turingpoint.

LEITFADEN

Den richtigen Pentest-Anbieter finden

20. August 2026 - Version 2.0

Erstellt von:
turingpoint GmbH

turingpoint GmbH
Neuer Wall 80
20354 Hamburg
Deutschland

Tel.: +49 40 52477883
Mail: hello@turingpoint.de
Web: turingpoint.de

Handelsregister: 157676
USt-IdNr: DE325011218

turingpoint.

Inhaltsverzeichnis

Einleitung

Die Suche nach dem richtigen Anbieter für Penetrationstests kann ein schwieriger Prozess sein, besonders für alle, die mit IT-Sicherheit nicht täglich zu tun haben. Was brauche ich überhaupt? Woran erkenne ich echte technische Expertise? Wie entlarve ich unqualifizierte Anbieter? Und wie sieht eine belastbare Dokumentation aus, die auch vor Aufsichtsbehörden und Wirtschaftsprüfern besteht?

In diesem Leitfaden stellen wir Ihnen **sieben Fragen**, die Sie jedem potenziellen Dienstleister für Ihren nächsten Pentest stellen sollten. Danach wissen Sie, worauf es bei der Auswahl ankommt, wie Sie Angebote vergleichen und die beste Wahl für Ihre Anforderungen treffen, ganz ohne eigene Security-Abteilung.

Zu jeder Frage zeigen wir zusätzlich transparent, **wie turingpoint sie beantwortet**. So können Sie unsere Qualifikation direkt als Maßstab für Ihren Vergleich nutzen.

> **Kurzprofil turingpoint**
>
> **BSI-zertifizierter** IT-Sicherheitsdienstleister. Zertifiziertes **ISMS nach ISO 27001**. Über **200 durchgeführte Projekte**. Eigene Schwachstellen-Forschung mit **über 50 veröffentlichten CVE-Advisories**. Erfahrung als **Red Teamer** (DORA, TIBER-EU, NIS-2).

Worauf es grundsätzlich ankommt: Reputation

Der Ruf eines Anbieters als hochwertig und vertrauenswürdig ist einer der wichtigsten Aspekte. Informieren Sie sich vor dem ersten Gespräch über Hintergrund und Fachkenntnisse: Was finden Sie, wenn Sie den Anbieter recherchieren? Gibt es tiefgehende Fachbeiträge, eigene Forschung oder Blogartikel, die zu Ihren technischen Anforderungen passen? Ein starker fachlicher Fußabdruck ist ein verlässliches Signal für echte Kompetenz und lässt sich nur schwer vortäuschen.

01

Wie stark ist der Pentest automatisiert?

TECHNISCHE EXPERTISE

Warum ist das wichtig? Automatisierte Werkzeuge und Scanner sind der Anfang jedes Pentests, übersehen aber regelmäßig die größeren, geschäftskritischen Risiken. Der Anteil manueller Tests ist deshalb ein einfacher Indikator für die Qualität eines Anbieters.

Ein hochwertiger Pentest ist überwiegend ein manueller, tiefgehender Prozess. Rund **90 % der Arbeit sollten manuell** erfolgen. Wenn ein Anbieter angibt, der Test sei größtenteils automatisiert, oder kaum Fragen zu Ihrer Umgebung stellt, ist Vorsicht geboten: Solche Assessments vermitteln ein falsches Sicherheitsgefühl und bringen zusätzliche Risiken mit sich.

Die Erfahrung des Pentesters hat größeren Einfluss auf das Ergebnis als die eingesetzten Werkzeuge. Scanner tragen nur wenig zu einem gründlichen Test bei.

So arbeitet turingpoint

Unsere Pentests sind manuell, strukturiert und angriffsorientiert, durchgeführt von erfahrenen Analystinnen und Analysten, die auch als **Red Teamer** reale Angreifer simulieren. Automatisierte Scans nutzen wir gezielt zur Abdeckung der Breite, die Tiefe entsteht durch manuelle Analyse.

02

Nach welchen Standards und Methoden wird getestet?

EFFEKTIVER PROZESS

Warum ist das wichtig? Jeder Pentest braucht eine klar definierte Methodik und einen strukturierten Prozess. Das etabliert einen nachvollziehbaren Ablauf, minimiert Missverständnisse und maximiert Sicherheitsnutzen und Aussagekraft der Ergebnisse.

Zu den etablierten Standards und Methoden zählen:

- **OWASP Testing Guide / OWASP Top 10** für Web-, API- und Mobile-Anwendungen (Branchenstandard)
- **OSSTMM, NIST SP 800-115, PTES, ISSAF** für Infrastruktur-Pentests
- **BSI-Leitfaden für Penetrationstests**, notwendig zur Einhaltung der Grundschutz-Normen
- **PCI DSS** als Mindeststandard für die Sicherheit von Zahlungssystemen
- **MITRE ATT&CK** als Rahmenwerk für realistische Angriffssimulationen und Red Teaming

Stellen Sie sicher, dass der Anbieter eine klar dokumentierte Methodik nach Industriestandard einsetzt und dass jeder Test mit einer sauberen Aufklärungs- bzw. Informationsbeschaffungs-Phase beginnt. Das ist ein oft vernachlässigtes, aber entscheidendes Detail.

So arbeitet turingpoint

Wir testen entlang **aller etablierten Methoden** (OWASP, OSSTMM, NIST, PTES, ISSAF, BSI-Leitfaden, PCI DSS und MITRE ATT&CK) und decken das gesamte Spektrum ab: Web- und API-Pentests, Mobile Apps, interne und externe Infrastruktur sowie Cloud-Umgebungen in **AWS, Azure und Google Cloud**. Als **BSI-zertifizierter** Dienstleister sind unsere Tests grundschutz- und regulatorik-konform.

03

Wie sieht der Dokumentationsprozess aus?

DOKUMENTATION

Warum ist das wichtig? Der Bericht ist das eigentliche Ergebnis eines Pentests: An ihm verstehen Sie, wo Risiken und Schwächen liegen, und er geht oft an Personen, die nie mit dem Anbieter gesprochen haben. Eine klare, gründliche Dokumentation ist deshalb entscheidend und muss zugleich technische Experten wie das Management adressieren.

Fordern Sie von jedem Anbieter einen **Beispielbericht** an. Gute Dienstleister halten Muster für jede angebotene Pentest-Art bereit. Ein belastbarer Bericht enthält immer:

- **Management Summary:** nicht-technischer Überblick über das Engagement für die Leitungsebene
- **Schwachstellenübersicht:** priorisiert nach Kritikalität (z. B. CVSS)
- **Detaillierte Findings:** mit Proof-of-Concept, Nachweis und Reproduzierbarkeit
- **Konkrete Maßnahmenempfehlungen:** umsetzbar für Ihre Teams
- **Nachvollziehbare Bewertung:** Methodik, Scope und Testtiefe transparent dargelegt

So arbeitet turingpoint

Unsere Berichte verbinden eine verständliche Management Summary mit technisch belastbaren Findings inklusive Proof-of-Concept und priorisierter Maßnahmenempfehlung. Auf Wunsch stellen wir Ihnen vorab einen **kostenlosen Beispielbericht** zur Verfügung.

04

Werden kostenlose Nachtests durchgeführt?

UMFANG & WIRKUNG

Warum ist das wichtig? Ein Pentest soll Sicherheit nicht nur bewerten, sondern verbessern. Ob Ihre Gegenmaßnahmen den gewünschten Effekt haben, zeigt sich erst in einer anschließenden Validierung. Beim Nachtest werden alle identifizierten Schwachstellen erneut geprüft und das Ergebnis in einen aktualisierten Abschlussbericht eingearbeitet. Diesen Nachweis können Sie auch externen Beteiligten vorlegen.

Ein Nachtest ist ein wichtiger Bestandteil eines Pentests. Ein guter Dienstleister stellt ihn Ihnen **nicht zusätzlich in Rechnung**. Wer identifizierte Schwachstellen sauber mit Proof-of-Concepts dokumentiert, hat beim Nachtest nur geringen Zusatzaufwand. Führende Anbieter bieten ihn deshalb kostenlos an.

> **So arbeitet turingpoint**
>
> Die Nachprüfung behobener Schwachstellen ist bei uns fester, **kostenloser** Bestandteil des Pentests. Sie erhalten einen aktualisierten Bericht, der die erfolgreiche Behebung belegt.

05

Gibt es Kompetenz im Bereich Security Engineering?

TECHNISCHE EXPERTISE

Warum ist das wichtig? Gefundene Schwachstellen müssen behoben werden. Security Engineering bildet die Brücke zwischen Softwareentwicklung und IT-Sicherheit: Erfahrene Security Engineers unterstützen Sie im schnelllebigen Entwicklungsalltag bei der Behebung und schon während der Entwicklung bei der sicheren Implementierung kritischer Programmteile.

Achten Sie darauf, dass Ihr Dienstleister Schwachstellen nicht nur **identifiziert**, sondern Sie auch bei der **Behebung** unterstützen kann. Fehlt Ihnen eine eigene Security-Abteilung, ist dieser Rückgriff auf erfahrene Berater besonders wertvoll.

So arbeitet turingpoint

Als Boutique-Beratung verbinden wir offensive Sicherheit (Pentest, Red Teaming) mit fundiertem Security Engineering und Security Architecture. Dass wir eigene **CVE-Advisories** veröffentlichen und Zero-Days erforschen, fließt direkt in belastbare, praxistaugliche Behebungsempfehlungen ein.

06

Werden kontinuierliche Sicherheitsprozesse angeboten?

NACHHALTIGKEIT

Warum ist das wichtig? In modernen Entwicklungsumgebungen (DevOps, CI/CD) sollten Sicherheitsprozesse nicht punktuell, sondern fest verankert sein. Ein Pentest ist eine Momentaufnahme und bei kurzlebigen Software-Artefakten schnell überholt. Automatisierte Sicherheit in der Pipeline ersetzt keinen vollwertigen Pentest, hält das Sicherheitsniveau aber dauerhaft hoch.

Fragen Sie deshalb auch bei manuellen Pentests nach Kompetenz im Bereich automatisierter und kontinuierlicher Sicherheit. So stellen Sie eine langfristige Zusammenarbeit sicher und prüfen, ob der Anbieter am Puls der Zeit ist und für künftige DevSecOps-Projekte taugt.

So arbeitet turingpoint

Wir integrieren Sicherheit über DevOps-Security und Security Architecture dauerhaft in Ihre Entwicklungs- und Betriebsprozesse, von der statischen Code-Analyse bis zur sicheren Cloud-Transformation. Als Betreiber eines **zertifizierten ISMS nach ISO 27001** wissen wir, wie sich Sicherheit prozessual und auditfest verankern lässt.

07

Wie wird mit KI-Systemen umgegangen?

ZUKUNFTSSICHERHEIT

Warum ist das wichtig? KI-Systeme wie große Sprachmodelle (LLMs), RAG-Anwendungen und autonome KI-Agenten schaffen völlig neue Angriffsflächen, die klassische Pentests nicht abdecken: Prompt Injection, Abfluss vertraulicher Daten über das Modell, unsichere Anbindung von Tools und Funktionen an KI-Agenten sowie manipulierte Trainings- und Wissensquellen. Wer KI in Produkte oder Prozesse integriert, braucht einen Anbieter, der diese Risiken versteht und gezielt prüft.

Achten Sie darauf, dass Ihr Dienstleister zweierlei kann: erstens **KI-Systeme absichern und testen**, orientiert an etablierten Referenzen wie den OWASP Top 10 für LLM-Anwendungen (Prompt Injection, RAG-Sicherheit, Absicherung von Agenten und deren Tool-Zugriffen). Zweitens sollte er **KI-gestützte Angriffs- und Analysemethoden** beherrschen und sinnvoll in Assessments einsetzen, ohne dabei die Tiefe manueller Arbeit zu ersetzen.

So arbeitet turingpoint

Mit unserem Bereich **AI in Cybersecurity** prüfen und härten wir KI-Systeme, von LLM-Anwendungen und RAG-Architekturen bis zu autonomen Agenten, entlang der OWASP Top 10 für LLMs. Zugleich setzen wir KI gezielt in unseren Assessments ein, um Breite und Effizienz zu erhöhen, während die sicherheitskritische Analyse in erfahrener Hand bleibt.

Warum turingpoint

Die sieben Fragen führen Sie sicher durch die Auswahl. Zusammengefasst erfüllt turingpoint sie so:

Unsere Qualifikationen auf einen Blick

- **BSI-zertifizierter IT-Sicherheitsdienstleister:** grundschutz- und regulatorik-konforme Penetrationstests
- **Zertifiziertes ISMS nach ISO 27001:** Sicherheit auditfest und prozessual verankert
- **Über 50 veröffentlichte CVE-Advisories:** eigene Schwachstellen-Forschung mit Root-Cause-Analysen und Proof-of-Concepts
- **Alle etablierten Testmethoden:** OWASP, OSSTMM, NIST, PTES, ISSAF, BSI-Leitfaden, PCI DSS, MITRE ATT&CK
- **Erfahrung als Red Teamer:** realistische Angriffssimulationen nach DORA (Art. 26/27), TIBER-EU und NIS-2 (Art. 21)
- **KI-Sicherheit:** Absicherung und Testing von LLM-Anwendungen, RAG und KI-Agenten (AI in Cybersecurity)
- **Über 200 durchgeführte Projekte:** für Kunden vom Startup bis zum Konzern
- **Kostenlose Nachtests:** als fester Bestandteil jedes Pentests

Eigene Forschung statt reiner Tool-Anwendung

Anders als reine Scanner-Anwender betreibt turingpoint **eigene Schwachstellen-Forschung**. Unser Team identifiziert, verifiziert und meldet Zero-Day-Schwachstellen in verbreiteter Software und veröffentlicht sie als Security Advisories mit **CVE-IDs**, Root-Cause-Analysen und Proof-of-Concepts. Diese offensive Tiefe fließt direkt in Ihre Pentests ein. Sie profitieren von Angreifer-Wissen aus erster Hand.

Vollständiges Testspektrum

Web- und API-Anwendungen, Mobile Apps, interne und externe Infrastruktur, Cloud-Umgebungen in AWS, Azure und Google Cloud sowie vollständige **Red-Team-Assessments** und die Absicherung von KI-Systemen, abgesichert durch Methodik nach Industriestandard und regulatorischer Konformität.

Über uns

turingpoint ist eine von Sicherheitsexperten gegründete Boutique-Beratung mit dem Schwerpunkt Cyber Security. Unsere erfahrenen Sicherheitsexpertinnen und -experten helfen Ihnen, Ihre Anwendungen und Systeme zu schützen und progressive Sicherheitskonzepte umzusetzen. Besonders in der IT-Sicherheit überzeugen wir durch neue Ideen, Kreativität und sorgfältige Arbeit, mit Standorten in Hamburg (Zentrale), Paderborn und Zürich.

Die Suche nach einem Anbieter für Penetrationstests kann herausfordernd sein. Die sieben Fragen in diesem Leitfaden führen Sie sicher durch den Prozess. Vertrauen, technische Expertise, die Qualität des Personals und die Tiefe der Berichterstattung gehören zu den wichtigsten Auswahlkriterien. Berücksichtigen Sie zusätzlich Preisstruktur, Referenzen und Branchenerfahrung und formulieren Sie eigene Fragen, bis Sie sich bei Ihrem Anbieter sicher fühlen.

Kontakt

E-Mail: hello@turingpoint.de **Telefon:** +49 (0)40 52477883 **Web:** turingpoint.de

Vereinbaren Sie ein unverbindliches Erstgespräch. Wir beraten Sie gern zu Ihrem nächsten Pentest.