**A6 Sicherheits-Fehlkonfiguration**

* **Leicht Verwundbar, wenn**
  + Standardeinstellungen bei Erstellung von Servern oder ähnlichem genutzt werden und somit leicht herauszufinden sind
  + Die Software die benutzt wird nicht auf dem aktuellen Stand ist, da Lücken im Programm gefunden worden sind und durch ein Update geschlossen werden sollten
  + Man zu bequem ist, Einstellungen zu überprüfen oder einzurichten
  + Relevante Informationen bei Warnmeldungen oder als Infomeldungen auftauchen
* **Beispiel Attacken**
  + Fehler im Programmcode können großen Schaden verursachen 🡪 Fehler können ausversehen oder absichtlich (Hintertür in Komponenten) sein
  + Daten auslesen, welche in Fehler-, Warn,- oder Infomeldungen eingetragen sind
  + Einloggen mit Standardpasswörtern bei Server Konten
  + Einen Port welcher als Standard offen gelassen wird um Zugriff für bestimmte Funktionen zu gewähren wird genutzt um Zugriff zu erhalten
* **Wie verhindert man Attacke auf verwundbare Stellen der/des Software/Betriebssystems**
  + Regelmäßige Überprüfungen der Software, ist Sie aktuell? Nein, also Updaten. Ist sie relevant? Nein, also entfernen.
  + Standardeinstellungen bei Benutzerkonten und Passwörtern vermeiden
  + Benötigt diese Software Zugriffsrechte für das gesamte System oder können diese eingeschränkt werden? Wenn nein, Verwendung von getrennter bzw. segmentierter Anwendungsarchitekur um Zugriffsmöglichkeiten einzuschränken
  + Ein aufwendiger,doch relativ sicherer Schutz ist es, eine konstante Überwachung des Systems bzw. der Konfigurationen vorzunehmen und somit nicht gewünschtes Verhalten erkennen und isolieren zu können.
* **Ziele eines Angreifers (Umgebung und Nutzen)**
  + Der Angreifer möchte Zugriff auf das Opfersystem erhalten. Daten stehlen oder manipulieren und somit Schaden anrichten bzw. einen Nutzen zu ziehen.
  + Die Umgebung welche angegriffen wird, sind Schwachstellen bei Programmen, Einstellungen welche Lücken hervorrufen und der Nutzer selbst, welcher aufgrund von Unwissenheit oder Unbedachtheit Einstellungen vorgenommen hat, welche der Systemsicherheit Schaden
* **Gefährdete Personengruppen**
  + Jeder Nutzer der ein System mit Internetzugang besitzt
  + Nutzer die keine Softwareupdates ausführen
  + Nutzer die sich auf Standardeinstellungen verlassen bzw. Standardpasswörter bei Konten verwenden