TÜV NORD GROUP

	Spot Check Level 1	Regular Pentest Level 2	Advanced Pentest Level 3
	Erste Einschätzung	**Für die meisten Anwendungen**	**Hohes Sicherheitsniveau**
	Erste Einschätzung des Sicherheitsniveaus im Rahmen einer Stichprobe.	Tiefergehende Untersuchung zur Ermittlung der häufigsten auftretenden Risiken bzw. Schwachstellen für Webanwendungen.	Erweiterte, tiefergehende Untersuchung mit mehr Testfällen, bspw. für Anwendungen die geschäftskritische Vorgänge & sensible Daten verarbeiten.
Allgemein			
Angreifer-Niveau	Simulation eines Angreifers, der **einfache Techniken** verwendet, um leicht zu findende/ ausnutzbare Schwachstellen (**Low-Hanging-Fruits**) zu ermitteln.	Simulation eines **entschlossenen Angreifers**, der **aktuelle Angriffstechniken** aus der Hackerszene anwendet.	Simulation eines **entschlossenen & geschickten Angreifers**, der **aktuelle Angriffstechniken** aus der Hackerszene anwendet & die **Webanwendung gezielt ins Visier** nimmt.
Testfälle	**Stichprobenartige Untersuchung**	Testfälle, welche die **OWASP Top 10** Schwachstellen berücksichtigen & somit die am häufigsten ausgenutzten Sicherheitsrisiken für Webanwendungen enthalten.	Testfälle, welche die **OWASP Top 10** Schwachstellen berücksichtigen (siehe Regular Pentest) **+** zusätzliche, ausgewählte Testfälle/Anforderungen aus dem **OWASP Application Security Verification Standard** (ASVS)
Testmethode			
	Stichprobenartige automatisierte Tests + **manuelle Penetrationstests**	**Automatisierte Tests** + **manuelle Penetrationstests,** die durch automatisierte Tools meist nicht gefunden werden.	**Automatisierte Tests** + **tiefergehende manuelle Penetrationstests**, die durch automatisierte Tools meist nicht gefunden werden.
Testinhalt & Bericht			
Portscans (Webserver)	**Basis** Portscan (Top 100 TCP)	**Erweiterter** Portscan (Top 1000 TCP/ Top 10 UDP)	**Kompletter** Portscan (alle 65535 TCP/ Top 10 UDP)

Schwachstellenscan (Webserver)		**Basis** Schwachstellenscan	**Vollständiger** Schwachstellenscan
SSL/TLS Überprüfung/Scans (Webserver)	✓	✓	✓
Bereitstellung technischer Anhänge, z.B. der Roh-Ergebnisse der Port- & Schwachstellenscans			✓
Optional: Übersicht aller Testfälle (auch positive)			✓

Sonstiges, Preise und Testzeiträume

Re-Test der Findings nach Behebung	**Nicht inklusive**	**Bis zu 5*** (innerhalb von 3 Monaten)	**Unbegrenzt*** (innerhalb von 3 Monaten)
Testzeitfenster	≤ 3 Tage	≥ 5 Tage	≥ 10 Tage
Preis	ab 3.900 €	ab 7.900 €	ab 14.900 €

* Nur als kritisch oder hoch eingestufte Schwachstellen