FORUM

# Penetrationstests in Unternehmen

## Aktueller Stand, Trends und Ausblick

## Sehr geehrte Leser*innen,

wir freuen uns, dass Sie sich für dieses Whitepaper interessieren.

Nachfolgend erhalten Sie wertvolle Einblicke, Tipps und Handlungsempfehlungen für Ihren Job.

Informieren Sie sich über aktuelle, praxisnahe Trends und Impulse direkt von unseren Expert*innen. Zusätzlich können Sie mit unserem Angebot an verschiedenen Weiterbildungen Ihr Fachwissen ausbauen und vertiefen.

Wir wünschen Ihnen viele neue Erkenntnisse beim Lesen.

Dieses Whitepaper wurde mithilfe von KI im Modus „Deep Research“ erstellt.

# Penetrationstests in Unternehmen – Aktueller Stand, Trends und Ausblick

**Executive Summary:** In einer global vernetzten, cloud- und KI-getriebenen IT-Welt bleiben viele Angriffsflächen ungeprüft. Studien zeigen, dass etwa 95 % der Unternehmen Penetrationstests (Pentests) als höchste Priorität einstufen, im Durchschnitt jedoch nur 32 % ihrer Angriffsfläche regelmäßig testen. Dies lässt rund 68 % der IT-Umgebung ungetestet eine alarmierende Lücke im Risikomanagement. Gleichzeitig treibt die Regulierung (z. B. EU-NIS2-Richtlinie und deutsches BSIG §30) verbindliche Sicherheitsmaßnahmen voran, zu denen auch regelmäßige Pentests zählen. Technologisch setzen Unternehmen zunehmend auf automatisierte und KI-gestützte Prüfformen (sogenannte „agentic AI“ oder fortlaufendes Validierungstesting), um mit dynamischen Cloud-Umgebungen Schritt zu halten. Dieses Whitepaper analysiert aktuelle Markttrends, regulatorische Rahmenbedingungen und technologische Entwicklungen rund um Penetrationstests. Es liefert Handlungsempfehlungen, einen praxisnahen Umsetzungsfahrplan sowie Kennzahlen (KPIs) für erfolgreiche Pentest-Programme.

## 1. Einführung: Bedeutung und Ziele von Penetrationstests

Penetrationstests (Pentests) sind simulationsbasierte Sicherheitsprüfungen, bei denen speziell ausgebildete Fachleute (»White Hat Hacker«) versuchen, gezielt in Systeme, Netzwerke oder Anwendungen einzudringen. Das Ziel ist es, Schwachstellen aufzudecken, bevor Angreifer sie ausnutzen können. In einem verantwortungsbewussten Risikomanagement erfüllen Pentests mehrere Aufgaben: Sie überprüfen die Wirksamkeit existierender Schutzmechanismen, helfen bei der Priorisierung von Sicherheitslücken und unterstützen die Erfüllung von Compliance-Anforderungen. Zugleich sensibilisieren Pentests Organisationen für reale Bedrohungsszenarien.

Die Zielgruppe dieses Whitepapers sind IT-Sicherheitsverantwortliche (*IT-Sicherheitsmanager*innen*), IT-Leitung, Geschäftsführer*innen, Projekt- und Qualitätsmanager*innen sowie alle an Cybersecurity- und Compliance-Aufgaben Beteiligten. Es liefert Grundlagen und Tiefenwissen, um den Status Quo zu bewerten und einen zukunftsfähigen Pentest-Ansatz zu planen. Der Umfang des Whitepapers umfasst neben einem Überblick zum Markt und zur Technologie auch Empfehlungen zur Ausgestaltung von Pentest-Programmen, inklusive Zeit- und Budgetplanung sowie Erfolgsmessung.

## 2. Regulatorischer Rahmen und Standards

Deutschland hat die EU-NIS2-Richtlinie (EU 2022/2555) umgesetzt, u. a. durch das neue **NIS2-Umsetzungsgesetz** (NIS2UmsuCG, in Kraft seit 6. Dezember 2025). Wesentlich ist dabei §30 BSIG, der von betroffenen Unternehmen die Umsetzung von zehn Risikomanagement-Maßnahmen verlangt. Unter Maßnahme 6 (§30 BSIG) fällt explizit die „Bewertung der Wirksamkeit von Maßnahmen“, wozu auch Penetrationstests zählen. Das bedeutet: Unternehmen müssen nicht nur

Schutzmaßnahmen implementieren, sondern deren Wirksamkeit regelmäßig prüfen etwa durch Pentests oder Audits. Verstöße können Bußgelder bis zu 10 Mio. € oder 2 % des Jahresumsatzes nach sich ziehen. Auch andere Gesetze und Standards fordern solche Tests (z. B. ISO 27001 Annex A.18.2.3 „Technical Vulnerability Management“ sieht Untersuchungen wie Prüfungen oder Penetrationstests vor).

Bereits in den Erwägungsgründen der NIS2-Richtlinie wird betont, dass Organisationen aktiv Schwachstellen aufdecken sollen. So nennt NIS2 Penetrationstests ausdrücklich als Mittel, um veraltete Software und schwache Zugangsdaten zu entdecken. Branchenspezifisch wird in Finanz-, Gesundheits- und Kritischen Infrastrukturen (KRITIS) oft ebenfalls eine regelmäßige Sicherheitsprüfung vorausgesetzt (z. B. DORA-Verordnung für Finanzdienstleister). Behörden wie das deutsche BSI stellen Leitfäden und Mindeststandards zur Verfügung (z. B. den BSI-Leitfaden „IS-Penetrationstests“). Zusammengefasst zwingt der regulatorische Druck Unternehmen, Penetrationstests systematisch in ihr Sicherheitsmanagement zu integrieren.

**3. Aktueller Stand des Marktes und Trends**

Der globale Markt für Pentest-Dienstleistungen wächst kräftig. Laut aktuellen Marktanalysen liegt der Umsatz bei mehreren Milliarden US-Dollar und steigt weiter zweistellig. So prognostiziert MarketsandMarkets ein Wachstum von USD 1,98 Mrd. (2025) auf USD 4,39 Mrd. (2031) bei einem Jahreswachstum (CAGR) von etwa 14,2 %. North America nimmt dabei 2025 schon etwa 35,9 % des Weltmarkts ein, während Europa insbesondere durch die EU-Regulierung und Datenschutzvorgaben (GDPR, NIS2) stark nachzieht. Nach Regionen wird erwartet, dass der asiatisch-pazifische Raum mit über 22 % CAGR am schnellsten wächst, getragen von Digitalisierung in China, Indien, Japan etc. . Die Marktsegmente entwickeln sich wie folgt:

- **Nach Service-Typ:** Derzeit dominieren noch manuelle Pentests (75,4 % Marktanteil 2025). Diese *Human-driven* Tests (rote Teams) werden ergänzt durch automatisierte bzw. halb-automatisierte Services (Scans, „Agentic Pentesting“). Zunehmend gefragt sind hybride Ansätze: Manuelles Testen wichtiger Ziele kombiniert mit automatisierten Containern/Agenten, die kontinuierlich prüfen.
- **Nach Angriffssurface:** Der größte Marktanteil entfällt auf klassische Netzwerk- und Applikationspentests. Die Cloud-Sicherheit wächst jedoch am stärksten (höchste CAGR ~15,9 %). Konfigurationen in Multi-Cloud-Umgebungen sowie API-Security werden immer wichtiger (84 % der Security-Profis berichteten über API-Sicherheitsvorfälle).
- **Nach Branche:** Derzeit treiben Finanzwesen, Behörden und Industrie (KRITIS) den Markt. Besondere Wachstumsraten werden im Gesundheitswesen erwartet (hohe Datenwerte).
- **Wettbewerbsumfeld:** Große Konzerne wie IBM (SecOps), Fortra/Trustwave, Sophos und spezialisierte Anbieter (NetSPI, Cigital/ForAllSecure etc.) dominieren

die Marktanteile. Emerging-Plattformen wie Aikido Security, Pentera, NowSecure, ZeroThreat o. ä. setzen dagegen stark auf KI-Automation und DevSecOps-Integration. In Deutschland bieten neben internationalen Firmen auch lokale IT-Dienstleister und Beratungen (z. B. SySS, ERNW, TÜV, secorvo) Pentesting-Services an.

Im Verbraucherverhalten zeigt sich: Nur etwa ein Drittel der Unternehmen führt regelmäßig jährliche Pentests durch, viele beschränken sich auf Erst-Tests bei Projekteingang. Studien belegen, dass Wiederholungstests deutlich effizienter sind: Firmen mit kontinuierlichen Prüfzyklen finden bis zu 70 % weniger kritische Schwachstellen als Erstprüfungen. Dennoch scheitern 1 von 3 Unternehmen an Budget- und Ressourcenfragen: Eine typische Penetration kostet im Schnitt etwa 18.300 $ (komplexe Tests können >100.000 $ kosten). Laut einer Ponemon-Studie testet 20 % der Firmen ihre Software gar nie auf Sicherheitslücken, was die Risiken exponentiell erhöht.

**Technologische Entwicklungen: KI, Cloud und Automatisierung**

Die Angriffsflächen von Unternehmen haben sich durch Cloud-Migration, „Software-as-a-Service“ und IoT massiv vergrößert. Klassische statische Pentest-Zyklen (z. B. halbjährlich) können mit dieser Dynamik nicht mehr Schritt halten. Entsprechend entstehen neue Konzepte:

- **Agentenbasierte KI-Pentests:** Führende Anbieter (Synack, Pentera etc.) entwickeln KI-Agenten, die automatisiert Szenarien durchspielen. 87 % der Befragten aus einer Synack/Omdia-Studie setzen bereits (oder planen) solche KI-gestützten Pentests ein. 95 % erwarten, dass solche Agenten traditionelle Pentests zumindest teilweise ersetzen werden. Wichtig ist dabei das Zusammenspiel: Die Mehrheit (64 %) bevorzugt ein Modell, bei dem KI-Tests unter menschlicher Aufsicht laufen – „Machine Speed“ kombiniert mit „Human Judgment“.
- **Continuous Testing und Plattformen:** DevOps-Teams integrieren Security-Tests direkt in CI/CD-Pipelines. Plattformen wie Pentera, Cobalt, ImmuniWeb oder ZeroThreat automatisieren Prüfungen bei jedem Deployment. Dieses *Continuous Validation*-Prinzip ermöglicht eine permanent aktuelle Sicht auf die Sicherheitslage – analog zu automatisierten *Chaos-Tests* für Resilienz.
- **Fokus auf KI/GenAI:** Mit dem boomenden Einsatz großer Sprachmodelle (ChatGPT, GPT-4, LLMs) in Unternehmen sind neue Angriffsziele entstanden. Ein Leitfaden der Allianz für Cyber-Sicherheit (ACS) der deutschen Behörden (September 2025) widmet sich bereits Penetrationstests von LLMs (KI-Modellen). Auch berichten Pentest-Firmen, dass spezifische KI-Schwachstellen (z. B. Prompt-Injection, Poisoning) zunehmen, je mehr Generative AI genutzt wird.

Insgesamt wandelt sich das Pentest-Feld von punktuellen Prüfungen hin zu umfassenden, skalierbaren Prüfstrategien, die auch Cloud- und KI-Komponenten abdecken. Gleichzeitig wächst der Bedarf an Pentest-Experten, was Personalmangel erschwert. Dieser Trend wird jedoch teilweise durch Software-Unterstützung ausgeglichen: Laut Umfragen verwenden heute über die Hälfte der Unternehmen Software-Tools zur Unterstützung interner Pentest-Programme.

**Bedrohungen und Risikofaktoren**

Angreiferwerkzeuge entwickeln sich rasant weiter (KI-gesteuerte Exploits, automatisierte Botnets etc.). Aktuelle Zahlen verdeutlichen das Risiko: Bis März 2026 waren bereits über 11.000 CVEs (Security Bulletins) veröffentlicht, Tendenz stark steigend. Trotz hoher Relevanz bleibt die Sicherheitslage vielerorts katastrophal: Rund 73 % aller erfolgreichen Unternehmensangriffe beruhten 2025 auf verwundbaren Web-Applikationen. Auch Mensch und Prozesse sind Schwachstellen: Phishing/Social Engineering sind nach wie vor häufigste Einfallstore. Eine Kaspersky-Studie findet, dass 40 % der Unternehmen keine ausreichende Cybersicherheit aufgebaut haben.

Angesichts dieser Lage entstehen Chancen und Risiken zugleich. Regulatorische Anforderungen (NIS2, DORA, ISO 27001) stärken die Nachfrage nach Pentests – zugleich erhöhen sie den Druck, Mängel nachzuweisen und zu beheben. Cyberversicherungen verlangen oft Nachweise regelmäßiger Prüfungen (über 50 % der U.S.-Unternehmen gaben an, Pentests aufgrund von Versicherungsanforderungen durchgeführt zu haben). Andererseits macht Fachkräftemangel und Kosten die Umsetzung anspruchsvoll. Laut Marktanalysen werden gerade diese Herausforderungen (Fachkräftie, Testkosten) als wesentliche Restriktionen genannt.

**4. Handlungsfelder und Empfehlungen**

Um die Lücke zwischen Potenzial und Praxis zu schließen, empfiehlt sich folgender Mehrjährigen-Fahrplan:

1. **Ist-Analyse und Scope-Definition:** Ermitteln Sie zunächst den aktuellen Stand: Welche Systeme, Applikationen und Schnittstellen sind kritisch? Welche Pentests wurden zuletzt durchgeführt? Die Analyse sollte alle Assets erfassen (Netzwerke, Apps, Cloud-Umgebungen, IoT, etc.) und Verantwortlichkeiten klären. Fokussieren Sie auf diejenigen Komponenten, die hohe Risiken bergen (Geschäftskritisch, sensible Daten, regulatorisch relevant).
2. **Teststrategie entwickeln:** Legen Sie fest, welche Testarten eingesetzt werden: extern vs. intern, white-box vs. black-box, manuelle vs. automatisierte Tests. Moderne Ansätze kombinieren Methoden („mischbetriebener Pentest“): etwa automatisierte Schwachstellenscanner und Penetrationstools, begleitet von gezielten Red-Team-Übungen. Berücksichtigen Sie auch neuartige Konzepte wie *Container-basierte Pentests* oder Agenten-basierte Prüfsoftware (KI-

Pentester). Definieren Sie die Testfrequenz – z. B. jährliche Volltests plus halbjährliche Teil- oder Ad-hoc-Scans.

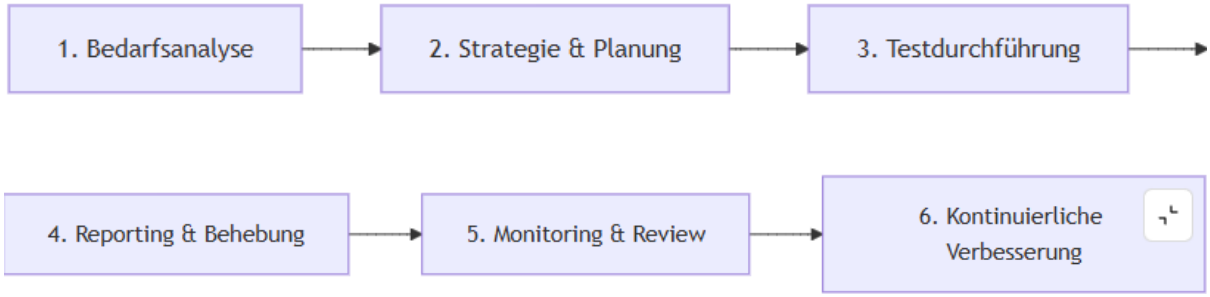
3. **Anbieterauswahl und Tools:** Entscheiden Sie, ob Pentests intern durchgeführt oder an spezialisierte Dienstleister (Pentest-Unternehmen, Certified Ethical Hackers) vergeben werden. Externe Pentester bringen unabhängige Expertise mit, sollten aber vertraglich strenge NDA-, Haftung- und Berichtspflichten erfüllen. Interne Teams (z. B. „Adversarial Teams“) eignen sich für regelmäßige Kontrollen, wenn sie entsprechend geschult sind. Unabhängig davon sollten moderne Pentest-Tools beschafft werden: z. B. professionelle Schwachstellenscanner, Plattformen für kontinuierliche Security-Validation, Penetrationstest-Frameworks (Metasploit, Kali, Burp Suite etc.) sowie KI-gestützte Analysewerkzeuge.
4. **Durchführung der Pentests:** Führen Sie Tests gemäß definiertem Scope durch. Dabei durchlaufen Pentests typischerweise die Phasen: Reconnaissance (Informationssammlung), Exploitation (Schwachstellen -Ausnutzung), Post-Exploitation (Ausweitung des Zugriffs), und Berichterstellung. Der Abschlussbericht sollte neben technischen Details klare Handlungsempfehlungen enthalten – organisatorisch, prozessual und technisch – und Prioritäten für die Behebung definieren. Wichtig ist die Dokumentation aller Schritte für Nachvollziehbarkeit und Compliance.
5. **Behebung & Monitoring:** Die festgestellten Schwachstellen sind zeitnah zu bewerten und zu beheben (Patch-Management, Konfigurationsänderungen, Policies). Verfolgen Sie die Remediation-Rate und stellen Sie sicher, dass kritische Befunde zügig geschlossen werden. Nach jedem Pentest sollte ein Review stattfinden: Haben sich neue Probleme ergeben? Brauchen Teile des Systems Nachtests? Parallel sollten Kennzahlen (KPIs) definiert und gemessen werden, z. B. Anzahl entdeckter kritischer Schwachstellen, durchschnittliche Behebungsdauer, Anteil der geprüften Infrastruktur.
6. **Kontinuierlicher Verbesserungsprozess:** Integrieren Sie die Erkenntnisse in Ihr Sicherheitsmanagement: Passen Sie Policies, Trainings und Budgets an. Evaluieren Sie neue Technologien laufend – etwa KI-Tools für Sicherheit, automatisierte Pentest-Dienste oder Simulationen (z. B. CBEST/TIBER-Übungen). Geben Sie Ihren Pentest-Prozess regelmäßig durch unabhängige Audits überprüfen, um Compliance-Anforderungen (z. B. ISO 27001, NIS2) zu erfüllen.

**Empfehlungen im Überblick:** Halten Sie einen regelmäßigen Testzyklus ein (mind. jährlich, bei schnell ändernder Infrastruktur häufiger). Priorisieren Sie die Prüfung *kritischer Ressourcen* und nutzen Sie realistische Angriffszenarien (mithilfe von Threat Intelligence). Kombinieren Sie manuelle und automatisierte Tests, um Effizienz und Tiefe zu steigern. Binden Sie die Geschäftsführung ein („Chefinnen und Chefsache“ Cybersicherheit) und adressieren Sie interne Stakeholder (z. B. *Sachbearbeiter*innen, IT-Administratoren, Entwicklerteams*) entsprechend.

Schulen Sie Mitarbeitende und schaffen Sie ein Bewusstsein für Sicherheitslücken, um die Gesamtresilienz zu erhöhen.

**5. Implementierungsschritte & Roadmap**

Die Einführung eines effektiven Pentest-Programms kann wie folgt als Meilenstein-Roadmap visualisiert werden:




- **1. Bedarfsanalyse:** Erfassen der aktuellen Infrastruktur und Sicherheitsziele, Risikobewertung (Vulnerabilitätsanalyse, Angriffssimulation).
- **2. Strategie & Planung:** Festlegung von Umfang (Scope) und Umfang (z. B. Netzwerk, Cloud, Applikation), Auswahl von Methoden (Black-/White-Box, Red Team) und Testfrequenz.
- **3. Testdurchführung:** Vorbereitung (Genehmigungen, Testaccounts), Pentest-Phase (Recon, Exploits), Koordination mit IT-Betrieb (um reale Umgebung zu schützen).
- **4. Reporting & Behebung:** Auswertung der Ergebnisse, Erstellen von Management- und Techniker-Berichten mit Schwachstellenliste und Maßnahmen. Priorisierung und Umsetzung von Gegenmaßnahmen.
- **5. Monitoring & Review:** Evaluierung der Umsetzungserfolge, Anpassung des Testumfangs für Folgezyklen, Lessons Learned.
- **6. Kontinuierliche Verbesserung:** Aktualisierung des Sicherheitskonzepts, Prozessoptimierung, evtl. Erweiterung auf neue Technologien (z. B. Pentesting von LLM-basierten Systemen).

**Tabelle: Vergleich Pentest vs. Schwachstellenscan**

| Aspekt | Penetrationstest | Schwachstellenscan |
|---|---|---|
| **Ziel** | Aktive Ausnutzung von Schwachstellen | Erkennung potenzieller Schwachstellen (ohne Exploits) |
| **Tiefe** | Sehr tief, inkl. Exploits und Post-Exploitation | Oberflächlich, automatisiert |
| **Zeitaufwand** | Hoch (Wochen), punktuell | Niedrig bis mittel (Stunden – Tage), laufend möglich |
| **Ergebnis** | Exploitable Lücken, Angreifbarkeit | Liste bekannter CVEs/Bulletins |
| **Anbieter/Rollen** | Pentesting-Spezialist*innen, Red Team | Security-Analyst*innen, Scanner |
| **Kosten** | Höher (externer Dienst oder spezialisierte Tools) | Geringer (Automatisierung, freie Tools) |
| **Bestandteile** | Kreativität, Ad-hoc-Exploits, Realitätsnähe | Regelmäßiger Check, Compliance-Bericht |
| **Zusatznutzen** | Gezielte Trainings für Security-Teams, Awareness | Breiter Überblick, Frühwarnung |

### 6. Kennzahlen (KPIs) zur Erfolgsmessung

Zur Beurteilung der Effektivität des Pentest-Programms sollten messbare Indikatoren festgelegt werden. Beispiele für mögliche **KPIs** sind:

- **Testabdeckung (%)**: Anteil der IT-Systeme, Applikationen und Netzwerke, die im Jahr getestet wurden.
- **Durchgeführte Tests/Jahr**: Anzahl der Pentest-Engagements oder –Scans pro Jahr (nach Typ gegliedert: intern/extern, Anwendung/Netzwerk).
- **Gefundene Schwachstellen**: Anzahl und Schwere der entdeckten Lücken pro Test (z. B. kritische, hoch, mittel, niedrig).
- **Behebungsquote**: Anteil der als kritisch eingestuften Schwachstellen, die innerhalb einer definierten Frist (z. B. 30 Tage) geschlossen wurden.
- **MTTR (Mean Time To Remediate)**: Durchschnittliche Zeitspanne von Fund bis Patch/Beseitigung.
- **Übrige Schwachstellen nach X Tagen**: Anzahl offener Schwachstellen nach einer bestimmten Zeit, zeigt Nachzügler.

- **Wiederholungsfunde**: Schwachstellen, die trotz vorheriger Tests erneut auftraten (zeigt Prozesslücken).
- **Testkostenanteil**: Verhältnis der Ausgaben für Pentests zum Gesamt-IT-Budget (Kontrolle der Kosteneffizienz).
- **Score in Security-Maturity-Modell**: z. B. Verbesserung im eigenen Reifegradmodell (SCAMPI, BSIMM o. Ä.).

Regelmäßige Berichte zu diesen KPIs (quartalsweise) helfen, den Fortschritt zu dokumentieren und gegenüber Führungsebene den Wert von Pentests nachzuweisen. Beispielsweise ist eine sinkende Anzahl kritischer Befunde bei konstantem Testschema ein positives Signal (bessere Grundabsicherung). Wichtig ist auch, qualitative Feedbacks einzuholen (z. B. wie aktuell die Testszenarien die realen Angriffsvektoren abbilden).

**7. Schlussfolgerungen und Ausblick**

Penetrationstests bleiben ein zentrales Element moderner IT-Sicherheitsstrategien. Die jüngsten Studien und Marktprognosen zeigen unmissverständlich: Der Bedarf an umfassenden, kontinuierlichen und technologisch modernen Pentests wächst. Unternehmen müssen aktiv auf diese Entwicklung reagieren. Die Kombination aus regulatorischem Druck (GDPR, NIS2, DORA), steigenden Cyberangriffen und neuen Technologien (Cloud, KI) verlangt ein proaktives Vorgehen.

Gleichzeitig bieten sich Chancen: Automatisierte Scans und KI-gestützte Sicherheitstools können Engpässe mildern und Pentests effizienter gestalten. Die Verschmelzung von Pentesting mit DevSecOps-Konzepten ermöglicht, dass Sicherheit stärker in den Entwicklungslebenszyklus integriert wird. Auch neue Prüfarten – etwa Pentests von künstlichen Intelligenzsystemen – eröffnen spezialisierte Beratungsfelder und Tools.

Zusammenfassend lässt sich sagen, dass Unternehmen durch ein strategisches Pentest-Programm ihre Sicherheitslage nachweislich verbessern können. Der Weg dahin erfordert Planung, Ressourcen und kontinuierliche Anpassung. Mit den in diesem Whitepaper vorgestellten Daten, Empfehlungen und Kennzahlen erhalten Entscheidungsträger und IT-Verantwortliche eine solide Grundlage, um Pentests effektiver zu gestalten und so Cyberrisiken nachhaltig zu reduzieren.

**Kernaussagen (Slide-Folien-Format)**

- **Große Testlücke:** 95 % aller Firmen halten Pentests für sehr wichtig – aber nur ~32 % testen regelmäßig ihre Systeme. Zwei Drittel der IT-Umgebungen bleiben so ungetestet.
- **Regulatorischer Zwang:** NIS2 (§30 BSIG) und andere Normen verpflichten zur Wirksamkeitsprüfung von Sicherheitsmaßnahmen (z. B. Pentests). Compliance- und Versicherungsanforderungen verstärken den Druck.

- **Marktwachstum:** Der globale Pentest-Markt wächst rasant (CAGR > 14 %). Prognosen sehen USD 4,39 Mrd bis 2031. Nordamerika führt (35,9 % Marktanteil), gefolgt von Europa (stärkerer Regulierungseffekt).
- **Technologie-Trends:** KI-gestützte „Agenten“ werden immer wichtiger. 87 % der Unternehmen pilotieren bereits KI-basierte Pentests. Automatisierung und Continuous Testing in DevOps-Umgebungen brechen traditionelle halbjährliche Testzyklen auf.
- **Herausforderungen:** Fachkräftemangel und Kosten sind die größten Barrieren. Gleichzeitig bieten KI-Tools und Plattformen neue Chancen (Anomalieerkennung, Simulation). Risikogesteuerte Ansätze (Threat-led Pentesting) gewinnen an Bedeutung.
- **Empfehlung:** Führen Sie ein **kontinuierliches Pentest-Programm** ein: Definieren Sie klare Scopes, kombinieren Sie manuelle und automatisierte Methoden, messen Sie Ihre Abdeckung (KPIs) und schließen Sie kritische Lücken zügig. Nutzen Sie Synergien mit anderen Prozessen (BCM, Incident Response, DevSecOps).
- **Langfristiger Nutzen:** Regelmäßige, gut integrierte Pentests senken langfristig das Risiko schwerer Sicherheitsvorfälle und stärken das Vertrauen von Kunden und Behörden in die Cyber-Resilienz des Unternehmens.

# Passende Weiterbildungen finden Sie hier:

## Weiterbildung zum Thema Recht

Finden Sie aus unserem erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

## e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt unverbindlich testen.

## Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

Wir garantieren fachlich hochwertige Weiterbildung für Ihren Erfolg – unsere ISO-Zertifizierungen nach 9001 und 21001 unterstreichen dies. Jetzt informieren

FORUM · Institut für Management GmbH · Postfach 10 50 60 · 69040 Heidelberg · Germany
Tel. +49 6221 500-500 · Fax +49 6221 500-555 · www.forum-institut.de