CHECKLISTE 12 PRÜFPUNKTE 9 MIN. GEPRÜFT 11.8.2026

Penetrationstest sinnvoll vorbereiten

Prüfziel, Systeme, Zugänge, Testregeln und Ergebnisweg vor einem Penetrationstest belastbar festlegen.

FÜR WEN

IT-Verantwortliche, Produktteams, Geschäftsführung und Informationssicherheit vor einem externen Sicherheitstest.

WANN NUTZEN

Vor Angebot und Beauftragung sowie erneut unmittelbar vor Beginn der aktiven Prüfung.

DIE KURZE ANTWORT

Ein Penetrationstest ist gut vorbereitet, wenn Prüfziel, Systemgrenzen, Rollen, erlaubte Methoden, Testzugänge, Notfallkontakte, Berichtsempfänger und Nachtest vor dem ersten aktiven Test eindeutig vereinbart sind.

Wichtige Grenze: Aktive Sicherheitsprüfungen können Systeme und Daten beeinflussen. Umfang, Freigabe und Abbruchweg müssen schriftlich vereinbart sein.

01 Ziel und Prüfbereich

Ein Test braucht eine konkrete Sicherheitsfrage und klar benannte Grenzen.

- [ ] **Prüfziel in einem Satz festlegen**

  Beschreibe, welche Risiken, Rollen oder Geschäftsabläufe bewertet werden sollen.

- [ ] **Systeme und Schnittstellen inventarisieren**

  Nenne Domains, APIs, mobile Anwendungen, Netze, Identitäten und externe Abhängigkeiten.

- [ ] **Ausnahmen sichtbar dokumentieren**

  Nicht prüfbare Systeme und Methoden erhalten eine fachliche Begründung und Risikobewertung.

- [ ] **Testmodell entscheiden**

  Black Box, Grey Box oder White Box werden passend zu Ziel, Zeit und verfügbarer Einsicht gewählt.

02 Sicherer Testbetrieb

Kontakte, Zeitfenster und Regeln schützen Betrieb, Beweislage und Testqualität.

- [ ] **Verantwortliche und Notfallkontakte benennen**

  Technik, Fachbereich und Testteam müssen während der Prüfung erreichbar sein.

- [ ] **Erlaubte Methoden und Grenzen vereinbaren**

  Lasttests, Social Engineering, Datenzugriff und produktive Änderungen werden ausdrücklich geregelt.

- [ ] **Testkonten und Daten vorbereiten**

  Rollen, Mehrfaktorzugang und datensparsame Testdaten werden vorab geprüft.

- [ ] **Abbruchkriterien definieren**

  Störung, Datenrisiko oder unerwartete Auswirkung brauchen einen sofort nutzbaren Entscheidungsweg.

03 Ergebnis und Behebung

Der Wert entsteht erst, wenn Funde verstanden, priorisiert und nachweisbar geschlossen werden.

- [ ] **Berichtsempfänger festlegen**

  Technische Teams und Leitung benötigen unterschiedliche Detailtiefe, aber dieselbe nachvollziehbare Risikobasis.

- [ ] **Kritische Meldung während des Tests regeln**

  Akut ausnutzbare Funde werden nicht bis zum Abschlussbericht zurückgehalten.

- [ ] **Maßnahmenprozess vorbereiten**

  Jeder relevante Fund erhält Verantwortung, Priorität, Termin und fachliche Rückfrage.

- [ ] **Nachtest vereinbaren**

  Umfang, Frist und erwarteter Nachweis der Behebung gehören in die ursprüngliche Beauftragung.

Ergebnis der gemeinsamen Prüfung

- Ein schriftlich abgegrenzter Prüfauftrag
- Ein sicherer Test- und Eskalationsweg
- Verwertbare Berichte für Technik und Leitung
- Ein vereinbarter Behebungs- und Nachtestprozess

Passende Vertiefung

- Penetrationstest im Detail →
- Cybersecurity →
- Web- und API-Penetrationstest →

Quellen und fachliche Grundlage

Die Arbeitshilfe übersetzt übergeordnete Empfehlungen in eine kompakte Erstprüfung. Maßgeblich bleiben die Primärquellen und der konkrete Kontext.

- BSI: Praxis-Leitfaden für IS-Penetrationstests →
- OWASP: Web Security Testing Guide →

Häufige Fragen

Reicht ein automatischer Schwachstellenscan?

Sollte direkt in Produktion getestet werden?

Browser-Häkchen werden nicht gespeichert und nicht an SudoPort übertragen.