführliche Analysen darüber zu erstellen
  + Transaktionen mit hohen Wert sollten einen Prüfpfad mit Integritätskontrollen aufweisen, um Manipulation oder Löschvorgänge zu verhindern
  + Wirksame Überwachung und Alarmierung sollten eingerichtet werden, damit verdächtige Aktivitäten innerhalb eine Zeitraumes erkannt werden