AWARE7 DIGITALE SICHERHEIT FÜR MENSCH & MASCHINE

WHITEPAPER

Penetrationstests in der Praxis

Der vollständige Leitfaden für Auftraggeber, Verantwortliche und Entscheider

HERAUSGEBER
AWARE7 GmbH

STAND
2026

VERSION
v1.0

KLASSIFIZIERUNG
TLP:GREEN

GRUNDLAGE
BSI IS-Pentest v1.2

ZIELGRUPPE
CISOs, IT-Leiter

Vorwort

Cyberangriffe sind heute keine Frage des Ob, sondern des Wann. Unternehmen jeder Größe sehen sich mit einer wachsenden Bedrohungslandschaft konfrontiert — von opportunistischen Ransomware-Kampagnen bis hin zu gezielten, staatlich geförderten Angriffen auf kritische Infrastrukturen.

Ein Penetrationstest ist eine der wirkungsvollsten Methoden, um die eigene Sicherheitslage realistisch zu bewerten. Er simuliert einen echten Angriff unter kontrollierten Bedingungen und zeigt auf, wo ein Angreifer tatsächlich eindringen könnte — bevor es ein echter Angreifer tut.

Dieses Whitepaper richtet sich an IT-Sicherheitsverantwortliche, CISOs und IT-Leiter, die erstmals einen Penetrationstest beauftragen, für dessen Durchführung verantwortlich sind oder die Ergebnisse in konkrete Maßnahmen übersetzen müssen. Es begleitet Sie durch den gesamten Lebenszyklus eines Pentests: von der rechtlichen Absicherung über die methodische Durchführung bis zur Auswertung und Remediation.

Als inhaltliche Grundlage dient der *Praxis-Leitfaden IS-Penetrationstests* des Bundesamts für Sicherheit in der Informationstechnik (BSI, Version 1.2), ergänzt durch die praktische Erfahrung der AWARE7 GmbH aus über einem Jahrzehnt offensiver Sicherheitsberatung.

> **AWARE7 GmbH** ist ein auf Offensive Security spezialisiertes Cybersicherheitsunternehmen mit Sitz in Gelsenkirchen. Unser Team aus zertifizierten Pentestern und Security-Analysten führt jährlich Hunderte von Penetrationstests für Unternehmen aus Industrie, Finanzwesen, Gesundheitswesen und öffentlicher Verwaltung durch.
>
> Weitere Informationen: a7.de

Inhaltsverzeichnis

1 Was ist ein Penetrationstest? 6
1.1 Abgrenzung: Was ein Pentest nicht ist 6
1.2 Angriffsszenarien: Black Box, Grey Box, White Box 6
1.3 Pentest vs. Red Team vs. Bug Bounty: Abgrenzung 7
1.4 Prüftiefe: Drei Stufen nach BSI 7
2 Rechtliche Grundlagen 10
2.1 Relevante Straftatbestände 10
2.2 Vertragsgestaltung: Rules of Engagement 10
2.3 DSGVO und Datenschutz 11
2.4 Betriebsrat und Mitbestimmung 11
2.5 Internationale Aspekte: Tests über Ländergrenzen hinweg 11
3 Scoping und Vorbereitung 14
3.1 Was gehört in den Scope? 14
3.2 Prüfumfang: Tiefe, Ort, Zeit 14
3.3 Notfallkommunikation und Eskalationspfade 15
3.4 Häufige Scoping-Fehler und wie Sie sie vermeiden 15
3.5 Vorbereitungs-Checkliste 16
4 Phasen der Durchführung 18
4.1 Übersicht: Phasen und BSI-Module 18
4.2 Phase 1: Informationsgewinnung (Reconnaissance) 18
4.3 Phase 2: Scanning und Enumeration 19
4.4 Phase 3: Schwachstellenanalyse (BSI-Module 1–3) 19
4.5 Phase 4: Exploitation (Modul 4) 19
4.6 Typische Werkzeuge und ihre Einsatzbereiche 20
5 Bewertungssysteme und Risikoklassifizierung 22
5.1 CVSS v3.1 — Common Vulnerability Scoring System 22
5.2 OWASP Top 10 (2021) 23
5.3 BSI-Klassifizierung 23
5.4 Risikobewertung im Kontext: Drei Fragen, die Sie stellen müssen 24
6 Reporting und Auswertung 26
6.1 Struktur eines professionellen Pentestberichts 26
6.2 Was einen guten von einem schlechten Bericht unterscheidet 26
6.3 Qualitätskriterien für den Abschlussbericht 27
6.4 Das Abschlussgespräch 27
7 Maßnahmen und Remediation 30
7.1 Priorisierung: Was zuerst beheben? 30
7.2 Quick Wins: Sofortmaßnahmen in 72 Stunden 30
7.3 Maßnahmenplan strukturieren 31
7.4 Re-Test: Verifikation der Maßnahmen 31
7.5 Typische Ursachen und strukturelle Gegenmaßnahmen 31
7.6 Pentest in der Sicherheitsstrategie: Wann und wie oft? 32
7.7 Lessons Learned 32
8 Fazit und nächste Schritte 35
8.1 Die wichtigsten Erkenntnisse auf einen Blick 35
8.2 Ihre Checkliste für den ersten Penetrationstest 35
8.3 Pentesting im regulatorischen Kontext 35

8.4 AWARE7 als Partner für Ihre Sicherheit 36
9 Anhang 38
9.1 Glossar 38
9.2 Beauftragungscheckliste 39
9.3 Weiterführende Ressourcen 40

01

Was ist ein Penetrationstest?

Definition, Abgrenzung und Prüftiefe nach BSI

Was ist ein Penetrationstest?

Ein IS-Penetrationstest (kurz: Pentest) ist ein autorisierter, gezielter Angriff auf ein IT-System, ein Netzwerk oder eine Anwendung, um dessen Angriffspotenzial zu ermitteln. Ziel ist es, realistische Aussagen darüber zu treffen, ob und wie weit ein Angreifer mit böswilliger Absicht in die untersuchten Systeme eindringen könnte.

DEFINITION

IS-Penetrationstest — Methode zur Feststellung des Angriffspotenzials auf IT-Netze, Systeme oder Anwendungen durch eine von der zu testenden Organisation unabhängige, qualifizierte Person unter Einsatz der Methoden und Werkzeuge eines tatsächlichen Angreifers — jedoch mit ausdrücklicher Genehmigung.

Abgrenzung: Was ein Pentest nicht ist

Ein Penetrationstest wird häufig mit anderen Prüfverfahren verwechselt. Die folgende Tabelle grenzt die wichtigsten Methoden ab:

Verfahren	Fokus	Typisches Ergebnis
Penetrationstest	Aktiver Angriff — kann ich eindringen?	Ausnutzbare Schwachstellen mit Nachweis
Schwachstellen-Scan	Automatisierte Erkennung — was ist potenziell anfällig?	Liste potenzieller Schwachstellen (ohne Verifikation)
IS-Revision / Audit	Konzeptionell — sind Maßnahmen geplant und dokumentiert?	Abweichungen von Soll-Zustand / Normen
Code Review	Statische Analyse — gibt es Fehler im Quellcode?	Sicherheitsmängel im Programmcode

Der Penetrationstest liefert als einziges Verfahren den *praktischen Nachweis* einer Ausnutzbarkeit. Er schließt damit die Lücke zwischen dem theoretischen Wissen über eine Schwachstelle und der Frage: „Kann ein Angreifer das wirklich ausnutzen?„

AWARE7-TIPP

Ein Schwachstellen-Scan ist kein Ersatz für einen Penetrationstest. Scanner erkennen bekannte Signaturen, aber keine logischen Fehler in Geschäftsprozessen, schwache Authentifizierungsimplementierungen oder verkettete Angriffe über mehrere Systeme. Für eine belastbare Sicherheitsbewertung ist der manuelle Pentest unverzichtbar.

Angriffsszenarien: Black Box, Grey Box, White Box

Je nach verfügbarem Vorwissen des Prüfers unterscheidet man drei grundlegende Angriffsszenarien:

Szenario	Vorwissen des Prüfers	Typischer Einsatz
Black Box	Keine Informationen — nur öffentlich verfügbare Daten	Simulation eines externen Angreifers ohne Insider-Wissen
Grey Box	Teilinformationen (z.B. Netzplan, Zugangsdaten)	Häufigster Fall in der Praxis — simuliert Insider-Bedrohung oder Partner mit Teilzugang
White Box	Volle Information (Architektur, Quellcode, Konfigurationen)	Maximale Prüftiefe — ideal für kritische Anwendungen und Quellcodeprüfungen

In der Praxis empfiehlt das BSI für die meisten Organisationen das *Grey-Box*-Szenario: Es ist effizienter als Black Box (weniger Zeit für Informationsgewinnung) und realistischer als White Box (deckt auch Konfigurationsfehler ab, die im Quellcode nicht sichtbar sind).

AWARE7-TIPP

Für einen Ersteinstieg empfehlen wir das Grey-Box-Szenario für externe Systeme kombiniert mit einem White-Box-Test für kritische Webanwendungen. So erhalten Sie maximale Abdeckung bei realistischem Budget.

Pentest vs. Red Team vs. Bug Bounty: Abgrenzung

Im Markt kursieren verschiedene Begriffe, die verwandte, aber unterschiedliche Leistungen beschreiben:

Leistung	Charakteristik	Typischer Einsatz	Zeitrahmen
Penetrationstest	Strukturierter, scope-definierter Test durch ein kleines Team; vollständige Dokumentation	Regelmäßige Sicherheitsüberprüfung, Compliance-Nachweis	1–4 Wochen
Red Team Exercise	Simulierter, langfristiger APT-Angriff auf Organisation und Menschen; kein fester Scope	Test von Detektions- und Reaktionsfähigkeit des gesamten Unternehmens	3–6 Monate
Bug Bounty Programm	Crowdsourcing von externen Sicherheitsforschern gegen Prämie; kein festes Team	Ergänzung zu regulären Tests; kontinuierliche Abdeckung	Dauerhaft
Vulnerability Assessment	Automatisierter Scan ohne manuelle Exploitverifikation	Schnelle Basislinie, häufige Wiederholung (wöchentlich/monatlich)	1–3 Tage

AWARE7-TIPP

Für die meisten mittelständischen Unternehmen ist der jährliche Penetrationstest der richtige Einstieg. Red Team Exercises empfehlen sich ab einer gewissen Sicherheitsreife — wenn Ihr SOC und Incident-Response-Prozesse bereits etabliert sind und Sie wissen möchten, ob diese auch in der Praxis funktionieren.

Prüftiefe: Drei Stufen nach BSI

Das BSI definiert drei Intensitätsstufen, die für unterschiedliche Risikoprofile und Budgets geeignet sind:

Stufe 1 — Sicherheitsaudit (nicht-invasiv)

Überprüfung von Konfigurationen, Patchständen und Netzwerkarchitektur ohne aktive Angriffe. Geringes Risiko für den Betrieb, aber begrenzte Aussagekraft über tatsächliche Ausnutzbarkeit.

Stufe 2 — Schwachstellenscan (nicht-invasiv)

Automatisierter Scan nach bekannten Schwachstellen. Kein aktives Ausnutzen der gefundenen Lücken. Gute Basislinie für regelmäßige Prüfungen, aber kein Nachweis der Ausnutzbarkeit.

Stufe 3 — Aktiver Penetrationstest (mit Exploits)

Gezielter manueller Einsatz von Exploits zur Verifikation von Schwachstellen. Höchste Aussagekraft, da der tatsächliche Angriffserfolg demonstriert wird. Das BSI empfiehlt, Exploits nur dann einzusetzen, wenn sie vom Prüfer vorab in einer Testumgebung validiert wurden, um Systemausfälle zu vermeiden.

> **AWARE7-TIPP**
>
> Für Produktionssysteme empfehlen wir Stufe 2 als Baseline und Stufe 3 für kritische Systeme in einem definierten Wartungsfenster. Destruktive Tests (DoS, Datenlöschung) sollten explizit ausgeschlossen werden.

02

Rechtliche Grundlagen

§§ 202a–303b StGB, DSGVO und Vertragsgestaltung

Rechtliche Grundlagen

Ein Penetrationstest ohne ausdrückliche schriftliche Genehmigung ist eine Straftat. Dies gilt uneingeschränkt — auch wenn ein Unternehmen den Test an eigenen Systemen durchführt, die sich in einer fremden Hosting-Umgebung befinden. Die rechtliche Absicherung ist daher der erste und wichtigste Schritt vor jedem Pentest.

DEFINITION

§ 202a StGB — Ausspähen von Daten — Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Relevante Straftatbestände

Paragraph	Tatbestand	Strafe
§ 202a StGB	Ausspähen von Daten (unberechtigter Zugang zu geschützten Systemen)	bis 3 Jahre
§ 202b StGB	Abfangen von Daten (Netzwerksniffing ohne Genehmigung)	bis 2 Jahre
§ 202c StGB	Vorbereitung (Besitz/Verbreitung von Hacking-Tools)	bis 2 Jahre
§ 303a StGB	Datenveränderung (unbeabsichtigte Modifikation von Daten)	bis 2 Jahre
§ 303b StGB	Computersabotage (Beeinträchtigung von Systemen)	bis 3 Jahre

Der Schlüssel zur legalen Durchführung ist die *Befugnis*: Liegt eine schriftliche, ausdrückliche Genehmigung des Systeminhabers vor, entfällt der Straftatbestand. Diese Genehmigung muss vor Testbeginn vorliegen — nicht nachträglich.

Vertragsgestaltung: Rules of Engagement

Ein Pentest-Vertrag (häufig als „Rules of Engagement„ bezeichnet) muss folgende Punkte explizit regeln:

- [ ] **Prüfumfang (Scope):** Welche IP-Adressen, Domains, Anwendungen, Netzwerke dürfen getestet werden? Explizite Ausschlüsse (Out-of-Scope) festhalten.
- [ ] **Zeitraum:** Start- und Enddatum, ggf. erlaubte Tageszeiten (z.B. außerhalb Geschäftszeiten für aktive Exploits).
- [ ] **Methoden:** Welche Angriffsmethoden sind erlaubt? Sind DoS-Tests, Social Engineering, physische Tests explizit eingeschlossen oder ausgeschlossen?
- [ ] **Notfallkontakte:** Wer ist beim Auftraggeber erreichbar, wenn ein kritischer Fund sofortige Meldung erfordert?
- [ ] **Datenschutz:** Wie werden personenbezogene Daten behandelt, die während des Tests zufällig gefunden werden? Speicherdauer, Löschfristen.

- [ ] **Geheimhaltung (NDA):** Vertraulichkeitsvereinbarung für alle gefundenen Schwachstellen und den Abschlussbericht.
- [ ] **Haftung:** Haftungsausschluss für Systemausfälle, die trotz sorgfältiger Testdurchführung entstehen.

> **AWARE7-TIPP**
>
> Prüfen Sie bei Cloud-Infrastruktur (AWS, Azure, GCP) immer die Penetration-Testing-Richtlinien des Cloud-Anbieters. Viele Anbieter verlangen eine separate Genehmigung oder schränken bestimmte Testmethoden ein. AWS z.B. erlaubt Pentests auf eigenen Ressourcen, verbietet jedoch DDoS-Simulationen.

DSGVO und Datenschutz

Während eines Penetrationstests werden möglicherweise personenbezogene Daten gefunden — in Datenbanken, Log-Dateien oder E-Mail-Systemen. Dies hat datenschutzrechtliche Konsequenzen:

Vor dem Test:
- Datenschutzbeauftragten (DSB) informieren und einbinden
- Vereinbarung zur Datenverarbeitung (AVV) mit dem Dienstleister abschließen
- Umgang mit gefundenen personenbezogenen Daten vertraglich regeln

Während des Tests:
- Gefundene personenbezogene Daten nur in dem Maß dokumentieren, wie für den Nachweis der Schwachstelle notwendig
- Keine unnötige Speicherung oder Weitergabe

Nach dem Test:
- Löschung aller personenbezogenen Daten beim Dienstleister nach definierter Frist
- Meldepflicht bei Datenpanne (Art. 33 DSGVO) prüfen, falls kritische Daten exponiert wurden

Betriebsrat und Mitbestimmung

In mitbestimmungspflichtigen Unternehmen ist der Betriebsrat bei Penetrationstests zu beteiligen, wenn Systeme getestet werden, über die Mitarbeiterdaten verarbeitet werden oder die Mitarbeiterüberwachung ermöglichen könnten (§ 87 Abs. 1 Nr. 6 BetrVG). Klären Sie dies frühzeitig mit Ihrer Rechts- oder HR-Abteilung.

> **AWARE7-TIPP**
>
> Beauftragen Sie niemals einen Penetrationstest, ohne vorher die Zustimmung aller betroffenen Systeminhaber schriftlich eingeholt zu haben — auch wenn es sich um gruppeninterne Systeme handelt. Eine mündliche Genehmigung reicht vor Gericht nicht aus.

Internationale Aspekte: Tests über Ländergrenzen hinweg

Bei grenzüberschreitenden Tests — etwa wenn ein deutsches Unternehmen Systeme in anderen Ländern testen lässt — gelten zusätzliche rechtliche Besonderheiten:

- **Anwendbares Recht:** Das Strafrecht des Landes gilt, in dem die Systeme betrieben werden. Ein Test aus Deutschland auf Server in den USA fällt unter US-amerikanisches Computerrecht (Computer Fraud and Abuse Act, CFAA).

- **Genehmigungen:** In vielen Ländern sind zusätzliche behördliche Genehmigungen für Sicherheitstests erforderlich.
- **Datenübertragung:** Werden im Test personenbezogene Daten übertragen, greift DSGVO und ggf. das Datenschutzrecht des Ziellandes.

AWARE7-TIPP

Klären Sie bei internationalen Tests frühzeitig mit Ihrem Rechtsanwalt und dem Pentest-Dienstleister, welches Recht gilt und welche Genehmigungen erforderlich sind. Dies gilt insbesondere für Tests auf Cloud-Infrastruktur, bei der Serverstandorte oft unklar sind.

03

Scoping und Vorbereitung

Scope-Definition, Prüfumfang und Notfallkommunikation

Scoping und Vorbereitung

Die Qualität eines Penetrationstests steht und fällt mit der Qualität des Scopes. Ein zu eng gefasster Scope führt zu einem blinden Fleck in der Sicherheitsbewertung; ein zu weit gefasster Scope sprengt Budget und Zeitplan.

Was gehört in den Scope?

Netzwerk-Scope

In-Scope (Beispiele)	Out-of-Scope (Beispiele)
Externes Perimeter (DMZ, Webserver, VPN-Gateways)	Produktionsdatenbanken mit Echtkundendaten
Internes Netzwerksegment (192.168.10.0/24)	OT/SCADA-Netzwerke (ohne expliziten Auftrag)
Active Directory / Domain Controller	Fremde Systeme (Mandanten, Partner)
Web Application Firewall (WAF) testen	DDoS-Simulation

Anwendungs-Scope

Für Webanwendungen und APIs sind zusätzlich festzulegen:
- Welche Domains / Subdomains sind in Scope?
- Welche Benutzerrollen dürfen getestet werden (Admin, normaler Nutzer, nicht-authentifiziert)?
- Gibt es Rate Limiting, das für den Test deaktiviert werden soll?
- Welche Testkonten werden bereitgestellt?

Cloud-Scope

Bei Cloud-Umgebungen (AWS, Azure, GCP) zusätzlich klären:
- Welche Subscriptions / Accounts / Projektbereiche sind in Scope?
- Ist die Cloud-Konfiguration (IAM-Policies, S3-Bucket-Permissions) Teil des Tests?
- Gelten die Pen-Testing-Richtlinien des Cloud-Anbieters?

Prüfumfang: Tiefe, Ort, Zeit

Das BSI empfiehlt, drei Dimensionen des Prüfumfangs vorab zu definieren:

Tiefe: Welche der drei BSI-Stufen (Sicherheitsaudit / Schwachstellenscan / aktiver Pentest) soll durchgeführt werden?

Ort:
- Remote-Test: Prüfer greift von außen über das Internet an (Standard für externe Perimeter)
- Vor-Ort-Test: Prüfer ist physisch im Netzwerk (erforderlich für interne Netzwerk-Tests)
- Hybrid: Remote für externe Systeme, Vor-Ort für interne Segmente

Zeit:
- Innerhalb der Geschäftszeiten (realistischste Simulation, aber höheres Betriebsrisiko)

- Außerhalb der Geschäftszeiten (geringeres Betriebsrisiko, gut für aktive Exploits)
- Über mehrere Wochen gestreckt (empfohlen für umfangreiche Tests)

Notfallkommunikation und Eskalationspfade

Definieren Sie vor Testbeginn einen klaren Eskalationspfad für folgende Szenarien:

- [ ] Kritische Schwachstelle gefunden: Sofortbenachrichtigung welcher Person?
- [ ] System bricht während des Tests ein: Wer ist der technische Ansprechpartner für Notabschaltung?
- [ ] Prüfer findet Hinweise auf aktiven Fremdangriff: Wie wird der Incident-Response-Prozess aktiviert?
- [ ] Testaktivitäten werden von SOC / SIEM blockiert: Wer kann die Whitelist-Freigabe erteilen?

AWARE7-TIPP

Führen Sie einen „Kickoff-Call„ mit allen Beteiligten durch, bevor der Test startet: Prüfer, IT-Betrieb, Projektverantwortlicher und ggf. SOC. Klären Sie Missverständnisse beim Scope, tauschen Sie Notfallkontakte aus und vereinbaren Sie das Kommunikationsprotokoll für kritische Funde.

FALLSTUDIE **Scope-Definition im Finanzdienstleistungssektor**

Ein mittelständischer Zahlungsdienstleister beauftragte AWARE7 mit einem externen Penetrationstest. Im Scoping-Gespräch stellte sich heraus, dass drei der fünf öffentlichen IP-Adressen zu einem Hosting-Partner gehörten, der separat kontaktiert werden musste. Zwei dieser Systeme befanden sich zudem in einer Cloud-Umgebung, für die der Anbieter eine gesonderte Test-Genehmigung benötigte.

Durch eine sorgfältige Scope-Definition und die frühzeitige Einholung aller Genehmigungen konnte der Test ohne Unterbrechungen durchgeführt werden. Kritisch: Einer der nicht genehmigten Cloud-Dienste enthielt — wie der anschließende White-Box-Test mit expliziter Genehmigung zeigte — eine kritische SSRF-Schwachstelle, die direkten Zugriff auf interne Cloud-Metadaten ermöglicht hätte.

Learnings: (1) Klären Sie Hosting-Zuständigkeiten vor dem Scoping-Gespräch. (2) Cloud-Dienste erfordern separate Genehmigungen. (3) Ein enger initialer Scope kann kritische Angriffsvektoren ausblenden.

Häufige Scoping-Fehler und wie Sie sie vermeiden

Aus unserer Praxis kennen wir die typischen Stolpersteine bei der Scope-Definition:

Häufiger Fehler	Empfehlung
„Testet einfach alles, was ihr findet“	Expliziten Scope definieren — offener Scope kann zu rechtlichen Problemen bei Drittsystemen führen
Produktionssysteme ohne Wartungsfenster testen	Aktive Exploits außerhalb der Geschäftszeiten vereinbaren; Notfallkontakt bereitstellen
Cloud-Systeme „automatisch“ in Scope annehmen	Genehmigung des Cloud-Anbieters vor Testbeginn einholen

SOC nicht informieren	Test-IPs whitelist-en; SOC-Team vor Testbeginn briefen, sonst False-Incident-Response
Scope nach Testbeginn erweitern	Scope-Änderungen nur schriftlich und mit Genehmigung — mündliche Erweiterungen sind rechtlich problematisch

Vorbereitungs-Checkliste

- [ ] Schriftliche Genehmigung aller Systeminhaber liegt vor
- [ ] Pentest-Vertrag mit Rules of Engagement unterzeichnet
- [ ] NDA mit dem Dienstleister abgeschlossen
- [ ] Datenschutzbeauftragten informiert, AVV abgeschlossen
- [ ] Scope-Dokument mit In-Scope und Out-of-Scope finalisiert
- [ ] Testkonten mit definierten Rechten bereitgestellt
- [ ] Notfallkontakte (IT-Betrieb, Management, Prüfer) ausgetauscht
- [ ] SOC / SIEM informiert
- [ ] Betriebsrat informiert / Mitbestimmung geprüft
- [ ] Bei Cloud: Genehmigung des Cloud-Anbieters eingeholt

04

Phasen der Durchführung

Von der Reconnaissance bis zur Dokumentation

Phasen der Durchführung

Ein professioneller Penetrationstest folgt einem strukturierten, methodischen Ablauf. Das BSI unterteilt die praktische Prüfung in vier Module, die aufeinander aufbauen.

Übersicht: Phasen und BSI-Module

Phase	Aktivitäten	BSI-Modul
1. Informationsgewinnung	OSINT, DNS-Enumeration, Service-Discovery	Modul 1: Konzeptionelle Schwächen
2. Scanning & Enumeration	Port-Scan, Service-Fingerprinting, Versionsidentifikation	Modul 2: Umsetzung Härtungsmaßnahmen
3. Schwachstellenanalyse	Automatisierter Scan, manuelle Analyse, CVE-Recherche	Modul 3: Bekannte Schwachstellen
4. Exploitation	Manuelle Exploit-Verifikation, Privilege Escalation, Pivoting	Modul 4 (optional): Exploit-Einsatz
5. Dokumentation	Lückenlose Aufzeichnung aller Aktivitäten, Screenshots, Logs	Grundlage für Abschlussbericht

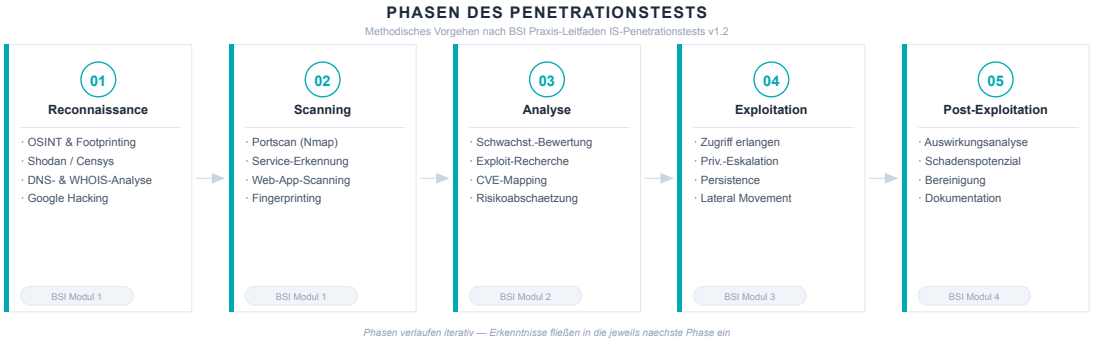

Abbildung 1: Typischer Ablauf eines Penetrationstests — von der Informationsgewinnung bis zur Dokumentation

Phase 1: Informationsgewinnung (Reconnaissance)

Ziel ist die systematische Sammlung aller öffentlich verfügbaren Informationen über das Ziel — ohne aktive Interaktion mit den Systemen (passives Recon) oder mit minimaler Interaktion (aktives Recon).

Typische Aktivitäten:

- **OSINT:** Suche nach Mitarbeiterdaten (LinkedIn, XING), E-Mail-Adressen, Technologie-Fingerprints (Shodan, Censys)
- **DNS-Enumeration:** Subdomain-Discovery, MX-Records, SPF/DKIM-Konfiguration
- **Google Dorking:** Suche nach exponierten Dateien, Login-Seiten, Konfigurationsfehlern
- **Certificate Transparency:** Subdomains aus SSL-Zertifikaten extrahieren

AWARE7-TIPP

Was Ihr Pentest-Dienstleister in Phase 1 über Sie herausfindet, kann ein echter Angreifer ebenfalls herausfinden — kostenlos und ohne Ihre Kenntnis. Beauftragen Sie daher regelmäßig eine *Angriffsflächen-Analyse* (Attack Surface Assessment), um Ihre öffentliche Sichtbarkeit zu kennen.

Phase 2: Scanning und Enumeration

Auf Basis der in Phase 1 gesammelten Informationen werden die in Scope befindlichen Systeme aktiv gescannt.

Typische Aktivitäten:
- **Port-Scan:** Identifikation offener TCP/UDP-Ports (Nmap, Masscan)
- **Service-Fingerprinting:** Identifikation laufender Dienste und ihrer Versionen
- **Betriebssystem-Identifikation:** Windows, Linux, Appliances
- **Web Application Discovery:** Crawling, Verzeichnis-Enumeration, API-Endpoint-Discovery

Scanning-Aktivitäten erzeugen Netzwerkverkehr, der von Firewalls und IDS/IPS-Systemen erkannt werden kann. Informieren Sie Ihr SOC-Team, damit Test-Traffic nicht als Incident behandelt wird.

Phase 3: Schwachstellenanalyse (BSI-Module 1–3)

Modul 1 — Konzeptionelle Schwächen: Überprüfung der Netzwerkarchitektur, Segmentierung, Firewall-Regeln und Authentifizierungskonzepte.

Modul 2 — Härtungsmaßnahmen: Sind alle bekannten Best Practices umgesetzt? Offene Ports, unnötige Dienste, Standard-Passwörter, veraltete Protokolle (Telnet, FTP, SNMPv1), fehlende Verschlüsselung.

Modul 3 — Bekannte Schwachstellen: Automatisierter Einsatz von Schwachstellen-Scannern (Nessus, OpenVAS) kombiniert mit manueller CVE-Recherche.

Phase 4: Exploitation (Modul 4)

Dies ist die Phase, in der aus potenziellen Schwachstellen echte Angriffsvektoren werden.

Typische Techniken:
- **Remote Code Execution (RCE):** Codeausführung auf dem Zielsystem
- **SQL Injection:** Extraktion von Datenbankdaten, ggf. Systemzugriff
- **Privilege Escalation:** Vom niedrig-privilegierten Benutzer zum Administrator/Root
- **Pass-the-Hash / Pass-the-Ticket:** Missbrauch von Windows-Authentifizierungs-Artefakten
- **Lateral Movement:** Ausbreitung im Netzwerk über kompromittierte Systeme
- **Pivoting:** Nutzung kompromittierter Systeme als Sprungbrett in weiter abgeschottete Segmente

Das BSI empfiehlt *moderate Angriffsstärke* und rät von destruktiven Tests ohne expliziten Auftrag ab.

AWARE7-TIPP

Fordern Sie vom Dienstleister lückenlose Protokollierung aller Exploitation-Aktivitäten — mit Timestamps, verwendeten Tools und Screenshot-Nachweisen. Das ist nicht nur für den Bericht wichtig, sondern auch für die Abgrenzung zu einem echten Angriff, falls Ihr SOC Alarm schlägt.

FALLSTUDIE **Angriffspfad in einem Industrieunternehmen**

Bei einem Grey-Box-Test eines Maschinenbauunternehmens identifizierte das AWARE7-Team zunächst in Phase 2 einen veralteten Citrix-Gateway mit einer bekannten CVE (CVSSv3: 9.8 — kritisch). Über diese Schwachstelle wurde ein initiales Foothold im DMZ-Segment erlangt.

Im internen Netzwerk fand das Team über Modul-2-Prüfung eine Vielzahl an Windows-Systemen mit veralteten SMB-Konfigurationen. Durch Pass-the-Hash-Angriff auf einen lokalen Admin-Account wurde Lateral Movement in das OT-nahe Segment möglich.

Ergebnis: Kompletter Angriffspfad vom Internet bis in die Nähe des OT-Netzwerks in weniger als 4 Stunden. Kein Single Point of Failure, sondern eine Kette aus: ungepatchtem Gateway + fehlender Netzwerksegmentierung + schwacher Password Policy.

Learnings: Einzelne Schwachstellen sind selten kritisch. Entscheidend ist die Kombination und die fehlende Tiefenverteidigung (Defense in Depth).

Typische Werkzeuge und ihre Einsatzbereiche

Ein professioneller Pentest-Dienstleister setzt eine Kombination aus etablierten Open-Source-Tools und kommerziellen Produkten ein. Die folgende Übersicht gibt Auftraggebern einen Einblick in gängige Werkzeuge — nicht um selbst zu testen, sondern um im Gespräch mit dem Dienstleister informiert zu sein.

Werkzeug	Einsatzbereich	Typ
Nmap	Port-Scanning, Service-Erkennung, OS-Fingerprinting	Open Source
Nessus / OpenVAS	Automatisierter Schwachstellenscan	Kommerziell / OS
Metasploit Framework	Exploit-Entwicklung und -Ausführung, Post-Exploitation	Open Source
Burp Suite	Web Application Testing, HTTP-Interception, Active Scanning	Kommerziell
BloodHound / SharpHound	Active Directory Angriffspfad-Analyse	Open Source
Mimikatz	Windows Credential Extraction, Pass-the-Hash	Open Source
Cobalt Strike	Red Team Command & Control, Lateral Movement	Kommerziell
theHarvester / Maltego	OSINT, E-Mail- und Domain-Enumeration	Open Source / Komm.

AWARE7-TIPP

Fragen Sie Ihren Pentest-Dienstleister nach dem eingesetzten Tool-Set. Ein seriöser Anbieter ist transparent über seine Methodik und kann erklären, warum er welches Werkzeug für welchen Zweck einsetzt. Werkzeuge allein machen keinen guten Pentest — es ist das Know-how, sie richtig einzusetzen und die Ergebnisse zu interpretieren.

05

Bewertungssysteme

CVSS v3.1, OWASP Top 10 und BSI-Klassifizierung

Bewertungssysteme und Risikoklassifizierung

Die Ergebnisse eines Penetrationstests sind nur so wertvoll wie die Methodik ihrer Bewertung. Ohne einheitliche Maßstäbe ist ein Vergleich zwischen Berichten verschiedener Dienstleister unmöglich.

CVSS v3.1 — Common Vulnerability Scoring System

Das CVSS ist der internationale Standard zur Bewertung der Schwere von Sicherheitslücken. Version 3.1 ist der aktuelle Standard; er wird u.a. von NIST, BSI und allen namhaften Schwachstellen-Datenbanken (NVD, CVE) verwendet.

Die drei CVSS-Vektoren

Base Score (0.0–10.0): Bewertet die intrinsischen Eigenschaften einer Schwachstelle — unabhängig von Umgebung und Zeit:

Metrik	Fragestellung	Werte
Attack Vector (AV)	Wie ist die Schwachstelle erreichbar?	Network / Adjacent / Local / Physical
Attack Complexity (AC)	Wie aufwändig ist der Angriff?	Low / High
Privileges Required (PR)	Welche Rechte braucht der Angreifer?	None / Low / High
User Interaction (UI)	Ist Nutzerinteraktion nötig?	None / Required
Confidentiality / Integrity / Availability	Welche Auswirkungen hat eine Ausnutzung?	None / Low / High

Temporal Score: Berücksichtigt die Verfügbarkeit eines Exploits und die Maturität des Patches.

Environmental Score: Passt den Score auf die spezifische Umgebung an.

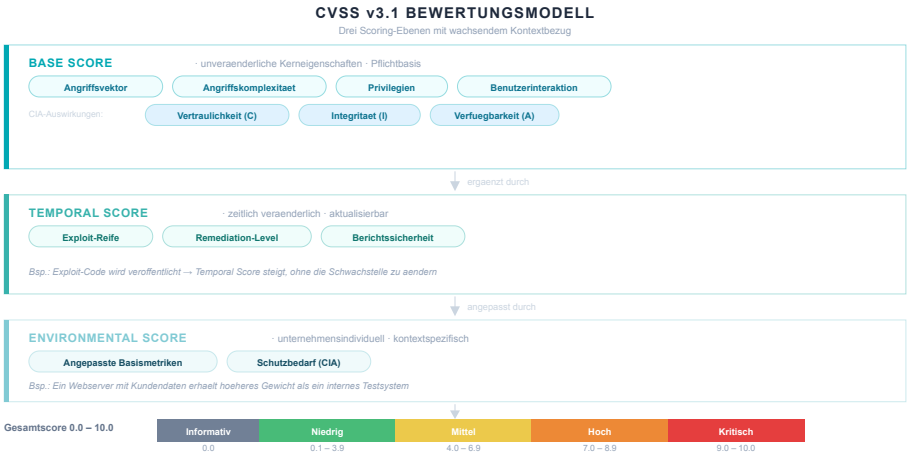

Abbildung 2: CVSS v3.1 — Dreischichtiges Bewertungsmodell von intrinsisch (Base) bis kontextbezogen (Environmental)

CVSS-Schweregrade und Handlungsempfehlungen

Score	Schwere	Handlungsempfehlung	Frist
9.0–10.0	KRITISCH	Sofortige Eskalation, Notfallpatch oder Isolierung des Systems	24–72h
7.0–8.9	HOCH	Patch im nächsten Wartungsfenster, Workaround umgehend	7–14 Tage
4.0–6.9	MITTEL	Patch im regulären Patch-Zyklus	30–60 Tage
0.1–3.9	NIEDRIG	Risikobewertung und ggf. Akzeptanz	90+ Tage

AWARE7-TIPP

CVSS ist kein absolutes Risikomaß — es bewertet die Schwachstelle, nicht Ihr spezifisches Risiko. Ein CVSS 9.5 auf einem System ohne Internetexposition kann weniger kritisch sein als ein CVSS 6.5 auf Ihrem öffentlichen Login-Portal. Fordern Sie immer eine kontextualisierte Risikobewertung vom Dienstleister.

OWASP Top 10 (2021)

Die *OWASP Top 10* ist für Webanwendungen der wichtigste Referenzrahmen:

Rang	Schwachstellenklasse
A01	Broken Access Control — Fehlende oder fehlerhafte Zugriffskontrolle
A02	Cryptographic Failures — Schwache oder fehlende Verschlüsselung
A03	Injection — SQL, LDAP, Command Injection
A04	Insecure Design — Architektonische Sicherheitsmängel
A05	Security Misconfiguration — Fehlkonfigurationen in allen Schichten
A06	Vulnerable and Outdated Components — Veraltete Bibliotheken/Frameworks
A07	Identification and Authentication Failures — Schwaches Passwort, fehlendes MFA
A08	Software and Data Integrity Failures — Supply-Chain-Angriffe
A09	Security Logging and Monitoring Failures — Fehlende Erkennungsfähigkeit
A10	Server-Side Request Forgery (SSRF)

BSI-Klassifizierung

Klasse	Beschreibung	Beispiel
Kritisch	Unmittelbare Ausnutzung ohne Voraussetzungen möglich, weitreichender Schaden	Unauthentifizierte RCE über Internet

Hoch	Ausnutzung mit geringem Aufwand, signifikanter Schaden	Authenticated SQL Injection mit DB-Dump-Möglichkeit
Mittel	Ausnutzung erfordert besondere Bedingungen oder weitere Schwachstellen	XSS ohne Zugriff auf sensible Daten
Niedrig	Minimales Schadenspotenzial, Information Disclosure	Versionsinformationen in HTTP-Headern

Risikobewertung im Kontext: Drei Fragen, die Sie stellen müssen

Ein CVSS-Score allein reicht nicht. Stellen Sie Ihrem Dienstleister nach dem Test diese drei Fragen für jedes kritische Finding:

Frage 1: Wie wahrscheinlich ist die Ausnutzung in unserem konkreten Umfeld? Ein Remote-Exploit ist nur dann kritisch, wenn das betroffene System tatsächlich aus dem Internet erreichbar ist. Systeme hinter VPN, Firewall oder in isolierten Segmenten haben ein deutlich geringeres Expositionsrisiko.

Frage 2: Was ist der tatsächliche Schaden, wenn die Schwachstelle ausgenutzt wird? CVSS bewertet theoretischen Maximalschaden. Realistische Frage: Was verlieren wir konkret? Kundendaten? Produktionsstillstand? Reputationsschaden? Die Antwort bestimmt die Geschäftsrelevanz des Findings.

Frage 3: Gibt es bereits kompensierende Kontrollen? Manche Schwachstellen werden durch vorhandene Schutzmaßnahmen (WAF, IDS/IPS, Netzwerksegmentierung, Monitoring) bereits teilweise mitigiert. Der Environmental Score in CVSS kann diese Faktoren abbilden.

> **AWARE7-TIPP**
>
> Fordern Sie für jede kritische oder hohe Schwachstelle eine schriftliche Antwort auf diese drei Fragen im Abschlussbericht. Das ist die Basis für eine informierte Risikoentscheidung des Managements.

> **AWARE7-TIPP**
>
> Bestehen Sie darauf, dass Ihr Dienstleister im Abschlussbericht sowohl den CVSS-Base-Score als auch eine kontextbezogene Risikoeinschätzung dokumentiert.

06

Reporting und Auswertung

Berichtsstruktur, Qualitätskriterien und Abschlussgespräch

Reporting und Auswertung

Ein Penetrationstest ist nur so gut wie sein Abschlussbericht. Ein professioneller Bericht übersetzt technische Befunde in verständliche Risikobewertungen, gibt klare Handlungsempfehlungen und ist auf unterschiedliche Zielgruppen zugeschnitten.

Struktur eines professionellen Pentestberichts

Teil 1: Management Summary (2–4 Seiten)

Richtet sich an Entscheider und IT-Führungskräfte ohne tiefes technisches Wissen.

Pflichtinhalt:

- **Auftrag und Scope:** Was wurde getestet, in welchem Zeitraum?
- **Gesamtbewertung:** Eine klare Gesamtaussage zur Sicherheitslage
- **Kernbefunde:** Die drei bis fünf kritischsten Schwachstellen in nicht-technischer Sprache
- **Angriffsnarration:** Wie weit hätte ein Angreifer kommen können?
- **Sofortmaßnahmen:** Was muss sofort getan werden?
- **Gesamtempfehlung:** Mittelfristige Handlungsempfehlung in 3–5 Punkten

Teil 2: Technischer Anhang (Hauptteil)

Richtet sich an Systemadministratoren, Entwickler und Security-Teams. Enthält für jede Schwachstelle:

- [ ] **Finding-ID:** Eindeutige Identifikation für Tracking im Maßnahmenplan
- [ ] **CVSS-Score:** Base Score + Vector String
- [ ] **Beschreibung:** Was ist die Schwachstelle technisch?
- [ ] **Nachweis (Evidence):** Screenshots, Logs, Netzwerktraffic-Auszüge
- [ ] **Angriffsszenario:** Wie kann ein Angreifer die Schwachstelle ausnutzen?
- [ ] **Risikobewertung:** Kontextualisierter Schaden für das konkrete Unternehmen
- [ ] **Handlungsempfehlung:** Konkrete, umsetzbare Maßnahme mit Referenz (CVE, CWE, OWASP)
- [ ] **Schwierigkeitsgrad der Behebung:** Einfach / Mittel / Komplex

Was einen guten von einem schlechten Bericht unterscheidet

Guter Bericht	Schlechter Bericht
Klare Management Summary ohne Fachjargon	Nur technische Details, kein Management-Teil
Kontextualisierte Risikobewertung für das Unternehmen	CVSS-Score ohne Kontextualisierung

Reproduzierbare Schritte für jedes Finding	Vage Beschreibungen ohne Nachweis
Konkrete, priorisierte Handlungsempfehlungen	Generische Empfehlungen („Bitte patchen“)
Angriffspfade visualisiert	Isolierte Einzelfunde ohne Zusammenhang
Aussagen zu getesteten und NICHT gefundenen Bereichen	Nur Schwachstellen, kein Nachweis der Abdeckung

Qualitätskriterien für den Abschlussbericht

Neben dem Inhalt ist auch die Form des Berichts ein Qualitätsmerkmal. Stellen Sie sicher, dass der Bericht folgende Kriterien erfüllt:

Nachvollziehbarkeit

Jedes Finding muss reproduzierbar sein. Ein guter Bericht enthält:
- Exakte Angaben zu Zeitstempel, verwendetem Tool und Version
- Screenshots mit Markierungen der relevanten Stellen
- Netzwerktraffic-Auszüge (z.B. aus Burp Suite oder Wireshark) als Beweis
- Schritt-für-Schritt-Anleitung zur Reproduktion der Schwachstelle

Vollständigkeit der Abdeckung

Der Bericht soll nicht nur dokumentieren, was gefunden wurde, sondern auch was geprüft und **nicht** als Schwachstelle bewertet wurde. Dies gibt Ihnen Sicherheit, dass bestimmte Bereiche tatsächlich getestet wurden.

Verständlichkeit für unterschiedliche Zielgruppen

Zielgruppe	Benötigte Information	Berichtsteil
Geschäftsführung / Board	Gesamtrisiko, Handlungsbedarf, Budget-Implikation	Executive Summary (1 Seite)
CISO / IT-Leiter	Priorisierte Findings, Maßnahmenplan, Zeitplan	Management Summary (3–4 Seiten)
Systemadministratoren	Technische Details, Reproduktionsschritte, konkrete Patches	Technischer Anhang
Entwickler	Schwachstellenklasse, CWE-Referenz, Code-Beispiel	Entwickler-spezifische Findings

> **AWARE7-TIPP**
>
> Ein Pentest-Bericht sollte nicht „für den Prüfer“ geschrieben sein, sondern für den Auftraggeber. Wenn Ihr IT-Team den Bericht nicht versteht oder das Management keine Entscheidungsgrundlage darin findet, hat der Bericht seinen Zweck verfehlt — unabhängig von der technischen Qualität der Tests.

Das Abschlussgespräch

Das Abschlussgespräch ist ein oft unterschätzter Teil des Pentest-Prozesses. Nutzen Sie es, um:

- **Befunde direkt zu besprechen:** Der Prüfer kann technische Fragen sofort klären
- **Prioritäten gemeinsam festzulegen:** Welches Finding ist für Ihr Unternehmen wirklich kritisch?
- **Quick Wins zu identifizieren:** Was kann in den nächsten 48 Stunden umgesetzt werden?
- **Maßnahmenplan zu initiieren:** Wer ist verantwortlich für welches Finding?

Laden Sie zum Abschlussgespräch ein: CISO / IT-Leiter, System-Owner der betroffenen Systeme und den Projektleiter.

FALLSTUDIE **Was einen Pentest-Bericht wirklich wirksam macht**

Ein öffentliches Versorgungsunternehmen erhielt nach einem Penetrationstest einen 80-seitigen technischen Bericht ohne Management Summary. Das IT-Team verstand die Befunde, hatte aber keine Möglichkeit, dem Management die Dringlichkeit zu vermitteln. Drei der fünf kritischen Schwachstellen blieben sechs Monate lang offen — mangels Budget-Freigabe.

Im Folgeauftrag bei AWARE7 wurde der Bericht in zwei Teile gegliedert: Eine 3-seitige Management Summary mit Ampelbewertung und Angriffspfad-Narration, gefolgt vom technischen Teil. Das Ergebnis: In der Management-Präsentation wurden alle kritischen Findings innerhalb von zwei Wochen priorisiert und mit Budget hinterlegt.

Learnings: Ein Bericht, den das Management nicht versteht, führt zu keinen Maßnahmen. Die Management Summary ist kein Anhang — sie ist das wichtigste Kapitel des Berichts.

AWARE7-TIPP

Fordern Sie vor Beauftragung ein Muster-Berichtsformat vom Dienstleister an. Ein schlechtes Berichtsformat ist ein Warnsignal für die Qualität des gesamten Tests.

07

Maßnahmen und Remediation

Priorisierung, Quick Wins und Re-Test

Maßnahmen und Remediation

Der Penetrationstest endet nicht mit dem Abschlussbericht. Die eigentliche Wertschöpfung entsteht erst durch die konsequente Umsetzung der empfohlenen Maßnahmen.

Priorisierung: Was zuerst beheben?

Quadrant	Beschreibung	Empfohlene Aktion
Hoch/Kritisch + Einfach	Hoher Schweregrad, geringer Behebungsaufwand	**Quick Wins** — sofort umsetzen (24–72h)
Hoch/Kritisch + Komplex	Hoher Schweregrad, hoher Behebungsaufwand	Workaround sofort, vollständige Behebung geplant
Mittel + Einfach	Mittlerer Schweregrad, geringer Aufwand	Im nächsten Patch-Zyklus (30 Tage)
Mittel/Niedrig + Komplex	Geringer Schweregrad, hoher Aufwand	Risikoakzeptanz prüfen oder langfristig einplanen

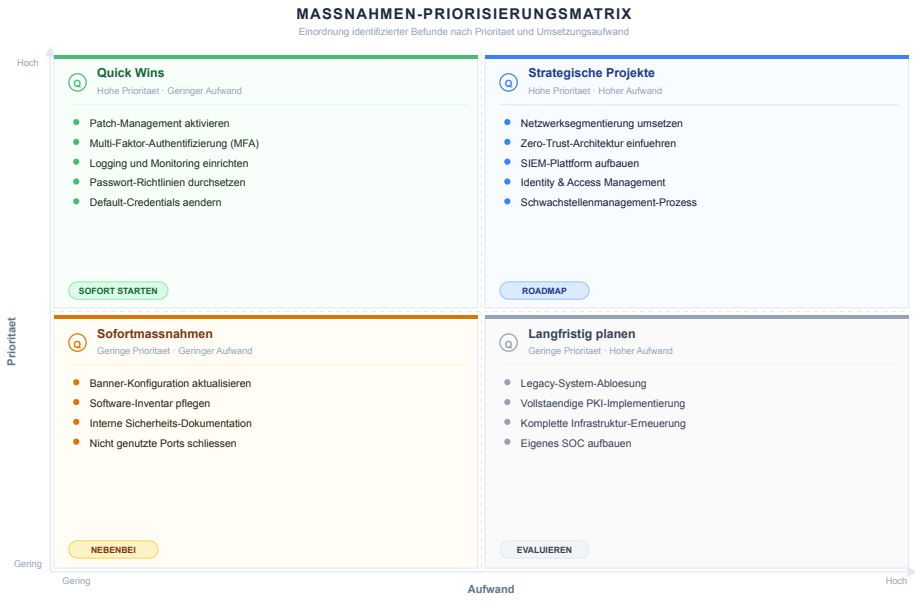

Abbildung 3: Maßnahmen-Priorisierungsmatrix nach Pentest — Schweregrad vs. Behebungsaufwand

Quick Wins: Sofortmaßnahmen in 72 Stunden

- [ ] Veraltete und unnötige Dienste deaktivieren (z.B. Telnet, FTP, SNMPv1)
- [ ] Standard-Passwörter auf Appliances und Diensten ändern
- [ ] Fehlende Security-Header in Webanwendungen ergänzen (HSTS, CSP, X-Frame-Options)

- [ ] Öffentlich exponierte sensible Dateien entfernen (.git, .env, Backup-Dateien)
- [ ] Multi-Faktor-Authentifizierung für Remote-Zugänge (VPN, RDP, Admin-Interfaces) aktivieren
- [ ] Kritische Patches für als ausnutzbar bestätigte CVEs einspielen

Maßnahmenplan strukturieren

Erstellen Sie für jedes Finding eine Maßnahme mit folgenden Pflichtfeldern:

Feld	Beschreibung
Finding-ID	Referenz auf den Pentest-Bericht (z.B. PT-2026-042)
Verantwortlich	Person oder Team, das die Maßnahme umsetzt
Fälligkeitsdatum	Basierend auf Priorität und Aufwand
Maßnahme	Konkrete technische Handlung (nicht: „Sicherheit verbessern“)
Status	Offen / In Bearbeitung / Umgesetzt / Akzeptiert
Nachweis	Screenshot, Change-Ticket, Test-Ergebnis als Beleg der Umsetzung

Re-Test: Verifikation der Maßnahmen

Vollständiger Re-Test: Erneute Durchführung des kompletten Penetrationstests nach 6–12 Monaten oder nach größeren Architekturänderungen.

Gezielter Verifikationstest: Nur die zuvor gefundenen Schwachstellen werden erneut geprüft. Kostengünstiger und schneller — ideal für den Nachweis der Behebung.

> **AWARE7-TIPP**
>
> Vereinbaren Sie den Re-Test bereits im initialen Pentest-Vertrag. Der Re-Test-Bericht ist auch ein wertvolles Dokument für Compliance-Nachweise gegenüber Versicherungen, Auditoren und Kunden.

Typische Ursachen und strukturelle Gegenmaßnahmen

Die Erfahrung aus Hunderten von Penetrationstests zeigt, dass die meisten kritischen Schwachstellen auf eine begrenzte Anzahl wiederkehrender Ursachen zurückzuführen sind. Die folgende Tabelle listet die häufigsten Ursachen und die empfohlenen strukturellen Gegenmaßnahmen:

Häufige Ursache	Strukturelle Gegenmaßnahme
Veraltete Softwareversionen / fehlendes Patch-Management	Etablierung eines regelmäßigen Patch-Zyklus (z.B. monatlich) mit Vulnerability-Tracking
Fehlende Netzwerksegmentierung	Netzwerk-Redesign nach Zero-Trust-Prinzip; Micro-Segmentierung für kritische Assets

Schwache oder fehlende Authentifizierung	MFA für alle externen Zugänge (VPN, RDP, Admin-Interfaces, SaaS); Passwort-Policy durchsetzen
Exponierte Management-Interfaces im Internet	Management-Zugänge nur über VPN; Jump-Host-Konzept einführen
Unsichere Webanwendungskonfiguration	Security-Header-Policy, WAF, regelmäßige DAST-Tests im CI/CD-Pipeline
Übermäßige Berechtigungen (Least Privilege verletzt)	Regelmäßige Berechtigungsreviews; Privileged Access Management (PAM) einführen
Fehlende Logging- und Monitoring-Fähigkeit	SIEM einführen oder ausbauen; Detection Engineering für kritische Angriffsmuster

AWARE7-TIPP

Betrachten Sie die Findings eines Penetrationstests nicht als isolierte technische Probleme, sondern als Symptome struktureller Schwächen. Eine Häufung bestimmter Schwachstellen (z.B. viele veraltete Dienste) deutet auf ein systematisches Problem hin — zum Beispiel fehlendes Patch-Management — das strategisch adressiert werden muss.

Pentest in der Sicherheitsstrategie: Wann und wie oft?

Ein Penetrationstest ist kein einmaliges Ereignis. Die Frage ist nicht ob, sondern wann und in welchen Zyklen. Die folgende Übersicht hilft Ihnen, die richtige Testfrequenz für Ihre Organisation festzulegen:

Auslöser	Empfohlene Testart	Begründung
Jährlicher Zyklus (Baseline)	Externer Pentest	Deckt neue Bedrohungen und Konfigurationsänderungen ab
Neue kritische Anwendung / Service-Launch	Web App Pentest	Sicherheitsfreigabe vor Produktionsstart
Größere Infrastruktur-Änderung (Cloud-Migration, Merger)	Interner Pentest	Neue Architektur bringt neue Angriffsflächen
Nach kritischem Sicherheitsvorfall	Re-Test + Red Team	Nachweis der Behebung und Resilienztest
Compliance (ISO 27001, DORA, NIS2)	Scope nach Norm	Nachweis für Zertifizierung / Auditoren

Lessons Learned

Nach jedem Pentest-Zyklus lohnt sich eine kurze Retrospektive:

- Welche Schwachstellen hätten durch bestehende Prozesse früher erkannt werden können?
- Wo war der Scope zu eng oder zu weit?
- Welche strukturellen Sicherheitsprobleme sollten vor dem nächsten Test adressiert werden?
- Hat die Kommunikation zwischen Prüfer und IT-Betrieb reibungslos funktioniert?
- Wurden alle Quick Wins innerhalb der vereinbarten Fristen umgesetzt?

Die Antworten auf diese Fragen fließen direkt in die Planung des nächsten Testzyklus ein. Dokumentieren Sie die Lessons Learned in einem kurzen internen Bericht und legen Sie ihn neben den Pentest-Abschlussbericht — so entsteht über mehrere Zyklen ein wertvolles institutionelles Gedächtnis über Ihre Sicherheitsentwicklung.

AWARE7-TIPP

Benchmarken Sie Ihre Findings über mehrere Testzyklen: Sinkt die Anzahl kritischer und hoher Schwachstellen? Verkürzen sich die Behebungszeiten? Diese Kennzahlen zeigen dem Management messbare Fortschritte Ihres Sicherheitsprogramms und rechtfertigen Investitionen in präventive Maßnahmen.

08

Fazit und nächste Schritte

Erkenntnisse, Checkliste und regulatorischer Kontext

Fazit und nächste Schritte

Ein Penetrationstest ist keine einmalige Maßnahme, sondern ein fester Bestandteil eines reifen Sicherheitsprogramms.

Die wichtigsten Erkenntnisse auf einen Blick

- **Rechtliche Grundlage zuerst:** Kein Pentest ohne schriftliche Genehmigung und klare Rules of Engagement.
- **Scope bestimmt den Wert:** Ein gut definierter Scope ist die Grundlage für einen Pentest mit echtem Erkenntnisgewinn.
- **Methodik schlägt Werkzeug:** Automated Scanning findet, was bekannt ist. Manuelle Tests finden, was versteckt ist.
- **CVSS kontextualisieren:** Ein Schweregrad ohne Kontext ist wertlos. Bestehen Sie auf einer unternehmensindividuellen Risikobewertung.
- **Der Bericht ist das Produkt:** Fordern Sie einen Bericht, der vom Management verstanden und vom IT-Team umgesetzt werden kann.
- **Remediation schließt den Kreis:** Der Test ohne Maßnahmenplan und Re-Test hat keinen nachhaltigen Sicherheitsgewinn.

Ihre Checkliste für den ersten Penetrationstest

- [ ] Ziel und Scope definiert
- [ ] Genehmigungen aller Systeminhaber eingeholt
- [ ] Datenschutzbeauftragten informiert, AVV abgeschlossen
- [ ] Pentest-Vertrag mit Rules of Engagement unterzeichnet
- [ ] Angriffsszenarien und Prüftiefe festgelegt
- [ ] Testkonten und Zugangsvoraussetzungen vorbereitet
- [ ] Notfallkontakte und Eskalationspfade definiert
- [ ] SOC / IT-Betrieb über den Testtermin informiert
- [ ] Abschlussgespräch mit allen Beteiligten eingeplant
- [ ] Re-Test-Termin vorgemerkt

Pentesting im regulatorischen Kontext

Penetrationstests sind zunehmend nicht nur eine Best Practice, sondern eine regulatorische Anforderung. Die folgende Übersicht zeigt, welche Normen und Gesetze Penetrationstests explizit fordern oder empfehlen:

Regulierung / Norm	Anforderung	Pflicht
ISO 27001:2022 (A.8.8)	Management von Schwachstellen in technischen Systemen	Empfohlen
NIS2-Richtlinie (Art. 21)	Sicherheitsmaßnahmen inkl. Penetrationstests für kritische Infrastrukturen	Pflicht (KRITIS)
DORA (Digital Operational Resilience Act)	Threat-Led Penetration Testing (TLPT) für Finanzunternehmen	Pflicht (Finanzsektor)
PCI DSS 4.0 (Req. 11.4)	Jährliche Penetrationstests auf Netzwerk- und Anwendungsebene	Pflicht (Zahlungsverkehr)
BSI IT-Grundschutz (ORP.4)	Regelmäßige Sicherheitsüberprüfungen als Teil des ISMS	Empfohlen
TISAX (VDA ISA)	Sicherheitsprüfungen als Voraussetzung für Automotive-Lieferanten	Pflicht (Automotive)

AWARE7-TIPP

Wenn Ihr Unternehmen unter NIS2, DORA oder PCI DSS fällt, ist ein Penetrationstest keine Kür mehr — er ist eine rechtliche Verpflichtung. Dokumentieren Sie den Test, den Bericht und die umgesetzten Maßnahmen sorgfältig, da Auditoren und Behörden diese Nachweise verlangen können.

AWARE7 als Partner für Ihre Sicherheit

AWARE7 ist ein auf Offensive Security spezialisiertes Cybersicherheitsunternehmen mit Sitz in Gelsenkirchen. Unser Team aus zertifizierten Penetrationstestern (OSCP, CEH, GPEN), Security-Analysten und Auditoren unterstützt Unternehmen aus Industrie, Finanzwesen, Gesundheitswesen und öffentlicher Verwaltung.

Unsere Leistungen im Bereich Penetrationstest:

- Externe und interne Netzwerk-Penetrationstests
- Web Application Penetration Testing (OWASP)
- Active Directory / Azure AD Assessments
- Red Team Exercises
- Social Engineering Assessments
- Mobile Application Security Testing
- Code Reviews (SAST)

Kostenloses Erstgespräch vereinbaren

Wir analysieren Ihre Ausgangssituation und empfehlen die geeignete Pentest-Methodik für Ihre Organisation — ohne Verpflichtung.

Website
a7.de

E-Mail
info@aware7.de

A

Anhang

Glossar, Beauftragungscheckliste und weiterführende Ressourcen

Anhang

Glossar

Begriff	Definition
Black Box	Pentest-Szenario ohne Vorwissen — simuliert externen Angreifer
CVE	Common Vulnerabilities and Exposures — Öffentliches Register bekannter Schwachstellen
CVSS	Common Vulnerability Scoring System — Bewertungsstandard für Schwachstellen-Schweregrade
DMZ	Demilitarisierte Zone — Netzwerksegment zwischen Internet und internem Netz
Exploit	Programm oder Technik zur Ausnutzung einer Schwachstelle
Grey Box	Pentest-Szenario mit Teilinformationen — häufigster Praxisfall
IS-Revision	Konzeptionelle Prüfung: Sind Sicherheitsmaßnahmen geplant und dokumentiert?
Lateral Movement	Ausbreitung im Netzwerk nach initialem Einbruch
NDA	Non-Disclosure Agreement — Geheimhaltungsvereinbarung
OSCP	Offensive Security Certified Professional — Industriestandard-Zertifizierung für Pentester
OWASP	Open Web Application Security Project — Gemeinnützige Organisation für Web-Sicherheitsstandards
Pentest	Penetrationstest — Autorisierter simulierter Angriff auf IT-Systeme
Pivoting	Nutzung eines kompromittierten Systems als Sprungbrett in weitere Segmente
RCE	Remote Code Execution — Codeausführung auf dem Zielsystem aus der Ferne
Re-Test	Nachtest zur Verifikation der Behebung gefundener Schwachstellen
Rules of Engagement	Schriftliche Vereinbarung über Scope, Methoden, Zeitraum und Kontakte eines Pentests
Scope	Prüfumfang — definiert, welche Systeme getestet werden dürfen
SSRF	Server-Side Request Forgery — Angriff über serverseitige HTTP-Anfragen
TLP	Traffic Light Protocol — Klassifizierungsschema für Informationsweitergabe
White Box	Pentest-Szenario mit vollständigem Vorwissen — maximale Prüftiefe

Beauftragungscheckliste

Diese Checkliste basiert auf dem BSI Praxis-Leitfaden IS-Penetrationstests v1.2.

Organisatorische Voraussetzungen

- [ ] Klare Zieldefinition: Was soll der Pentest nachweisen?
- [ ] Genehmigung der Unternehmensleitung liegt vor
- [ ] Systeminhaber aller zu testenden Systeme haben schriftlich zugestimmt
- [ ] Bei Fremdsystemen / Hosting: Genehmigung des Betreibers eingeholt
- [ ] Bei Cloud-Systemen: Genehmigung des Cloud-Anbieters geprüft
- [ ] Datenschutzbeauftragter informiert und eingebunden
- [ ] Betriebsrat / Mitbestimmungspflicht geprüft
- [ ] NDA mit dem Dienstleister unterzeichnet
- [ ] AVV (Auftragsverarbeitungsvertrag) nach DSGVO abgeschlossen

Technische Voraussetzungen

- [ ] Scope-Dokument: IP-Adressen, Domains, Anwendungen, Netzwerke definiert
- [ ] Out-of-Scope explizit dokumentiert
- [ ] Prüftiefe vereinbart (Sicherheitsaudit / Schwachstellenscan / aktiver Pentest)
- [ ] Angriffsszenario vereinbart (Black / Grey / White Box)
- [ ] Testzeitraum und Tageszeiten festgelegt
- [ ] Remote- oder Vor-Ort-Test festgelegt
- [ ] Testkonten mit definierten Rechten bereitgestellt

Kommunikation und Notfallplanung

- [ ] Notfallkontakte (Auftraggeber + Prüfer) ausgetauscht
- [ ] Eskalationspfad für kritische Funde definiert
- [ ] SOC / IT-Betrieb über Testtermin informiert
- [ ] Kickoff-Call mit allen Beteiligten durchgeführt

Qualitätsanforderungen an den Bericht

- [ ] Management Summary (nicht-technisch) gefordert
- [ ] Technischer Teil mit CVSS-Scores und Evidence gefordert
- [ ] Konkrete Handlungsempfehlungen gefordert
- [ ] Abschlussgespräch vereinbart

Weiterführende Ressourcen

Ressource	Verfügbar unter
BSI Praxis-Leitfaden IS-Penetrationstests v1.2	bsi.bund.de
OWASP Testing Guide v4	owasp.org
CVSS v3.1 Specification	first.org/cvss
NVD — National Vulnerability Database	nvd.nist.gov
PTES — Penetration Testing Execution Standard	pentest-standard.org
AWARE7 GmbH — Cybersecurity-Beratung	a7.de